MODELLO DI ORGANIZZAZIONE E GESTIONE (D. lgs. 231/2001 e succ. mod)

MONDIALPOL S.R.L.

PARTE SPECIALE

STORIA DELLE REVISIONI		
DATA	MOTIVO	APPROVATO DAL LEGALE RAPPRESENTANTE
15.05.2023	ENTRATA IN VIGORE - PRIMA STESURA	
30.07.2024	REVISIONE ANNUALE 2024	
01.03.2025	REVISIONE ANNUALE 2025	
10.10.2026	REVISIONE ANNUALE 2026	
	REVISIONE ANNUALE___	
	REVISIONE ANNUALE___	
	REVISIONE ANNUALE___	

MODELLO DI ORGANIZZAZIONE E GESTIONE (D. lgs. 231/2001 e succ. mod)

MONDIALPOL S.R.L.

PARTE SPECIALE

STORIA DELLE REVISIONI		
DATA	MOTIVO	APPROVATO DAL LEGALE RAPPRESENTANTE
15.05.2023	ENTRATA IN VIGORE - PRIMA STESURA	
30.07.2024	REVISIONE ANNUALE 2024	
01.03.2025	REVISIONE ANNUALE 2025	
10.10.2026	REVISIONE ANNUALE 2026	
	REVISIONE ANNUALE___	
	REVISIONE ANNUALE___	
	REVISIONE ANNUALE___	

SOMMARIO

Parte Speciale 1: Prevenzione dei Reati di corruzione nei rapporti con la Pubblica Amministrazione e con soggetti privati in base alla normativa italiana.....7

Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01)..... 7

Corruzione fra privati (art. 2635 c.c.)..... 7

Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)..... 7

Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)..... 7

Concussione (art. 317 c.p.)..... 8

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-320 c.p.)..... 8

Istigazione alla corruzione (art. 322 c.p.)..... 9

Corruzione in atti giudiziari (art. 319-ter)..... 9

Truffa in danno dello Stato, di altro ente pubblico o dell'Unione Europea(art. 640, comma 2, n. 1, c.p.) 9

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bisc.p.)..... 9

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-terc.p.)..... 10

Funzione della Parte Speciale 1..... 10

a) Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di un pubblico servizio: elenco esemplificativo..... 10

Pubblici Ufficiali..... 11

Pubblico Ufficiale..... 11

Pubblica funzione amministrativa..... 11

Norme di diritto pubblico..... 11

Incaricati di un pubblico servizio..... 12

b) Criteri per la definizione dei manager indicati nell'art. 2635 c.c..... 13

Attività Sensibili nei rapporti con la Pubblica Amministrazione e con i soggetti privati..... 14

Regole generali..... 14

Il sistema in linea generale..... 14

Principi generali di comportamento..... 16

Parte Speciale 2: Reati societari - Le fattispecie dei reati societari (art. 25 ter del D.Lgs.231/01)..... 18

False comunicazioni sociali (artt. 2621 e 2622 c.c.)..... 18

Falso in prospetto (art. 2623 c.c.)..... 19

Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)..... 19

Impedito controllo (art. 2625 c.c.)..... 19

Omessa comunicazione di conflitto di interessi (art. 2629-bis c.c.)..... 20

Formazione fittizia del capitale (art. 2632 c.c.)..... 20

Indebita restituzione dei conferimenti (art. 2626 c.c.)..... 20

Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.)..... 21

Illecite operazioni sulle azioni o quote sociali o della società controllante(art. 2628 c.c.)..... 21

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)..... 22

Illecita influenza sull'assemblea (art. 2636 c.c.)..... 22

Ostacolo all'esercizio delle funzioni pubbliche di vigilanza (art. 2638 c.c.)....22
Funzione della Parte Speciale 2....23
Attività Sensibili nell'ambito dei reati societari....24
Regole generali....24
Il sistema in linea generale....24
Principi di comportamento....24
Altre regole finalizzate alla prevenzione dei reati societari in genere Attività soggette a vigilanza....28
Altre attività....29
Area responsabilità strategica generale....30
Protocolli specifici per la gestione della crisi d'impresa e delle procedure concorsuali....30
Protocollo A: Gestione dei flussi informativi verso gli Organi della Procedura e il Revisore Legale 30
Protocollo B: Dismissione di asset e compimento di atti di straordinaria amministrazione....31
Protocollo C: Gestione del conflitto di interessi e recupero crediti verso Amministratori....32
I REATI FISCALI....33
Le fattispecie: panoramica....33
FOCUS SUI REATI FISCALI....34
LE ALTRE FATTISPECIE INTRODOTTE....35
Parte Speciale 3: Il Reato di Autoriciclaggio ed i Reati di Criminalità Organizzata....36
Generalità sul reato di Autoriciclaggio....36
Sanzioni previste....37
La responsabilità 231 per i fatti di autoriciclaggio....38
Condotte punibili....40
La prevenzione del reato di Autoriciclaggio in MONDIALPOL....42
Generalità dei reati inerenti la criminalità organizzata....43
Art. 24-ter - (Delitti di criminalità organizzata)....44
La tipologia dei reati di criminalità organizzata (art. 24- ter deldecreto legislativo 231/2001)....44
Associazione per delinquere (art. 416 c.p.)....44
Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.)....45
Scambio elettorale politico-mafioso (art. 416 ter)....45
Lo schema applicativo dell'art. 24 ter....46
Principali attività a rischio di commissione dei reati....48
Destinatari della parte speciale – principi generali di comportamento nelle aree di attività a rischio....49
Principi di attuazione dei comportamenti descritti....51
Compiti dell'Organismo di vigilanza....51
Parte Speciale 4: Reati di omicidio colposo e lesioni personali colpose derivanti da inosservanza di norme poste a tutela della salute e sicurezza dei lavoratori....52
1. Tipologia di reati previsti....52
Omicidio colposo (art. 589 c.p.)....53
Lesioni colpose gravi o gravissime (art. 590, terzo comma c.p.)....53

2. Funzione della parte speciale - reati in materia si salute e sicurezza sul lavoro..... 54
3. Mappatura del rischio.....56
3.1. Reati in materia di sicurezza sul lavoro - principale attività sensibile.....56
4. Principali attività a rischio..... 57
5. Principi generali di gestione dell'area di rischio..... 64
5.1. Organizzazione aziendale in tema di Salute e Sicurezza Sul Lavoro.....64
5.2 Compiti e responsabilità dei Dirigenti e dei Preposti.....64
5.3 Organizzazione del Servizio di Prevenzione e Protezione.....64
6. Attivita' di monitoraggio e verifica..... 65
7. I flussi informativi..... 66
7.1 Comunicazioni esterne.....67
7.2 Comunicazioni interne.....67
7.3 Coinvolgimento del personale..... 68
7.4 Comunicazioni con l'Organismo di Vigilanza (OdV).....68
8. Regolamentazione delle singole attivita' sensibili..... 68
8.1 Valutazione dei rischi e programma di miglioramento..... 68
8.2 Aggiornamento normativo e verifica di conformità legislativa..... 69
8.3 Sorveglianza Sanitaria.....70
8.4 Formazione, Informazione e Addestramento.....71
8.5 Gestione degli infortuni.....72
8.6 Rapporto con i fornitori..... 72
8.7 Acquisto impianti, macchine e attrezzature.....73
8.8 Manutenzioni.....74
8.9 Verifica dei luoghi di lavoro.....74
8.10 Gestione dei Dispositivi di Protezione Individuale.....75
9. Procedure di riferimento..... 75
Parte Speciale 5: I Reati Ambientali.....77
Le origini comunitarie della tutela penale dell'ambiente.....77
Parte Speciale 6: I Delitti Informatici e il Trattamento illecito dei dati..... 78
Considerazioni generali.....78
L'art. 24 bis D.lgs. 231/2001 - Delitti informatici e trattamento illecito di dati.....79
Il significato dell'art. 24 bis: fattispecie e conseguenze..... 80
LA CONDOTTA TIPICA.....80
SOGGETTO AGENTE..... 80
IL PRESUPPOSTO 231..... 81
LA PREVENZIONE DEL MODELLO ORGANIZZATIVO..... 81
LE SANZIONI..... 81
I reati presupposto.....81
Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico..... 81

Art. 617 - quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche....83
Art. 617-quinquies c.p. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche....84
Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici....85
Art. 635 c.p. - Danneggiamento....85
Art. 635-ter c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità....86
PRINCIPI GENERALI DI COMPORTAMENTO....87
Le "attività sensibili relative ai delitti informatici e di trattamento illecito di dati" ai fini del d.lgs. 231/2001....89
Principi generali di controllo....89
Principi di riferimento specifici relativi alle regolamentazione delle singole attività sensibili....90
Utilizzo di risorse e informazioni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore....90
I controlli dell'organismo di vigilanza....91
Parte Speciale 7: Privacy e Data Protection - GDPR....92
Inquadramento generale della normativa....92
Le regole da applicare....94
Scopo....94
Responsabilità....94
Obblighi....95
La risk analysis in materia di protezione dei dati personali....95
Il consenso....96
La sicurezza dei dati....96
Il DPO (Data Protection Officer)....96
Violazioni dei dati (Data Breach – art. 33 e 34)....97
Sanzioni....97
Diritti degli interessati....98
Diritto alla cancellazione, limitazione e rettifica....98
Diritto alla portabilità....98
Le esigenze dell'organizzazione....99
L'osservanza del regolamento nel modello organizzativo....100
Il principio di funzionamento del sistema....100
L'applicazione delle regole e l'implementazione delle azioni di sistema....100
Parte Speciale 8: Le Segnalazioni Anonime - WHISTLEBLOWING....101
1. Definizioni....101
2. Premessa....106
3. Scopo....106
4. Le Segnalazioni oggetto della presente procedura....107

5. Ambito di applicazione....108
6. Processo di gestione delle Segnalazioni....109
6.1. Canali di Segnalazione....109
6.1.1. Segnalazione interna....109
6.1.2. Segnalazione esterna....110
6.1.3. Divulgazione pubblica....110
6.2. Invio della Segnalazione interna....111
6.3. Ricezione e analisi della Segnalazione interna....111
Verifica preliminare....111
Segnalazioni che non superano la verifica preliminare....112
Segnalazioni che superano la verifica preliminare....113
7. Sistema sanzionatorio e disciplinare....114
7.1. Attivazione del Sistema Sanzionatorio e disciplinare....114
8. Tutele della Persona segnalante e applicazione delle misure di protezione....115
8.1. Limitazioni della responsabilità....117
9. Conservazione e Archiviazione....118
10. Reporting....118
11. Casi particolari....119
12. Delibere dell'OdV....119
13. Divulgazione della procedura....119
ALLEGATO 1 - MODULO DI SEGNALAZIONE....120
ALLEGATO 2: INFORMATIVA PRIVACY PER LA PERSONA SEGNALANTE....121

Parte Speciale 1: Prevenzione dei Reati di corruzione nei rapporti con la Pubblica Amministrazione e con soggetti privati in base alla normativa italiana

Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/01).

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapportitra la Società e la P.A. Si descrivono qui di seguito brevemente le singole fattispecie richiamate nel D.Lgs. 231/01 agli artt. 24 e 25, cui seguono degli esempi astratti di comportamenti vietati da tali norme.

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

Tale ipotesi di reato è stata introdotta quale presupposto della responsabilità penale delle persone giuridiche con la l. 190/2012, che ha sancito la punibilità dell'ente per i comportamenti di corruzione posti in essere nell'interesse della Società, verso soggetti che rivestano posizioni decisionali all'interno di un'altra società, per indurlo a compiere atti in contrasto con gli interessi della Società a cui fa riferimento.

Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta,senza che rilevi che l'attività programmata si sia comunque svolta).

Esempio: uno o più Dipendenti cui sia stata affidata la gestione dei fondiutilizzano gli stessi per scopi diversi da quelli per i quali sono stati erogati (ad es.dei fondi conferiti per scopi formativi o sociali, vengono utilizzati, in parte, per coprire spese di rappresentanza etc.).

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 mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti,

mutui agevolati o altre erogazioni dello stesso tipo 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 (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.

Infine, va evidenziato che tale ipotesi di reato, a differenza della fattispecie precedente, si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Esempio: un Dipendente della società, allo scopo di ottenere una erogazione da parte delle Comunità Europee, presenta alla competente autorità dei documenti falsamente attestanti l'esistenza in capo alla Società di un requisito indispensabile per l'ottenimento del contributo.

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua posizione, costringa taluno aprocurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. 231/01.

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319-320 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale italiano o estero riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere oritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente). L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (adesempio: velocizzare una pratica la cui evasione è di propria competenza), sia inun atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaroper garantire l'aggiudicazione di una gara).

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

Esempio: un Dipendente della società offre una somma di danaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività della società.

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

Corruzione in atti giudiziari (art. 319-ter)

Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

Esempio: un Dipendente offre un'ingente somma di danaro al Pubblico Ministero che conduce indagini penali in merito ad attività svolte dalla società per occultare fatti illeciti ed ottenere l'archiviazione del procedimento.

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

Esempio: un Dipendente, allo scopo di ottenere una licenza od un'autorizzazione amministrativa, induce in errore i pubblici ufficiali incaricati facendo apparire agli stessi una falsa rappresentazione della realtà attraverso la produzione di documenti falsi.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bisc.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.

Esempio: un Dipendente, allo scopo di ottenere delle erogazioni pubbliche induce volontariamente in inganno i pubblici funzionari dell'ufficio competente a decidere della domanda attraverso il concorso di soggetti terzi, i quali, attestino l'esistenza di situazioni fittizie.

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

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico dell'ente pubblico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi.

Funzione della Parte Speciale 1

La presente Parte Speciale si riferisce a comportamenti che possono essere posti in essere dai Dipendenti e dagli Organi Societari di MONDIALPOL nonché dai suoi Consulenti e Partner come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati. Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare i principi procedurali che i Dipendenti, gli Organi Societari, i Consulenti e Partner di MONDIALPOL sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'O.d.V. e ai responsabili delle altre funzioni aziendali che cooperano con esso, i principi cui devono ispirarsi gli strumenti esecutivi necessari per esercitare le attività di controllo, monitoraggio e verifica.

a) Criteri per la definizione di Pubblica Amministrazione e di soggetti incaricati di un pubblico servizio: elenco esemplificativo

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire unelenco esemplificativo di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del D.Lgs. 231/01, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose previste nel Decreto Legislativo citato.

Pubblici Ufficiali

Ai sensi dell'art. 357, comma 1, c.p., è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

Il secondo comma della norma citata si preoccupa poi di definire la nozione di "pubblica funzione amministrativa". Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di "funzione legislativa" e "funzione giudiziaria"in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.

Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "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 ".

In altre parole, è definita "pubblica" la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Il secondo comma dell'art. 357 c.p. elenca alcuni dei principali criteri di massimaper differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico".I caratteri distintivi della prima figura possono essere sintetizzati come segue:

Pubblico Ufficiale

colui che esercita una pubblica funzione legislativa, giudiziaria o amministrativa.

Pubblica funzione amministrativa

viene disciplinata da norme di diritto pubblico e da atti autoritativi ed è caratterizzata dalla formazione e manifestazione della volontà della pubblica amministrazione, o dal suo svolgersi per mezzo di poteri autoritativi o certificativi.

Norme di diritto pubblico

norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico.

Incaricati di un pubblico servizio

La definizione della categoria di "soggetti incaricati di un pubblico servizio" non è allo stato concorde in dottrina così come in giurisprudenza. Volendo meglio puntualizzare tale categoria di "soggetti incaricati di un pubblico servizio", è necessario far riferimento alla definizione fornita dal codice penale e alle interpretazioni emerse a seguito dell'applicazione pratica. In particolare, l'art. 358 c.p. recita che "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 ed alla prestazione di opera meramente materiale.

Il "servizio", affinché possa definirsi "pubblico", deve essere disciplinato – così come la "pubblica funzione" – da norme di diritto pubblico; tuttavia il servizio si caratterizza per l'assenza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

La legge inoltre precisa che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine" né la "prestazione di opera meramente materiale".

La giurisprudenza ha individuato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

(a) la sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici;
(b) la presenza di una convenzione e/o concessione con la pubblica amministrazione;
(c) l'apporto finanziario da parte dello Stato;
(d) la presenza dell'interesse pubblico in seno all'attività economica.

Sulla base di quanto sopra riportato, l'elemento discriminante per indicare se un soggetto rivesta o meno la qualità di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

I caratteri peculiari della figura dell'incaricato di pubblico servizio sono sintetizzati di seguito definendo tale soggetto come colui che a qualunque titolo, presta un pubblico servizio ovvero un'attività:

1. disciplinata da norme di diritto pubblico;
2. caratterizzata dalla mancanza da poteri di natura deliberativa, autorizzativi e certificativi (tipici della Pubblica funzione amministrativa);
3. mirata alla cura di interessi pubblici o al soddisfacimento di bisogni di interesse generale.

Non può mai costituire pubblico servizio lo svolgimento di semplici mansioni di ordine né la prestazione di opera meramente materiale.

b) Criteri per la definizione dei manager indicati nell'art. 2635 c.c.

L'art. 2635 c.c. identifica ai commi 1 e 2 i soggetti che possono divenire destinatari di attività corruttiva analoga a quella considerata per i Pubblici Ufficiali Incaricati di Pubblico Servizio:

1) gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori;
2) chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma

Le figure indicate al comma 1 sono identificate in modo diretto e chiaro, e non pongono particolari problemi. Quelle richiamate al comma 2 invece sono oggetto di un rinvio generale, che si presta a ricomprendere la più vasta tipologia di funzioni aziendali e posizionamento gerarchico. La caratteristica necessaria è quella di detenere un potere decisionale in merito ai rapporti commerciali o comunque di interesse economico che coinvolgano le due società, ovvero quella ipoteticamente "corruttrice" e quella potenzialmente vittima del manager corrotto.

A titolo meramente esemplificativo si indicano alcune figure generalmente presente nel management aziendale, che potrebbero corrispondere alla tipologia rappresentata al punto 2):

- responsabile acquisti e logistica;
- responsabile IT;
- responsabile commerciale;
- responsabile qualità;
- responsabile sicurezza e ambiente;
- responsabile HR;
- responsabile bilancio e fiscalità;
- responsabile operativi.

I manager indicati potrebbero essere fatti oggetto di proposte corruttive per ottenere vantaggi o favori che rappresentino un concreto interesse per la società"corruttrice" nel senso indicato al punto precedente, qualora ciò si rendesse necessario per superare o forzare le corrette dinamiche commerciali e di concorrenza.

Attività Sensibili nei rapporti con la Pubblica Amministrazione e con i soggetti privati

Le principali attività che MONDIALPOL ha individuato al proprio interno come Aree Sensibili nei rapporti con la Pubblica Amministrazione e con i soggetti privati, in relazione ai reati di corruzione e di corruzione fra privati, sono le seguenti:

- gestione del processo commerciale
- gestione del patrimonio mobiliare;
- rapporti con le istituzioni e con le autorità di vigilanza;
- gestione delle ispezioni da parte della Pubblica Amministrazione;
- gestione delle transazioni e delle proposte di trattamento dei crediti tributari e contributivi ex art. 88 CCII nei confronti di Agenzia delle Entrate, INPS e INAIL;
- cessione a terzi del ramo d'azienda "Business 1" inerente gli appalti pubblici e gestione delle procedure di subentro ex art. 120 d.lgs. 36/2023.

Regole generali

Il sistema in linea generale

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, alle procedure ed ai regolamenti aziendali rilevanti nonché alle regole contenute nel presente Modello.

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

Gli strumenti organizzativi della società (organigrammi, comunicazioni organizzative, procedure, ecc.) devono essere improntati a principi generali di:

a) conoscibilità all'interno della società;
b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;

c) chiara descrizione delle linee di report.

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati (rintracciabilità ed evidenziabilità delle Attività Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

Si intende per "procura" il negozio giuridico unilaterale con cui la società attribuisce ad un soggetto dei poteri di rappresentanza nei confronti dei terzi. Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza vengono conferite delle procure di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "delega".

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei Reati sono i seguenti:

a) tutti coloro che intrattengono per conto di MONDIALPOL rapporti con la P.A. econ i soggetti privati, devono essere dotati di delega formale in tal senso;
b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
c) ciascuna delega deve definire in modo specifico ed inequivoco i poteri del delegato e il soggetto (organo o individuo) cui il delegato riporta gerarchicamente ed, eventualmente, gli altri soggetti ai quali le deleghe sono congiuntamente o disgiuntamente conferite;
d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
e) il delegato deve disporre di poteri di spesa ed amministrativi adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

a) le procure, sia speciali che generali, sono conferite esclusivamente a soggetti dotati di delega interna;

b) le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione aziendale che fissi l'estensione di poteri di rappresentanza ed i limiti di spesa numerici;
c) la procura può essere conferita a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche, che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
d) una procedura ad hoc deve disciplinare modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, ecc.);
e) le procure indicano gli eventuali altri soggetti cui sono conferiti congiuntamente o disgiuntamente, in tutto o in parte, i medesimi poteri di cui alla procura conferita.L'O.d.V. verifica periodicamente, con il supporto delle altre funzioni competenti,il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

Principi generali di comportamento

I seguenti principi di carattere generale si applicano, in via diretta, ai Dipendenti e agli Organi Societari di MONDIALPOL e, in forza di apposite clausole contrattuali, ai Consulenti ed ai Partner.

Nei rapporti con i soggetti indicati al precedente punto 1.2), è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati singolarmente o complessivamente, siano idonei ad integrare le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/01). Sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

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

a) effettuare elargizioni in denaro;

b) offrire doni o gratuite prestazioni al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo il cui valore non sia esiguo o sia eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare non devono essere offerti, né direttamente né indirettamente,qualsiasi regalo, doni o gratuite prestazioni che possano essere o, comunque,apparire connessi con il rapporto di affari con la società o miranti ad influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la società stessa. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore e sono volti a promuovere iniziative di carattere benefico o culturale ol'immagine della società.

Le spese di cortesia in occasione di ricorrenze o, comunque, attinenti la sfera dell'immagine e della comunicazione, ivi comprese le sponsorizzazioni, sonosempre autorizzate dalla Direzione, che ne vaglia la rispondenza ai caratteri e dai principi sopra esposti. In ogni caso, qualora sorgano dubbi in merito alla legittimità di una spesa di cortesia è opportuno sempre richiedere l'autorizzazione anche da parte del proprio superiore gerarchico diretto. Quest'ultimo e il Responsabile Acquisti procedono a darne comunicazione informativa all'O.d.V. In tutti i casi i regali o gli omaggi o le spese di cortesia devono essere documentati in modo adeguato per consentire le verifiche da parte dell'O.d.V.

Le liberalità di carattere benefico o culturale eccedenti i valori sopra descritti devono restare nei limiti permessi dalle relative disposizioni legali e dal Modello Organizzativo e dal Codice Etico; inoltre la funzione interessata predispone l'istruttoria e la sottopone alla Direzione. Di tali liberalità e/o contributi viene immediatamente informato l'O.d.V.;

c) accordare, direttamente o indirettamente, vantaggi di qualsiasi natura tali (o effettuati con modalità tali da) costituire una violazione dei principi esposti nel Modello Organizzativo o nel Codice Etico;
d) eseguire prestazioni e riconoscere compensi in favore dei Consulenti o dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
e) presentare dichiarazioni non veritiere ad organismi pubblici nazionali, comunitari e internazionali al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
f) destinare eventuali somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

Parte Speciale 2: Reati societari - Le fattispecie dei reati societari (art. 25 ter del D.Lgs.231/01)

La presente Parte Speciale si riferisce ai reati societari. Si descrivono qui di seguito brevemente le singole fattispecie contemplate nell'art. 25 ter del D.Lgs. 231/01, cui seguono degli esempi astratti di comportamenti vietati da tali norme.

False comunicazioni sociali (artt. 2621 e 2622 c.c.)

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

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- il reato di cui all'articolo 2622 c.c. è punibile a querela, salvo che si tratti di società quotate.

Esempio: il Consiglio di Amministrazione ignora l'indicazione del Responsabile Amministrativo circa l'esigenza di un accantonamento (rettifica) al fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 c.c.).

Falso in prospetto (art. 2623 c.c.)

Tale condotta criminosa consiste nell'esporre nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, false informazioni idonee ad indurre in errore od occultare dati o notizie con la medesima intenzione.

Si precisa che:

- deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto;
- la condotta deve essere idonea a trarre in inganno i destinatari del prospetto;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.Esempio: il Consiglio di Amministrazione omette consapevolmente di rappresentare nel documento informativo destinato alla pubblicazione a seguito di una sollecitazione all'investimento rivolta al pubblico, elementi idonei a formare un giudizio veritiero sui titoli (es. elevato grado di rischio dell'investimento).

Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 2624 c.c.)

Il reato consiste in false attestazioni o nell'occultamento di informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, da parte dei responsabili della revisione contabile, al fine di conseguire per sé o per altri un ingiusto profitto.

La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni. Sebbene i possibili autori di questo reato sono i responsabili della società di revisione (reato proprio), è possibile che i componenti degli organi di amministrazione e di controllo e i suoi Dipendenti possano essere coinvolti a titolo di concorso. È, infatti, ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del responsabile della società di revisione.

Impedito controllo (art. 2625 c.c.)

Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione. Esempio: un funzionario della Società non fornisce al

Revisore Legale o ai Commissari Giudiziali i documenti da questi richiesti nell'esercizio delle proprie attività di controllo, quali, ad esempio, i documenti concernenti le azioni legali intraprese dalla società per il recupero di crediti.

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

L'articolo 2629 bis contempla una fattispecie di reato omissivo. Il comportamento quindi è punito solo se esiste un obbligo giuridico di attivarsi. In questi casi l'obbligo si rinviene direttamente nella legge.

L'obbligo risulta dall'art. 2391 c.c. che disciplina l'ipotesi in cui l'amministratore si trovi in conflitto di interessi con la società, conflitto che sorge quando questi abbia un interesse per conto proprio o di terzi, in una determinata operazione della società. Tuttavia non sempre l'omessa comunicazione del conflitto comporta l'invalidità della delibera del consiglio di amministrazione: questa omissione può diventare penalmente rilevante, anche se non in tutti i tipi di società, ma, in generale, quando tale omissione provenga da un amministratore di una società quotata nei mercati regolamentati o con titoli diffusi tra il pubblico in misura rilevante.

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

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

Esempio: gli amministratori danno luogo ad un aumento del capitale sociale per mezzo dell'offerta di azioni per un valore inferiore a quello dichiarato.

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

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

Esempio: l'Assemblea della Società, su proposta del Consiglio diAmministrazione, delibera la compensazione di un debito del socio nei confrontidella Società con il credito da conferimento che

quest'ultima vanta nei confronti del socio medesimo, realizzando in pratica una restituzione indebita del conferimento.

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

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

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

Esempio: l'Assemblea della Società, su proposta del Consiglio diAmministrazione, delibera la distribuzione di dividendi che costituiscono, non unutile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.

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

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

Esempio: l'organo amministrativo procede all'acquisto o alla sottoscrizione di azioni della Società o di una società controllante fuori dai casi di cui agli artt. 2357e 2359-bis c.c., determinando così facendo una lesione del patrimonio sociale.

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

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

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

Esempio: gli amministratori danno luogo ad un'operazione straordinaria di fusione con una società in stato di forte sofferenza, senza rispettare la procedura prevista dall'art. 2503 c.c. a garanzia dei creditori.

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

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.
Essendo il reato ipotizzabile in sede di liquidazione della Società non appare rilevante in questa sede fornire la descrizione di un esempio di condotta criminosa.

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

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.
Esempio: il Consiglio di Amministrazione della Società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinate anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso consiglio intende acquisire, in modo da ricavarne un indiretto profitto.

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

In tale fattispecie di reato sono soggetti attivi: gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, il revisore legale e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti; nonostante il gran numero di soggetti attivi, si tratta di reato proprio.
Nel testo di legge si identifica il fatto tipico distinguendo due comportamenti diversi, sostenuti da due differenti tipi di dolo.

1. nelle comunicazioni che i soggetti attivi devono, in base alla legge, inviare all'autorità di vigilanza:

a. espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza
b. occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.

In entrambe queste ipotesi l'elemento soggettivo è il dolo specifico, perché il reo deve agire al fine di ostacolare l'esercizio delle funzioni di vigilanza.

2. i medesimi soggetti attivi
    a. in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza, consapevolmente ne ostacolano le funzioni.

Come si vede si tratta di reato a forma libera che può realizzarsi anche con un'omissione, mentre il dolo è generico, poiché l'ostacolare consapevolmente le funzioni delle autorità di vigilanza, più che indicare il fine per il quale agisce il soggetto attivo, sembra voler escludere a priori la possibilità di responsabilità per colpa. È inoltre reato di pericolo. La pena prevista in tutti e due i tipi di condotta è della reclusione da uno a quattro anni, si tratta quindi di delitto. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Funzione della Parte Speciale 2

La presente Parte Speciale si riferisce a comportamenti che possono essere posti in essere dai Dipendenti e dagli Organi Sociali di MONDIALPOL , nonché dai suoi Consulenti e Partner come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati. Nello specifico, la presente Parte Speciale ha lo scopo di:

a) indicare le procedure che i Dipendenti, gli Organi Sociali, i Consulenti e Partnerdella società sono chiamati ad osservare ai fini della corretta applicazione del Modello;
b) fornire all'O.d.V., e ai responsabili delle altre funzioni aziendali che cooperanocon esso, i principi cui devono ispirarsi gli strumenti esecutivi necessari per esercitare le attività di controllo, monitoraggio e verifica.

Attività Sensibili nell'ambito dei reati societari

Le principali attività che MONDIALPOL come già esposto nella Parte Generale del presente documento, ha individuato al proprio interno come Aree Sensibili nell'ambito dei reati societari sono:

- Esercizio delle forme di controllo societario e di direzione di gruppo;
- attività di formazione del bilancio;
- gestione e comunicazione verso l'esterno di notizie e dati relativi allaSocietà;
- operazioni sul capitale sociale;
- gestione dei dati e dei documenti per l'attestazione del professionista indipendente e per i Commissari Giudiziali nel Concordato Preventivo;
- dismissione del patrimonio immobiliare, mobiliare e recupero crediti verso amministratori.

Regole generali

Il sistema in linea generale

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello e, in particolare, a quelle indicate ai successivi paragrafi, gli Organi Societari (e i Dipendenti e Consulenti nella misura necessaria alle funzioni dagli stessi svolte) devono in generale conoscere e rispettare:

- l'organizzazione, nonché le procedure aziendali e il sistema di controllodella gestione che lo compongono;
- la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale;
- le norme inerenti il sistema amministrativo, contabile, finanziario, direporting;
- il sistema di comunicazione al personale e di formazione dello stesso;
- il sistema disciplinare di cui al CCNL;
- in generale, la normativa italiana applicabile.

Principi di comportamento

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali della società, presenti (o futuri in caso di trasformazioni societarie), e deiDipendenti e Consulenti nella misura

necessaria alla funzioni dagli stessi svolte,di porre in essere, collaborare o dare causa alla realizzazione di comportamentitali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 ter del D.Lgs. 231/01); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale. La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- tenere un comportamento corretto, trasparente e collaborativo, nelrispetto delle norme di legge e delle procedure aziendali interne, in tutte le attivitàfinalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società.

In conseguenza, è fatto divieto di:

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci,relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziariadella società;
b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società.
c) alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi;
d) 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;
e) fornire dati falsi od omettere informazioni rilevanti in ordine alla situazione economica e patrimoniale ai professionisti incaricati per l'attestazione, al Tribunale e ai Commissari Giudiziali;
f) distrarre, occultare o alienare immobili, automezzi o altri asset sociali in pregiudizio ai creditori concorsuali, al di fuori delle previsioni del piano di concordato o senza il rispetto di procedure competitive.

- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.

In particolare, è fatto divieto di agire in modo tale da far si che gli Organi Sociali Competenti adottino uno dei seguenti comportamenti o atti:

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

- assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

In conseguenza, è fatto divieto di:

a) 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 dei soci;
b) 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.

- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

In conseguenza, è fatto divieto di:

a) omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabilenei confronti delle autorità di vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;

b) esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;

c) 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).

L'attività di formazione del bilancio e, in particolare, predisposizione delle comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della società (bilancio d'esercizio e bilancio consolidato corredati dalla relazione sulla gestione, relazioni trimestrali e semestrale, ecc.), devono essere redatti in modo tale che sia garantito il rispetto dei seguenti precetti aziendali:

- i dati e le informazioni, fornite da ciascuna funzione ai fini della redazione dei documenti volti a rappresentare la situazione economica, patrimoniale e finanziaria della società, devono:
  - rispondere a principi di chiarezza e completezza;
  - essere interpretati in conformità ai criteri contabili utilizzati per la elaborazione dei dati;
- le valutazioni delle singole voci di bilancio e delle relazioni infrannuali devono essere eseguite in conformità alle disposizioni di legge;
- i documenti volti a fornire una rappresentazione della situazione economica, patrimoniale e finanziaria della società devono esporre e illustrare tutte le informazioni e i dati, anche di carattere complementare, da ritenersi necessari alfine di dare una rappresentazione veritiera e corretta della situazione della Società;
- la redazione deve essere effettuata a seguito del preventivo esame e approvazione della Direzione, per ciò che concerne i comunicati stampa riguardanti le informazioni a carattere periodico e le operazioni straordinarie (aumenti di capitale, fusioni, ecc).

Inoltre:

- gli Organi Sociali, i Dipendenti e i Consulenti sono tenuti a mantenere riservati i documenti e le informazioni rilevanti acquisite nello svolgimento delle loro funzioni e a rispettare le procedure dettate per la comunicazione all'esterno di talidocumenti e informazioni;

- è fatto assoluto divieto a chiunque di rilasciare interviste a organi di stampa o fare dichiarazioni che si riferiscano a fatti rilevanti che non siano già stati resi pubblici a norma di legge.
- tutte le operazioni sul capitale sociale di MONDIALPOL , nonché la costituzionedi società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle procedure aziendali all'uopo predisposte;
- è fatto divieto di porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento dell'attività di controllo o di revisione della gestione sociale della società da parte del revisore legale o degli organi della procedura concorsuale..

Altre regole finalizzate alla prevenzione dei reati societari in genere Attività soggette a vigilanza

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

- alle segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti(ad es., bilanci e verbali delle riunioni degli Organi Sociali);
- alla trasmissione di dati e documenti specificamente richiesti dalle autorità divigilanza;
- al comportamento da tenere nel corso degli accertamenti ispettivi.I principi a cui tali procedure si informano sono i seguenti:
- attuazione di tutti gli interventi di natura organizzativo-contabile necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni edil loro puntuale invio all'autorità di vigilanza, secondo le modalità ed i tempi stabiliti dalla normativa applicabile;
- adeguata formalizzazione delle procedure in oggetto e successiva documentazione dell'esecuzione degli adempimenti in esse previsti, con particolare riferimento all'attività di elaborazione dei dati;

- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di interloquire con l'autorità;
- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati ed essere tenuto informato l'O.d.V. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati gli appositi verbali. Dell'avvio di ispezioni deve essere tempestivamente informato l'O.d.V., con nota scritta da parte del responsabile della funzione coinvolta.

Altre attività

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

- attivazione di un programma di formazione-informazione periodica delpersonale rilevante sulle regole e sui reati societari;
- trasmissione all'Autorità competente, con congruo anticipo, di tutti i documentirelativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensidi legge;
- formalizzazione e/o aggiornamento di regolamenti interni e procedure aventiad oggetto l'osservanza della normativa societaria.

Fermo restando il potere discrezionale dell'O.d.V. di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello) e ferme restando le specifiche attribuzioni di cui al precedente paragrafo, l'O.d.V. effettua periodicamente, anche coadiuvato da soggetti terzi, controlli a campione sulle attività sociali potenzialmente a rischio di commissione di reati societari, al fine di verificare chela gestione concreta di tali attività avvenga in maniera conforme alle regole e coerente con i principi dettati dal presente Modello (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato reporting verso gli organi deputati,ecc.).

In ragione dell'attività di vigilanza attribuita all'O.d.V. nel presente Modello, a taleorganismo viene garantito, in generale, libero accesso a tutta la documentazione aziendale che lo stesso ritiene rilevante al fine del monitoraggio dei Processi Sensibili individuati nella presente Parte Speciale (vedi Parte Generale).

Area responsabilità strategica generale

Devono essere rispettati i limiti di budget di spesa previsti dalle deleghe. Eventuali superamenti di tali limiti dovranno essere preventivamente approvati dal C.d.A. su richiesta del delegato motivata e fornita di idonea documentazione.La delibera di spesa per atti eccedenti i limiti delega deve essere trasmessa all'O.d.V.

Protocolli specifici per la gestione della crisi d'impresa e delle procedure concorsuali

In ragione dell'accesso della Società alla procedura di Concordato Preventivo in continuità aziendale (*ex* artt. 84 e ss. CCII), al fine di prevenire la commissione di reati societari, fallimentari e di ostacolo all'esercizio delle funzioni di vigilanza (con particolare riferimento a Commissari Giudiziali, Attestatore indipendente e Revisore Legale), i Destinatari del presente Modello sono tenuti alla rigorosa osservanza dei seguenti protocolli di controllo:

<u>Protocollo A: Gestione dei flussi informativi verso gli Organi della Procedura e il Revisore Legale</u>

Il presente protocollo è finalizzato a garantire la massima trasparenza, veridicità e completezza dei dati economici, patrimoniali e finanziari trasmessi agli organi preposti al controllo e all'omologazione del piano concordatario, scongiurando i reati di False comunicazioni sociali (artt. 2621 e 2622 c.c.) e Ostacolo all'esercizio delle funzioni pubbliche di vigilanza (art. 2638 c.c.).

Tracciabilità delle fonti: Qualsiasi dato, prospetto contabile o proiezione finanziaria fornita al Professionista Indipendente (Attestatore), ai Commissari Giudiziali o al Tribunale deve essere estratto dai sistemi informativi aziendali ufficiali. Il percorso di estrazione e il file sorgente devono essere salvati e immodificabili.

Certificazione interna: Prima della trasmissione all'esterno, ogni documento o report (inclusi i report periodici ex art. 44 CCII) deve essere validato dal Responsabile dell'Area Amministrativa e formalmente approvato dall'Amministratore Delegato.

Gestione delle richieste degli Organi di Controllo: Le richieste di documentazione da parte del Revisore Legale e dei Commissari Giudiziali devono essere evase con la massima tempestività. In caso di oggettiva impossibilità a rispettare le scadenze richieste, il Responsabile della funzione interpellata deve inviare comunicazione formale e motivata agli Organi richiedenti e, per conoscenza, all'OdV.

Divieto di filtro: È fatto assoluto divieto a chiunque di filtrare, alterare, manipolare o occultare informazioni, contratti o passività (inclusi potenziali contenziosi, pendenze tributarie o inadempimenti) idonei a influenzare il giudizio dell'Attestatore o l'esito della procedura concorsuale.

Protocollo B: Dismissione di asset e compimento di atti di straordinaria amministrazione

Il presente protocollo disciplina le alienazioni del patrimonio mobiliare e immobiliare (es. immobili non strumentali, flotta aziendale, cessione del ramo d'azienda "Business 1") al fine di tutelare la par condicio creditorum e prevenire il reato di Operazioni in pregiudizio dei creditori (art. 2629 c.c.) e le condotte distrattive.

Autorizzazioni preliminari: Qualsiasi atto di disposizione del patrimonio sociale (vendita, permuta, affitto di ramo d'azienda, costituzione di pegni o ipoteche) non rientrante nell'ordinaria gestione deve essere preventivamente autorizzato con delibera del Consiglio di Amministrazione e, ove prescritto dal CCII, dal Giudice Delegato, previo parere dei Commissari Giudiziali.

Congruità dei valori: Le alienazioni di beni immobili e rami d'azienda devono avvenire sulla base di perizie di stima giurate, redatte da professionisti indipendenti.

Procedure competitive: Salvo diversa e motivata autorizzazione del Tribunale, la cessione di asset significativi o rami d'azienda deve avvenire mediante procedure competitive a evidenza pubblica o,

per i beni minori (es. singoli automezzi), mediante l'acquisizione tracciabile di almeno tre preventivi/offerte di acquisto da soggetti terzi indipendenti.

Tracciabilità finanziaria: I proventi derivanti dalle dismissioni devono confluire esclusivamente su conti correnti dedicati e vincolati alla procedura concordataria. È fatto divieto di operare compensazioni dirette tra crediti della società e debiti verso l'acquirente senza l'autorizzazione degli organi della procedura.

Protocollo C: Gestione del conflitto di interessi e recupero crediti verso Amministratori

In relazione alla presenza di posizioni creditorie della Società verso i propri esponenti aziendali (crediti verso amministratori), il protocollo mira a prevenire l'omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.) e l'infedeltà patrimoniale (art. 2634 c.c.).

Segregazione delle funzioni (Segregation of Duties): Gli Amministratori debitori della società non possono in alcun modo partecipare alle deliberazioni consiliari aventi ad oggetto le modalità di rientro, le transazioni, gli accolli o la rinuncia ai crediti vantati dalla Società nei loro confronti, dovendosi astenere ai sensi dell'art. 2391 c.c.

Validazione dei piani di rientro: Eventuali accordi di dilazione, datio in solutum (es. cessione di immobili personali a saldo del debito) o atti di accollo relativi al debito degli amministratori devono essere istruiti dal Responsabile dell'Area Amministrativa/Legale, certificati nella loro convenienza per la Società dal Revisore Legale, e sottoposti alla vincolante autorizzazione del Tribunale o dei Commissari Giudiziali.

Monitoraggio dell'OdV: Le scritture private, gli atti notarili e le evidenze dei flussi finanziari relativi al rientro del debito degli amministratori devono essere trasmessi in copia all'Organismo di Vigilanza entro 5 giorni lavorativi dal loro perfezionamento.

I REATI FISCALI

A pochi mesi dal Decreto Fiscale, il D.Lgs. 75/2020 (in vigore dal 30 luglio 2020)estende nuovamente il catalogo dei reati presupposto per la responsabilitàdell'ente. La novella richiama fattispecie di diritto penale tributario, ma non solo:viene ampliato anche il novero dei reati in danno alla PA e viene prevista la responsabilità degli enti per i reati di contrabbando.

Reati 231 aggiornati 2020: in gazzetta ufficiale del 15 luglio 2020 è statopubblicato il decreto legislativo 14 luglio 2020 n. 75, che recepisce la "direttiva europea (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".

Le fattispecie: panoramica

Quella dell'inserimento dei reati tributari nel novero dei reati presupposto per la responsabilità degli enti ex D.Lgs. 231/2001 è, come noto, una vicenda che risalealla c.d. Direttiva PIF (UE 2017/1371), con cui l'Unione europea ha demandato ai legislatori nazionali l'adozione di misure adeguate a contrastare, anche con gli strumenti del diritto penale, le cc.dd. gravi frodi IVA, con ciò dovendo intendersi quelle condotte caratterizzate da fraudolenza e transnazionalità che recano un danno agli interessi finanziari dell'Unione Europea non inferiore a euro 10 mln.

Nel catalogo dei reati presupposto per l'applicazione delle sanzioni cosiddette amministrative da reato è stato inserito il delitto di frode in pubbliche forniture (art.356 codice penale), si è integrato l'art. 25 con il riferimento all'Unione Europea quale soggetto finanziariamente leso nei casi di peculato, anche mediante profitto dell'errore altrui (articoli 314 e 316 codice penale) e abuso d'ufficio (articolo 323 codice penale).

Per i reati in materia di imposte sui redditi e sul valore aggiunto ai sensi del decreto legislativo 10 marzo 2000 n. 74, da oggi 30 luglio 2020 sono previste sanzioni amministrative severe (da trecento a cinquecento quote) se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro. L'art. 25-sexiesdecies, di nuova introduzione, inoltre, aggiunge al catalogo dei reati presupposto il contrabbando, punito con sanzioni da duecento a quattrocento quote, a seconda del valore dei diritti di confine evasi (inferiore o superiore centomila euro).

In tutti questi casi (art. 25-sexiesdecies) si applicano le sanzioni interdittive:

- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenerele prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventualerevoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

FOCUS SUI REATI FISCALI

Il Decreto Fiscale ha introdotto la responsabilità amministrativa degli enti per idelitti di:

- dichiarazione fraudolenta di cui all'art. 2 , co. 1 (sanzione pecuniaria fino a 500quote), all'art. 2, co. 2-bis (sanzione pecuniaria fino a 400 quote) e all'art. 3 (sanzione pecuniaria fino a 500 quote) D.Lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti di cui all'art. 8, co 1 (sanzione pecuniaria fino a 500 quote) e all'art. 8, co. 2-bis (sanzione pecuniaria fino a 400 quote), D.Lgs. 74/2000;
- occultamento o distruzione di documenti contabili di cui all'art. 10 D.Lgs.74/2000 (sanzione pecuniaria fino a 400 quote);
- sottrazione fraudolenta al pagamento di imposte di cui all'art. 11 D.Lgs. 74/2000(sanzione pecuniaria fino a 400 quote).

Il Decreto Fiscale ha inoltre previsto:

- una circostanza aggravante all'art. 25-quinquiesdecies, co. 2, D.Lgs. 231/2001 (con aumento della sanzione pecuniaria fino a un terzo) per il caso in cui l'ente abbia conseguito un profitto di rilevante entità dall'illecito;
- l'applicazione delle sanzioni interdittive richiamate all'art. 25-quinquiesdecies, co. 3, D.Lgs. 231/2001 (che richiama l'art. 9, co. 2, lett. c), d), ed e)), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

LE ALTRE FATTISPECIE INTRODOTTE

Le novità introdotte dal D.Lgs. 75/2020 in materia di responsabilità degli enti nonsi esauriscono ai reati tributari.

Viene infatti altresì modificato l'art. 24 D.Lgs. 231/2001, così ampliando il catalogo dei reati in danno alla Pubblica Amministrazione (nella cui ampia nozione deve ora ricomprendersi, secondo la novella che ha interessato l'art. 24,anche l'Unione europea):

- Al comma primo viene aggiunto il delitto di frode nelle pubbliche forniture ex art.356 c.p., cui consegue una sanzione pecuniaria fino a 500 quote;
- È poi aggiunto un comma 2-bis, che prevede l'applicazione della sanzione pecuniaria fino a 500 quote in caso di frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L.898/1986).

Anche per le nuove fattispecie ora richiamate dall'art. 24 è prevista l'applicazione della circostanza aggravante prevista dal co. 2 (per il caso in cui l'ente abbia conseguito un profitto di rilevante entità ovvero dall'illecito sia derivato un danno di particolare gravità: in questo caso la sanzione pecuniaria sarà da 200 a 600 quote) e delle sanzioni interdittive previste dal co. 3, che richiama l'art. 9, co. 2, lett. c), d), ed e), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

Sempre all'area dei reati che recano danno alla PA devono essere ricondotte le fattispecie che il D.Lgs. 75/2020 ha affiancato a quelle già previste all'art. 25, co.1, D.Lgs. 231/2001:

- I reati di peculato di cui all'art. 314 c.p., primo comma (rimanendo dunque escluso il peculato d'uso) e all'art. 316 (ossia la particolare forma di peculato mediante profitto dell'errore altrui);
- Il reato di abuso d'ufficio di cui all'art. 323 c.p.

Alle predette fattispecie è collegata una sanzione pecuniaria per l'ente fino a 200 quote, "quando il fatto offende gli interessi finanziari dell'Unione Europea".

Infine, il D.Lgs. 75/2020 introduce nel D.Lgs. 231/2001 un nuovo art. 25- sexiesdecies rubricato "Contrabbando", che inaugura la responsabilità degli enti per i reati previsti dal D.P.R. 43/1973 in materia doganale, che prevede (in particolare, si veda l'art. 295, norma fra l'altro interessata da alcune modifiche apportate proprio dal D.Lgs. 75/2020) sanzioni anche penali in caso di mancato pagamento dei diritti di confine. Il nuovo art. 25-sexiesdecies prevede per questi casi:

- La sanzione pecuniaria fino a 200 quote;
- Un'aggravante per il caso in cui l'ammontare dei diritti di confine dovuti superi euro 100.000 (sanzione pecuniaria fino a 400 quote);

L'applicazione delle sanzioni interdittive di cui all'art. 9, co. 2, lett. c), d), ed e), ossia: il divieto di contrattare con la PA (salvo che per ottenere prestazioni di un pubblico servizio); l'esclusione da agevolazioni, finanziamenti, contributi o sussidie l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

Parte Speciale 3: Il Reato di Autoriciclaggio ed i Reati di Criminalità Organizzata

Generalità sul reato di Autoriciclaggio

Il reato (nuovo art. 648-ter.1, c.p.) punisce colui che impiega, sostituisce, trasferisce in attività economiche, finanziarie, imprenditoriali o speculative ildenaro, i beni o le altre utilità derivanti dal delitto non colposo (di seguito, anche"reato-base") che lo stesso ha commesso o concorso a commettere. Ciò a condizione che la condotta sia idonea a ostacolare concretamente l'identificazione della provenienza illecita della provvista.

Fermo restando che si prevede la non punibilità delle condotte di mero utilizzo o godimento personale della provvista illecita, in linea con l'assunto per cui tali ipotesi costituiscono la naturale prosecuzione del reato- base (il c.d. post factum non punibile).

La nuova disciplina incontra l'interesse di MONDIALPOL poiché è stato inserito tra i reati presupposto della responsabilità amministrativa degli enti ai sensi del Decreto legislativo n. 231/2001 (art. 25-octies).

Le nuove previsioni sono oggetto a tutt'oggi di un vivace dibattito dottrinale, in assenza di applicazioni giurisprudenziali significative, dal momento che la portata applicativa delle stesse appare a molti piuttosto vasta, consentendo di introdurre de facto molte fattispecie finora escluse dalla qualifica di reato presupposto. A titolo di esempio possiamo indicare che, sulla scorta di alcuni orientamenti della giurisprudenza in tema di riciclaggio, se il reato tributario dell'infedele dichiarazione è compiuto dall'amministratore nell'interesse della società, il risparmio di imposta si confonde nel patrimonio sociale e quindi si configura in via automatica il reimpiego in attività economica. Pertanto, se questa impostazione dovesse essere confermata anche in materia di

autoriciclaggio, l'amministratore autore della dichiarazione infedele potrebbe essere chiamato a rispondere anche per l'autoriciclaggio, ad esempio, per aver pagato i dipendenticon la provvista illecita, anche laddove non si sia attivato per far perdere la tracciadel collegamento tra il delitto-base e l'utilità.

L'azienda auspica che che non si incorra in imputazioni automatiche per autoriciclaggio e che si dia seguito alle intenzioni del legislatore, richiamate ancheda una parte della dottrina, interpretando con rigore l'art. 648-ter.1 e, quindi, valorizzando l'elemento più caratterizzante delle condotte di riciclaggio, vale a dire l'idoneità a nascondere la natura illecita dei proventi. Questo approccio consentirebbe, infatti, di escludere la configurazione in concreto dell'autoriciclaggio nei casi in cui non è possibile identificare e isolare dal patrimonio del contribuente il provento illecito oggetto delle successive operazioni di reimpiego, sostituzione o trasferimento.

(Fonti: Istituto di Studi sulla Responsabilità Amministrative degli Enti. Circolare n.19867 Confindustria)

Tenuto conto degli orientamenti che si profilano, Il Modello Organizzativo di MONDIALPOL ha inserito il nuovo reato fra i presupposti della responsabilità e ha adeguato le relative previsioni di rischio per le attività sensibili che possono risultare interessate dalle disposizioni di legge, aumentando le pene relative.

Le sessioni di audit per verificare la concreta pericolosità delle attività stesse dovranno essere svolte nel corso del 2017 - 2018, e verranno opportunamente documentate nei progressivi verbali, e relazionate nel report finale dello stesso anno.

Sanzioni previste

L'art. 648 ter 1 punisce con la pena della reclusione da due a otto anni e la multa da euro 5.000 a euro 25.000 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.

Al secondo comma si prevede una cornice edittale più tenue - reclusione da uno a quattro anni e multa da 2.500 a 12.500 euro - se il delitto non colposo presupposto è punito con la reclusione non superiore nel massimo a cinque anni. Tornano invece ad applicarsi le più severe pene di cui al primo

comma se si tratta di delitto commesso con le condizioni e le modalità di cui all'art. 7 del Decreto Legge n. 152 del 1991, convertito dalla Legge n. 203 del 1991, che contempla l'aggravante del c.d. metodo e fine dell'agevolazione mafiosa.

Al quarto comma si stabilisce invece una causa di non punibilità per «le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale».

La disposizione si chiude con la previsione di una circostanza aggravanteallorché i fatti sono commessi

nell'esercizio di attività bancaria o finanziaria odialtra attività professionale e con una diminuzione rilevante di pena - fino alla metà

- nel caso l'autore «si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto».

Il quarto comma dell'art. 648 ter 1 c.p. stabilisce che «fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale». Tale previsione sembra definire in negativo i contorni della fattispecie: da un lato, l'area della rilevanza penale segnata dall'impiego in attività economiche, finanziarie, imprenditoriali o speculative, dall'altro, l'area della non punibilità costituita dal mero utilizzo o godimento personale.

La responsabilità 231 per i fatti di autoriciclaggio

Con l'inserimento del nuovo delitto di autoriciclaggio all'interno dell'art. 25 octies,e posto che ogni «delitto non colposo» produttivo di un provento può costituire il reato-presupposto del delitto di autoriciclaggio, la teorica espansione della responsabilità da reato dell'ente, ricorrendone ovviamente tutte le altre condizioni previste dal D.Lgs. 231/2001 deve essere temperata dall'applicazione rigorosa dei principi di legalità e tassatività.

In particolare, per potersi configurare responsabilità dell'ente ai sensi del D.Lgs.231/2001 per il reato di autoriciclaggio, appare necessario che:

1. un soggetto apicale o subordinato commetta o concorra a commettere un delitto non colposo produttivo di un provento, presumibilmente (ma non necessariamente) nell'interesse

o a vantaggio dell'ente; quest'ultimo ne sarà responsabile ai sensi del D.Lgs. 231 /2001 solo se ciò sia espressamente previsto da detto Decreto.

2. lo stesso soggetto poi impieghi, sostituisca o trasferisca (in attività economiche, finanziarie, imprenditoriali o speculative) quel provento (in ciò concretandosi la condotta di autoriciclaggio) «nell'interesse o a vantaggio» dell'ente (che quindi abbia la disponibilità o tragga vantaggio dall'utilizzo dei proventi del delitto non colposo commesso dal proprio soggetto apicale o dal dipendente), "in modo da ostacolare concretamente l'identificazione della provenienza delittuosa" del provento medesimo. È dubbio peraltro che l'art. 25 octies possa essere interpretato nel senso di escludere la rilevanza, ai fini della configurabilità dell'illecito amministrativo dell'ente, di condotte che abbiano a oggetto proventi di reati non previsti nell'elenco dei reati presupposto. È comunque essenziale la funzione selettiva, sia ai fini della responsabilità penale del soggetto agente, che della responsabilità amministrativa dell'ente, svolta dal requisito del concreto ostacolo alla provenienza delittuosa: esso dovrà essere puntualmente riscontrato, per evitare il rischio di punire per autoriciclaggio anche operazioni di reimpiego delle utilità illecite prive di quell'ulteriore disvalore penale che fonda la punibilità del reato di cui all'art. 648 ter c.p. In altri termini, sarà necessario accertare la sussistenza di condotte dissimulatorie ovvero anomale rispetto all'ordinaria attività mentre semplici operazioni "tracciabili", non avendo tali caratteristiche, non dovrebbero assumere rilevanza penale;diversamente si priverebbe di significato la precisa scelta del legislatore di esigere una idoneità 'qualificata' dell'operazione a impedire la ricostruzione dellaprovenienza delittuosa del denaro, dei beni e della utilità che sono oggetto.
3. Il reato di autoriciclaggio sussiste nelle ipotesi in cui le relative condotte siano successive al perfezionamento del reato che ha dato origine ai proventi illeciti, anche se compiute dopo la sua estinzione (ad es. per prescrizione), o anche se l'autore del medesimo non sia imputabile o punibile, oppure manchi una condizione di procedibilità (ad es., per difetto di querela, oppure di richiesta del Ministro della Giustizia, necessaria per perseguire i reati comuni commessi all'estero, ai sensi degli artt. 9 e 10 c.p.).

Le attività sub 2) erano già punibili, peraltro, a titolo di riciclaggio o reimpiego, conconseguente possibile responsabilità dell'ente, ad eccezione però dei casi in cuiad agire fosse l'autore o

concorrente nel delitto presupposto, situazione oggi coperta dall'art. 648 ter 1 c.p. (Fonte: Circolare ABI n. 6 del 1 Dicembre 2015)

Condotte punibili

L'autoriciclaggio (al pari del riciclaggio) è un reato a forma libera, che può essere integrato da qualsiasi condotta idonea ad ostacolare concretamente l'identificazione della provenienza delittuosa del bene impiegato, sostituito ovvero trasferito, in attività economiche, finanziarie, imprenditoriali o speculative.

In questa prospettiva possono essere utili le osservazioni già svolte dalla giurisprudenza di legittimità con riguardo al riciclaggio: è stato infatti osservato dalla Suprema Corte (es., Cass. Sez. IV del 23.3.2000) che le condotte devono essere concretamente idonee a dissimulare la provenienza delittuosa del bene con la conseguenza di impedire, tra l'altro, possibili iniziative investigative.Rilevano in questo ambito anche tutte quelle attività volte a ostacolare la segnalazione di operazione sospetta ai sensi dell'art. 41 del D.Lgs. 231/2007, con la conseguenza che appaiono sempre più legate la disciplina penale (rectiusartt. 648-bis, 648- ter, 648-ter.1) e la disciplina dei presidi antiriciclaggio che ha dato applicazione alla III Direttiva.

Ciò posto, in giurisprudenza sono state individuate talune condotte che, pur essendo calibrate sul reati di cui agli artt.648-bis e 648-ter c.p., a mio avviso possono comunque essere applicabili anche al reato di autoriciclaggio. Segnatamente:

- integra il reato di riciclaggio il compimento di operazioni volte non solo adimpedire in modo definitivo, ma anche a rendere difficile l'accertamento della provenienza del denaro, dei beni o delle altre utilità, attraverso un qualsiasi espediente che consista nell'aggirare la libera e normale esecuzione dell'attività posta in essere (ex plurimis, Cass. 2818/2006; Cass. 16980/2007);
- il semplice trasferimento di danaro di provenienza illecita da un conto corrente a un altro integra gli estremi del reato di riciclaggio, essendo sufficienteа tal proposito il solo dolo eventuale. Il delitto di riciclaggio è infatti configurabile attraverso un "qualsiasi prelievo o trasferimento di fondi successivo a precedentiversamenti o anche con un mero trasferimento di denaro di provenienza da un conto corrente bancario a un altro diversamente intestato, e

acceso presso un differente istituto di credito" ovvero anche tra conti correnti accesi presso lo stesso istituto di credito;

- integra di per sé un autonomo atto di riciclaggio, essendo il reato di cui all'art. 648- bis c.p. a forma libera e potenzialmente a consumazione prolungata,attuabile anche con modalità frammentarie e progressive, qualsiasi prelievo o trasferimento di fondi successivo a precedenti versamenti, ed anche il mero trasferimento di denaro di provenienza delittuosa da un conto corrente bancario ad un altro diversamente intestato, ed acceso presso un differente istituto di credito. (Fattispecie in cui è stata ritenuta penalmente rilevante l'operazione di svuotamento della cassa di un gruppo societario ed il successivo trasferimento del denaro ad un soggetto, attraverso assegni circolari e bonifici, con l'incarico direimpiegare le somme per finanziare altra società - Cass, Sez. II, 43881/2014);
- integra il delitto di riciclaggio la sostituzione, con denaro, di documenti fiscali provenienti dal delitto di cui all'art. 8, D.Lgs. 10.3.2000, n. 74 (Cass., Sez.II, 17.5.2013, n. 29452);
- commette il delitto colui che accetta di essere indicato come beneficiario economico di conti correnti accesi all'estero, formalmente intestati a società aventi sede in paradisi fiscali, ma in realtà appartenenti a terzi, e sui quali confluiscono i proventi di attività delittuosa (Cass., Sez. VI, 22.5.2013, n. 24548). A seguito dell'evoluzione normativa delle fattispecie del codice penale e della disciplina penal-tributaria, il rapporto tra la disciplina antiriciclaggio e il fenomeno dell'evasione fiscale è ancora più stretto, in ragione dell'indubbio arricchimento (in termini sia di elementi informativi acquisibili, sia di strumenti di contrasto) assicurato dal sistema antiriciclaggio alla lotta contro i fenomeni evasivi, soprattutto se connotati da elevata insidiosità.

In questa prospettiva, secondo l'insegnamento della Suprema Corte, i delitti dichiarativi e di emissione di fatture fittizie possono sicuramente essere reati presupposto dell'autoriciclaggio, poiché nel concetto di "altre utilità" ben si può ricomprendere il risparmio di spesa che l'agente ottiene evitando di pagare le imposte dovute anche se commesso all'estero.

Non è un caso, infatti, che la costante giurisprudenza della Suprema Corte ritieneche costituisca profitto dei reati tributari la somma corrispondente all'impostaevasa, sicché , ai sensi della Legge Finanziaria n. 244 del 2007, art. 1, comma 143, se ne ammette il sequestro preventivo finalizzato alla successiva confisca. Di conseguenza è assolutamente evidente che chi commette un reato tributario

oggi potrebbe vedersi perseguito anche per autoriciclaggio, qualora occulti oreimpieghi i proventi dell'evasione; specularmente, a carico di società potrebberotrovare applicazione tanto le sanzioni tributarie quanto le rischiosissime sanzioni "231/2001". Posto che, come noto, la legge n. 186/2014 inserisce l'autoriciclaggioanche nell'elenco dei reati presupposto della responsabilità degli enti disciplinatadal D.Lgs. n. 231/2001.

Ma proprio in relazione a quest'ultime Confindustria segnala che tale scelta del legislatore rende particolarmente severa la risposta sanzionatoria (con dubbi di compatibilità con il principio ordinamentale del ne bis in idem – Corte europea dei diritti dell'uomo del 4.3.2014), in quanto per i reati tributari si cumulerebbero le seguenti sanzioni:

- amministrativa;
- penale per il reato base;
- penale per l'autoriciclaggio;
- amministrativa ai sensi del Decreto 231, a carico dell'impresa.

(Fonte: Giovanni Barbato, Commento alla Circolare n. 19867 di Confindustria)

La prevenzione del reato di Autoriciclaggio in MONDIALPOL

Indicatori di rischio

Alcuni esempi di indicatori di rischio con riferimento a operazioni ovvero flussi in entrata e in uscita "sospetti":

- pagamento agli amministratori di emolumenti non deliberati ovverodeliberati, ma in misura sproporzionata all'attività;
- pagamenti ai parenti degli amministratori per non meglio precisate attivitàdi consulenza;
- pagamento di compensi agli amministratori a titolo di consulenza;
- pagamento di consulenze a società che si trovano in paesi black list o off- shore;
- pagamenti effettuati per attività svolte da controparti italiane, maaccreditate su conti correnti di società in paesi black list o off-shore;
- aumenti di capitale effettuati da società con sedi in paesi black list o off-shore;
- finanziamenti soci provenienti da società fiduciarie o esterovestite;

- finanziamenti soci ricorrenti anche da parte di una società del gruppo partecipante o controllante senza una sottostante ragione di ordine imprenditoriale e reiterati prelievi a titolo di rimborso finanziamento soci non deliberati dal CdA;
- movimentazione eccessiva del conto di cassa senza una descrizione analitica delle operazioni compiute nel mastrino di cassa o nel libro giornale;
- sponsorizzazioni o donazioni per importi sensibili a Fondazioni o Onlus non meglio individuate;
- operazioni di significativo ammontare in assenza di motivazioni correlate al proprio business;
- operazioni ripetute e di ammontare significativo effettuate in contropartita con società che risultano create di recente e hanno un oggetto sociale generico o incompatibile con il business della società;
- stipula di rapporti contrattuali con vincoli o pegni a favore di terzi che non presentano alcun collegamento con la società;
- acquisto di un ingente ammontare di strumenti finanziari a elevata liquidità seguito dalla richiesta di prestiti garantiti dagli stessi strumenti finanziari;
- frequenti operazioni di investimento a lungo termine in strumenti finanziari immediatamente seguite dalla richiesta di liquidare la posizione e di trasferire i relativi proventi

Generalità dei reati inerenti la criminalità organizzata

Con la Legge n. 94 del 23 luglio 2009, recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonche in materia di energia (c.d. Legge Sicurezza Pubblica) il legislatore italiano ha disposto modifiche al decreto legislativo 231/2001. In conseguenza, dopo l'art. 24-bis relativo ai delitti informatici, è stato inserito l'art. 24-ter in materia di delitti di criminalità organizzata.

L'inserimento dei delitti contro la criminalità organizzata tra i reati presupposto previsti dal d.lgs. 231/01 risale all'applicazione dell'art. 10 della legge 146/2006 "Ratifica della Convenzione ONU sulla lotta alla criminalità organizzata transnazionale" aveva già previsto alcuni delitti associativi tra i reati presupposto nel caso in cui tali reati avessero carattere transnazionale. Tale introduzione ed estensione anche all'ambito nazionale risponde all'esigenza di rafforzare la lotta contro la criminalità di impresa.

Art. 24-ter - (Delitti di criminalità organizzata).

1In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416- bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosidelle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolarel'attività delle associazioni previste dallo stesso articolo, nonché ai delitti previsti dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.

In relazione alla commissione di taluno dei delitti di cui all'articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applica la sanzione pecuniaria da trecento a ottocento quote.

Nei casi di condanna per uno dei delitti indicati nei commi 1 e 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno.

Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati indicati neicommi 1 e 2, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3.

Il nuovo articolo 24-ter del d.lgs. 231/2001 presenta, quindi, due diverse tipologie di delitti di criminalità organizzata con trattamento sanzionatorio differenziato.

La tipologia dei reati di criminalità organizzata (art. 24- ter deldecreto legislativo 231/2001).

Si riporta di seguito una breve descrizione dei reati contemplati nell'art. 24-ter del Decreto 231 la cui commissione possa comunque comportare un interesse e/o un vantaggio per la Società.

Associazione per delinquere (art. 416 c.p.)

Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. I capi soggiacciono alla stessa pena stabilita per i promotori. Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più. Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioniconcernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di

cui al decreto legislativo 25 luglio 1998, n. 286, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.

Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.)

Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone,è punito con la reclusione da sette a dodici anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da nove a quattordici anni. 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 deriva 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. Se l'associazione è armata si applica la pena della reclusione da nove a quindici anni nei casi previsti dal primo comma e da dodici a ventiquattro anni nei casi previsti dal secondo comma. 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. Se 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 pene stabilite nei Modello di organizzazione, gestione e controllo commi precedenti sono aumentate da un terzo alla metà. Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono e furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego. Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e 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.

Scambio elettorale politico-mafioso (art. 416 ter)

La pena stabilita dal primo comma dell'articolo 416 bis si applica anche a chi ottiene la promessa di voti prevista dal terzo comma del medesimo articolo 416 bis in cambio di erogazione di denaro. Le

norme in esame riguardano la criminalità organizzata, fenomeno che provoca un elevato allarme sociale nella collettività a causa della maggiore potenzialità delinquenziale delle organizzazioni rispetto al singolo autore di reato, ovvero della maggiore pericolosità del programma criminoso dell'organizzazione rispetto al disegno criminoso del singolo individuo.

Le fattispecie di cui sopra si riferiscono alla semplice partecipazione, nonché alla promozione, direzione, costituzione, organizzazione di un'associazione, composta da tre o più persone e dotata, anche in minima parte, di una "strutturazione" (divisione di compiti, gerarchie etc.), e di "stabilità" che permettono di distinguerla dal semplice concorso di persone nel reato, caratterizzato, invece, dall'occasionalità e accidentalità dell'accordo criminoso. Lo scopo dell'associazione deve essere, anche se non unico e prevalente, quellodi realizzare un programma criminoso, cioè la commissione di uno o più reati.

Lo schema applicativo dell'art. 24 ter

L'art. 24 ter, con una formulazione non troppo lineare, riferendosi genericamente ai reati di cui all'art. 416 c.p., considera come "ipotesi base" la commissione, in forma organizzata di qualsiasi delitto, ad esclusione di quelli, ritenuti più gravi, dicui all'art. 416 c. 6 c.p. (v. appresso), nonché dei delitti previsti dal 407 c. 2 lett.

a) n. 5 c.p.p. (delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110). Lo stesso articolo 24 ter, prevede poi, alcune "ipotesi aggravate" di "reato/i-fine"rispetto all'ipotesi base:

- richiamando l'art. 416 c. 6 c.p., include tra queste la commissione in forma associata dei reati di:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavi (art. 602)
- Promozione, direzione, organizzazione, finanziamento del trasporto, o il trasporto stesso, di stranieri nel territorio dello Stato in violazione delle norme contro l'immigrazione clandestina, ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio

dello Stato, ovvero di altro Stato del quale lapersona non è cittadina o non ha titolo di residenza permanente, in presenza di due o più delle seguenti condizioni:

a) il fatto riguarda l'ingresso o la permanenza illegale nel territorio dello Stato di cinque o più persone;
b) la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
c) la persona trasportata è stata sottoposta a trattamento inumano o degradanteper procurarne l'ingresso o la permanenza illegale;
d) il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
e) gli autori del fatto hanno la disponibilità di armi o materie esplodenti.

- richiamando gli articoli 416 bis, 416 ter e 630 c.p. si riferisce alla commissione in forma associata dei reati di:

- Associazioni di tipo mafioso anche straniere • Scambio elettorale politico- mafioso
- Sequestro a scopo di rapina o di estorsione

- richiamando (i delitti di cui al)l'art. 74 del D.P.R. n. 309/1990 si riferisce alla:

- Associazione finalizzata al traffico di sostanze stupefacenti o psicotrope

Altre ipotesi aggravate a cui fa riferimento l'art. 24 ter sono quelle in cui i delitti (qualsiasi delitto) vengano commessi in forma associata avvalendosi della forzadi intimidazione del sodalizio di tipo mafioso e della condizione di assoggettamento e di omertà che ne deriva, e quella in cui i delitti medesimi vengano commessi al fine di agevolare l'attività delle associazioni di tipo mafioso.Modello di organizzazione, gestione e controllo E' opportuno precisare che è associazione di tipo mafioso quella in cui, coloro che ne fanno parte, si avvalgono della forza intimidatrice e della condizione di assoggettamento e di omertà che ne deriva, per commettere delitti, nonché per acquisire in modo diretto o indiretto la gestione o il controllo di attività economiche, concessioni, autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti ovvero impedire il libero esercizio del voto odi procurare voti a sè o ad altri. E' punita, inoltre, la condotta di chi agevola l'attività delle associazioni di tipo mafioso o ottiene la promessa di voti in cambiodi erogazione di denaro. Le disposizioni dell'articolo 416 bis si applicano anche alla camorra, alla 'ndrangheta e 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.

La Legge n. 94 del 23 luglio 2009, recante disposizioni per lo sviluppo el'internazionalizzazione delle imprese, nonché in materia di energia (c.d. Legge Sicurezza Pubblica) ha disposto modifiche al decreto legislativo 8 giugno 2001,

n. 231. In particolare, dopo l'art. 24-bis relativo ai delitti informatici, è stato inseritol'art. 24-ter in materia di delitti di criminalità organizzata.

L'inserimento dei delitti contro la criminalità organizzata tra i reati presupposto previsti dal d.lgs. 231/01 non rappresenta una novità assoluta. Infatti, l'art. 10 della legge 146/2006 "Ratifica della Convenzione ONU sulla lotta alla criminalità organizzata transnazionale" aveva già previsto alcuni delitti associativi tra i reati presupposto nel caso in cui tali reati avessero carattere transnazionale. Tale introduzione ed estensione anche all'ambito nazionale risponde all'esigenza di rafforzare la lotta contro la criminalità di impresa.

Principali attività a rischio di commissione dei reati

Lo scopo di questa Parte Speciale è di definire canoni comportamentali volti a disciplinare aspetti propri della gestione caratteristica per i quali, tramite attività di risk assessment, sono stati rilevati potenziali profili di rischiosità in relazione aldettato del D.Lgs. 231/01. In particolare, si fa riferimento a quanto previsto dal Decreto in relazione alle seguenti tipologie di attività:

- Approvvigionamento di beni e servizi e inserimento anagrafiche fornitori nel sistema;
- Gestione delle attività amministrativo-contabili e dei pagamenti relativi ad approvvigionamento di beni e servizi;
- Gestione contratti di appalto e inserimento anagrafiche clienti nel sistema;
- Gestione delle attività amministrativo-contabili e degli incassi relativi al ciclo attivo;
- Attività di dismissione dei cespiti aziendali e relativi adempimenti amministrativo-contabili e di incasso;
- Operazioni su quote di capitale sociale e altre operazioni straordinarie e di quelle di acquisto/vendita di strumenti finanziari; Modello di organizzazione, gestione e controllo

- Gestione del personale: dipendenti, agenti e rappresentanti, consulenti e altri collaboratori esterni e relativi adempimenti amministrativo-contabili e dipagamento;
- Attività di sponsorizzazione e gestione di eventi.

Le Leggi che regolano questa materia prevedono sanzioni penali per chiunque ne trasgredisca la lettera e lo spirito. Tra gli specifici presidi di controllo che l'azienda deve adottare per esimersi dalla responsabilità per i nuovi reati con finalità associativa (art. 24-ter), si deve tenere conto che il rischio maggiore è rappresentato dalla "controparte": in concreto, la principale attività di prevenzione per questo categoria di reati è rappresentata dalla verifica che la persona fisica o giuridica con la quale la Società intrattiene rapporti commerciali sia in possessodi adeguati requisiti di professionalità e di onorabilità.

Particolare attenzione viene data alla stipula di contratti ed al puntuale ed effettivosvolgimento di prestazioni concordate in conformità delle leggi vigenti. E' necessario verificare l'affidabilità dei fornitori e delle parti terze con i quali MONDIALPOL intrattiene rapporti di fornitura di tali servizi. Particolare attenzione dovrà essere posta alla stipula dei contratti ed al puntuale ed effettivo svolgimento delleprestazioni concordate in conformità alle leggi vigenti.

Destinatari della parte speciale – principi generali di comportamento nelle aree di attività a rischio

Questa Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti della Società nelle aree di attività a rischio,nonché da Collaboratori, Consulenti e Partners con essa operanti sulla base di un rapporto contrattuale, anche temporaneo (qui di seguito, tutti denominati "Destinatari").

Al fine di individuare l'ownership dei processi svolti nelle aree sensibili, tutti i Destinatari sono considerati "responsabili" per ogni singola operazione a rischioda loro direttamente compiuta o comunque effettuata nell'ambito della funzione di loro riferimento.

La presente Parte Speciale ha l'obiettivo di disciplinare la condotta dei Destinatari affinché adottino comportamenti conformi a quanto previsto nel Modello Organizzativo, al fine di impedire il verificarsi dei reati contemplati nel Decreto. Quanto premesso, tra gli attori coinvolti nei processi di gestione e monitoraggio nelle aree sensibili si rilevano:

- Presidente;
- Consiglio di Amministrazione;

- Direzione Generale;
- Responsabile Area Amministrativa;
- Responsabile Area Acquisti;
- Responsabile Qualità;
- Collaboratori esterni.

Rimane inteso che tutti i soggetti interni ed esterni alla Società, quali che siano tipo e livello della loro collaborazione, sono tenuti alla stretta osservanza di quanto prescritto nel Modello. In linea generale, è espressamente vietato agli organi societari e ai dipendenti della Società (nonché ai Consulenti ed i Partner nella misura necessaria alle funzioni dagli stessi svolte):

- porre in essere, promuovere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato tra quelle considerate nella presente sezione (art. 24-ter e art. 25-novies del D.Lgs. 231/2001);
- utilizzare stabilmente l'ente o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei Reati di cui alla presente sezione;
- promuovere, costituire, organizzare o dirigere associazioni che si propongono ilcompito di atti di violenza con fini illeciti;
- assumere commesse, fornire prodotti o effettuare qualsivoglia operazionecommerciale e/o finanziaria, sia in via diretta che per il tramite di interposta persona, con soggetti – persone fisiche o persone giuridiche - i cui nominativi siano stati segnalati dalle autorità europee e internazionali preposte alla prevenzione dei Reati di associazione a delinquere;
- effettuare operazioni o assumere commesse ritenute anomale per tipologia o oggetto ed instaurare o mantenere rapporti che presentano profili di anomalia; effettuare prestazioni in favore delle società di servizi, dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi; Modello di organizzazione, gestione e controllo
- riconoscere compensi in favore delle società di servizi, dei Consulenti e dei Partner che non trovino adeguata giustificazione in relazione al tipo di incarico dasvolgere ed alle prassi vigenti in ambito locale.

Principi di attuazione dei comportamenti descritti

Al fine dell'efficace attuazione di quanto sopra riportato, i dipendenti, gli organi societari (nonché i Consulenti ed i Partner nella misura necessaria alle funzioni dagli stessi svolte) operano in base a procedure che consentono quanto segue:

- i dati raccolti relativamente ai rapporti con clienti, Consulenti e Partner devono essere completi ed aggiornati, sia per la corretta e tempestiva individuazione deimedesimi sia per una valida valutazione del loro profilo;
- la gestione anomala dei rapporti sia preventivamente rilevata e tempestivamente rifiutata e gli indici di anomalia predefiniti siano in grado di selezionare tale anomalia.
- forniture a prezzi/ condizioni generali palesemente non allineate agli standard di mercato, determinabili secondo la normale diligenza devono essere segnalateall'OdV;
- raccolta di informazioni sul fornitore che consentano di valutare in modo più completo il profilo reputazionale della controparte. Tali verifiche possono anche essere affidate a strutture esterne alla Società;
- visite in loco presso le unità produttive del fornitore volte a valutare la capacità di fornire beni che rispettino gli standard qualitativi richiesti e le specifiche di Legge applicabili;

Compiti dell'Organismo di vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'art. 24 ter del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso. I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne idelitti di cui all'art. 24 ter del D. Lgs. n. 231/2001 del Decreto sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cuiall'art. 24 ter del Decreto;

- proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti connessi ai reati di criminalità organizzata di cui alla presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti. Qualora fossero accertate dall'OdV violazioni del Modello Organizzativo, ivi comprese le specifiche procedure adottate, lo stesso Organismo di Vigilanza informa di ciò, senza indugi, il Consiglio di Amministrazione e il Collegio Sindacale, qualora nominato.

Parte Speciale 4: Reati di omicidio colposo e lesioni personali colpose derivanti da inosservanza di norme poste a tutela della salute e sicurezza dei lavoratori.

In considerazione delle caratteristiche societarie ed organizzative, la presente Parte Speciale riguarda i reati previsti dall'art. 25−septies del D. Lgs. n. 231/01 (di seguito, anche, i "Reati in materia di salute e sicurezza sul lavoro") e, in particolare, i comportamenti che devono essere tenuti dai soggetti che operano nelle aree a rischio reato.

La presente Parte Speciale è inerente alle condotte poste in essere dai componenti degli Organi Sociali e dai Dipendenti, compresi il Datore di Lavoro ed il Responsabile del Servizio di Prevenzione e Protezione (RSPP), anche per il tramite di fornitori, consulenti e lavoratori autonomi e parasubordinati, che svolgono la propria prestazione all'interno della Società coinvolti nei processi sensibili in materia di salute e sicurezza sul lavoro.

Tutti i destinatari della Parte Speciale sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato, al fine di prevenire la commissione dei reati individuati nell'ambito della normativa di riferimento.

1. Tipologia di reati previsti

L'art. 9 della Legge 13 agosto 2007, n. 123 ha introdotto nel Decreto l'art. 25−septies, il quale prevede l'applicazione delle relative sanzioni agli Enti i cui esponenti commettano i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme

antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (se l'Ente viene condannato per uno dei delitti di cui alla presente parte speciale, si applicano le sanzioni interdittive di cui all'art. 9, comma 2 del Decreto, per una durata non inferiore a tre mesi e non superiore ad un anno nonché una sanzione pecuniaria in misura non inferiore a mille quote). Si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nel citato art. 25− septies.

Omicidio colposo (art. 589 c.p.)

La fattispecie in esame si realizza quando si cagioni per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Il reato si potrebbe realizzare in caso di morte di un lavoratore cagionata da una violazione delle norme in materia di salute e sicurezza sul lavoro finalizzata, ad esempio, ad un risparmio economico o di tempi da parte della Società.

Lesioni colpose gravi o gravissime (art. 590, terzo comma c.p.)

La fattispecie in esame si realizza quando si cagiona ad altri per colpa una lesione personale grave o gravissima con violazione delle norme per la prevenzione degli infortuni sul lavoro.

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

Ai sensi dell'art. 583 c.p., la lesione personale è:

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

E' gravissima se dal fatto deriva:

1. una malattia certamente o probabilmente insanabile;
2. la perdita di un senso;
3. la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o delle capacità di procreare, ovvero una permanente e grave difficoltà della favella;

4. la deformazione, ovvero lo sfregio permanente del viso.

Per quanto riguarda la disciplina in materia antinfortunistica, nello specifico, è richiesta l'osservanza non solo di tali norme ma anche dell'articolo 2087 c.c., laddove vengano omesse quelle misure e quegli accorgimenti tali da consentire una più efficace tutela delle integrità fisica dei lavoratori.

2. Funzione della parte speciale - reati in materia si salute e sicurezza sul lavoro

La presente parte del Modello riferita alle fattispecie di reato previste dall'art. 25 septies, ossia i reati commessi in violazione delle norme antinfortunistiche e tutela dell'igiene e della salute sul lavoro, descrive e documenta la struttura del Sistema di Gestione della Salute e Sicurezza, in linea con la Norma OHSAS 18001:2007, implementato e applicato da Mondialpol S.R.L. e costituisce il riferimento primario per la verifica periodica della conformità del Modello da parte dell'Organismo di Vigilanza.

Tale parte del Modello è implementata in conformità a quanto previsto dall'art. 30 del D.Lgs. 81/2008 e

s.m.i. L'evento dannoso, sia esso rappresentato dalla lesione grave o gravissima o dalla morte, può essere perpetrato tramite un comportamento attivo (l'agente pone in essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante un atteggiamento omissivo (l'agente semplicemente non interviene a impedire l'evento dannoso).

Di norma, si ravviserà una condotta attiva nel dipendente che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva sarà usualmente ravvisabile nel personale apicale che non ottempera agli obblighi di vigilanza e controllo e in tal modo non interviene ad impedire l'evento da altri causato.

Sotto il profilo soggettivo, l'omicidio o le lesioni rilevanti ai fini della responsabilità amministrativa degli enti dovranno essere realizzati mediante colpa.

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

- evidenziare il sistema formalizzato delle deleghe adottato da Mondialpol Security come strumento organizzativo che permette di definire i ruoli, i compiti e gli incarichi operativi dei vari soggetti aziendali, con particola−re riferimento a quelli relativi alle attività di prevenzione e di sicurezza nei luoghi di lavoro;

- indicare le regole procedurali che tutti i soggetti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi e le informazioni necessarie per esercitare le attività di controllo, monitoraggio e verifica.

Oltre alle regole di cui al presente Modello, i Destinatari devono in generale conoscere e rispettare, con riferimento alla rispettiva attività, tutte le regole e i principi contenuti nei seguenti documenti:

- Codice Etico;
- Documento di Valutazione dei Rischi;
- tutte le procedure/istruzioni/disposizioni aziendali poste in essere in materia di salute e sicurezza sul lavoro previste dal Sistema di Gestione per la Salute e la Sicurezza.

In conformità alla normativa vigente in materia di salute e sicurezza del lavoro, Mondialpol S.R.L. adotta un'organizzazione basata sui seguenti principi e norme di comportamento:

- evitare i rischi e prevenire le situazioni di rischio;
- valutare i rischi che non possono essere evitati;
- ridurre i rischi alla fonte;
- adeguare il lavoro all'uomo, in particolare per quanto concerne la concezione dei posti di lavoro e la scelta delle attrezzature di lavoro e dei metodi di lavoro e di produzione, in particolare per attenuare il lavoro monotono e il lavoro ripetitivo e per ridurre gli effetti di questi lavori sulla salute;
- tener conto del grado di evoluzione della tecnica;
- sostituire ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- programmare la prevenzione, mirando a un complesso coerente che integri nella medesima la tecnica, l'organizzazione del lavoro, le condizioni di lavoro, le relazioni sociali e l'influenza dei fattori dell'ambiente di lavoro;
- dare la priorità alle misure di protezione collettiva rispetto alle misure di protezione individuale; promuovere e attuare attività di formazione, informazione e addestramento sulla sicurezza;
- impartire adeguate istruzioni ai lavoratori;

- favorire il coinvolgimento di tutte le funzioni aziendali nelle attività di analisi e prevenzione dei rischi.

Tutta l'azienda, sia ai livelli apicali che a quelli operativi, deve attenersi a questi principi, in particolare quando devono essere prese delle decisioni o fatte delle scelte e, in seguito, quando le stesse devono essere attuate.

3. Mappatura del rischio

3.1. Reati in materia di sicurezza sul lavoro - principale attività sensibile

SETTORE	AREE DI ATTIVITÀ	REATI	PRINCIPALI DIREZIONI / UNITA' COINVOLTE	PRINCIPALI SOGGETTI ESTERNI COINVOLTI	RISCHIO INERENTE
Prevenzione e protezione	Gestione della salute e sicurezza sul luogo di lavoro. Le aree aziendali di attività nelle quali possono essere concretamente essere sviluppati i fattori di rischio generali validi per tutti i lavoratori e i terzi. Sono analiticamente individuati all'interno del Documento di valutazione dei rischi della Società	Omicidio colposo Lesioni personali colpose	Legale rappresentante (datore di lavoro) Responsabile del servizio di Prevenzione e Protezione Responsabile del personale	Medico competente	RISCHIO MEDIO

4. Principali attività a rischio

Tenendo conto delle attività di rilevazione e valutazione dei rischi, dei sistemi di controllo previsti dalla legge, dell'attuazione delle misure di prevenzione e protezione ai fini di tutelare i dipendenti e garantire la sicurezza e la salute nei luoghi di lavoro, tale processo ha portato all'individuazione di alcune attività (attività sensibili), che, perla loro natura o per l'organizzazione nel cui contesto sono svolte, potrebbero in concreto comportare il rischio di configurazione di fattispecie di reati quali l'omicidio o le lesioni colposi.

Elemento fondamentale per l'individuazione dei rischi relativi al compimento dei reati in questione è il "Documento di valutazione dei rischi", nel quale vengono indicati i rischi eventuali in relazione alle norme infortunisti che ed alla tutela nei luoghi di lavoro.

In ragione delle prescrizioni del decreto legislativo 81/2008 e s.m.i. e della normativa vigente in materia di antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro e alla luce dei controlli attualmente esistenti presso l'azienda, sono stati, quindi, individuati i principi di comportamento e i protocolli di prevenzione che devono essere attuati per prevenire, per quanto ragionevolmente possibile, l'omissione di presidi alla sicurezza e alla salute nei luoghi di lavoro e la conseguente commissione della descritta tipologia di reati.

La seguente tabella consente di identificare, nei diversi processi aziendali, le attività a rischio potenziale, dalle quali possono derivare potenziali cause di reato.

In premessa è importante sottolineare che anche in questo caso, nessun amministratore della Società, così come nessun collaboratore risulta condannato ovvero inquisito per le fattispecie di reato di cui trattasi.

E' inoltre importante sottolineare che il Mondialpol S.R.L. si è dotata di un Sistema di Gestione per la Salute e la Sicurezza dei Lavoratori in conformità con la BS OHSAS 18001: 2007, secondo le previsioni normative dell'art. 30 del D.Lgs. 81/2008 e s.m.i..

PROCESSO SENSIBILE	DESCRIZIONE ATTIVITA' DI RISCHIO	RESPONSABILE DEL PROCESSO	POTENZIALI CAUSE DI REATO	MISURE DI MITIGAZIONE - PROTOCOLLI IN ESSERE	RISCHIO RESIDUO
	Elaborazione e aggiornamento	Legale rappresentante	Mancata individuazione	Procedura di gestione dei	

Valutazione dei rischi e programma di miglioramento	del documento di valutazione rischi	(datore di lavoro) Responsabile del servizio di Prevenzione e protezione	e aggiornamento dei rischi e delle misure di prevenzione e protezione	documenti e delle registrazione (PO02) Procedura di individuazione e gestione dei rischi (PO16) Documenti di valutazione dei rischi ai senti del D.lgs. 81/08 e s.m.i. Procedure di gestione delle modifiche (PO23)	BASSO
	Definizione e gestione del programma delle misure	Legale rappresentante (datore di lavoro) Responsabile del servizio di Prevenzione e protezione	Incidente che si verifica a fronte di un rischio per il quale erano previsti interventi ma non sono stati eseguiti. Assenza di vigilanza nell'attuazione del programma	Documenti di valutazione dei rischi ai sensi del D.Lgs 81/08 e s.m.i. Procedura di gestione dei controlli (PO10) Procedura Audit interni (PO17)	BASSO
	Predisposizione del bilancio previsionale aziendale	Legale rappresentante (datore di lavoro)	Mancata destinazione di risorse per l'attuazione del programma	Documenti di valutazione dei rischi ai sensi del D.Lgs 81/08 e s.m.i. Procedura Riesame della Direzione (PO01) Programma annuale di miglioramento	BASSO
Aggiornamento normativo	Identificazione ed esegesi delle norme	Legale rappresentante (datore di lavoro)	Incidente che si verifica in ambiti regolati da	Procedura di gestione dei documenti e registrazioni	

		Responsabile del Servizio di Prevenzione e Protezione	specifiche norme di legge non conosciute dall'azienda	(PO02) Procedura di individuazione e gestione dei rischi (PO16) Procedura gestione informazione, formazione e addestramento (PO18) Gestione degli Audit interni(PO17)	BASSO
	Attuazione e controllo delle attività di adeguamento	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e protezione Caposervizio	Incidente che si verifica in ambiti regolati da specifiche norme di legge conosciute dall'azienda ma non applicate o applicat in modo errato		
Gestione emergenze	Redazione aggiornamento e diffusione del piano di emergenza	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Mancata adozione delle misure necessarie ai fini della prevenzione incendi, dell'evacuazion e dei lavoratori e del pronto soccorso in azienda	Procedura di gestione delle emergenze (PO20) Procedura gestione informazione, formazione e addestramento (PO18) Istruzioni operative Mansionario (Allegato 4) Manuale ad uso della Guardia Particolare Giurata e dell'operatore Documento di valutazione dei rischi Piano di Emergenza Interno Documento di valutazione del rischio incendio Registro delle sorveglianze Piano di	BASSO
	Nominae formazione degli addetti all'emergenza	Legale rappresentante (datore di lavoro)	Mancata formazione dei lavoratori incaricati alla gestionedelle emergenze. Non presenza di addetti al momento dell'incidente		
	Addestramento emergenze	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Assenza d'istruzioni per l'abbandono delle aree pericolose in caso di emergenza.		

				Emergenza delle aziende committenti DUVRI aziende committenti	
Sorveglianza sanitaria	Gestione della verifica di idoneità dei lavoratori	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione Responsabile del personale Caposervizio Medico competente	Incidente dovuto alla non idoneità del lavoratore alla mansione	Procedura di sorveglianza sanitaria (PO21) Procedura di controllo del servizio (PO09)	BASSO
	Aggiornamento del protocollo sorveglianza sanitaria	Medico competente	Malattia professionale non indagata dal medico competente per assenza di informazioni sui rischi di mansione o sulle attività specifiche dell'addetto nell'ambito della mansione	Procedura di sorveglianza sanitaria (PO21)	BASSO
Formazione lavoratori	Formazione lavoratori Nuove assunzioni Cambi mansioni	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Mancata formazione sui rischi e sulle modalità operative	Procedura gestione informazione, formazione e addestramento (PO18)	BASSO
	Analisi eventi e definizione azioni	Legale rappresentante (datore di	Mancata attuazione di specifiche	Procedura gestione informazione,	

Gestione incidenti e infortuni	correttive	lavoro) Responsabile del Servizio di Prevenzione e Protezione Caposervizio	misure di prevenzione e protezione al verificarsi di un evento che non ha causato infortuni, o ne ha causato di lieve entità, solo per circostanze casuali	formazione e addestramento (PO18) Procedura di gestione delle non conformità (PO12) Registro infortuni Documento di valutazione dei rischi Procedura di controllo del servizio (PO09)	BASSO
Contratti d'appalto e d'opera	Qualifica dei fornitori	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Assenza di verifica dell'idoneità tecnico professionale del fornitore	Documento di valutazione dei rischi Procedura di gestione dei lavori in appalti (PO22) Procedura di gestione dei documenti e delle registrazioni (PO02)	BASSO
	Informazioni sui rischi, misure di prevenzione ed emergenza		Carenza di informazioni ai fornitori sui pericoli esistenti nelle aree nelle quali opera o sui divieti		
	Vigilanza sull'operato dei fornitori		Conseguenze per lavoratori dovuta ad omessa vigilanza sulle misure di prevenzione		
	Valutazione dei rischi per interferenze		Mancata analisi dei rischi correlati alla presenza contemporanea di diversi fornitori o dall'attività		

			dell'azienda in presenza di fornitori		
Modifica strutture, impianti e processi	Definizione e/o progettazione di modifiche di processo, di layout o strutturali	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Mancata applicazione del controllo preventivo del rischio Mancata valutazione dei rischi / aggiornamento	Documento di valutazione dei rischi Procedura di gestione delle modifiche (PO23)	BASSO
Manutenzione	Esecuzione e registrazione manutenzioni, delle verifiche periodiche su attrezzature e impianti che possono generare incidenti	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Assenza o carenza di attività di manutenzione, verifica e controllo	Procedura di controllo del servizio (PO09)	BASSO
	Esecuzione e registrazione manutenzione, verifica e controllo delle verifiche periodiche sui presidi di prevenzione e protezione			Procedura di gestione dei documenti e delle registrazioni (PO02) Registro delle sorveglianze	BASSO
Luoghi di lavoro	Verifica dello stato dei luoghi di lavoro	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Mancata vigilanza sulla idoneità di strutture e luoghi di lavoro	Documento di valutazione dei rischi Procedura di gestione dei documenti e delle registrazioni (PO02) Audit interni	BASSO
	Scelta dei DPI	Legale	Scelta di DPI	Procedura di	

Gestione DPI		rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	non adeguati ai rischi	gestione dei DPI aziendali (PO19) Documento di valutazione dei rischi	BASSO
	Distribuzione, manutenzione e informazione sull'utilizzo dei DPI	Responsabile del Servizio di Prevenzione e Protezione Ufficio personale	Mancata fornitura, manutenzione sostituzione dei DPI		
	Formazione dei lavoratori	Responsabile del Servizio di Prevenzione e Protezione	Mancata informazione sul corretto utilizzo dei DPI	Procedura di gestione dei DPI aziendali (PO19) Procedura di informazione, formazione e addestramento (PO18)	BASSO
	Controllo dei lavoratori	Responsabile del Servizio di Prevenzione e Protezione Preposti	Mancata sorveglianza sul corretto uso dei DPI	Procedura di gestione dei DPI aziendali (PO19) Procedura di gestione dei controlli (PO10)	BASSO
Attività esterne presso committenza	Attività di vigilanza ispettiva	Legale rappresentante (datore di lavoro) Responsabile del Servizio di Prevenzione e Protezione	Mancata valutazione dei rischi specifici	Documento di valutazione del rischio Documento di valutazione rischio specifico Procedura di gestione dei documenti e delle registrazioni (PO02) Procedura di	BASSO
			Mancata formazione e informazione al lavoratore sul DUVRI e Piano emergenza committente		

				gestione delle offerte e contratti (PO12) Procedura di informazione, formazione e addestramento (PO18)	

5. Principi generali di gestione dell'area di rischio

5.1. Organizzazione aziendale in tema di Salute e Sicurezza Sul Lavoro

E' predisposto un adeguato sistema di designazioni in materia di salute e sicurezza secondo i principi di:

- effettività − sussistenza e compresenza di autonomia decisionale e finanziaria del delegato;
- idoneità tecnico−professionale del delegato;
- vigilanza sull'attività del delegato, non acquiescenza, non ingerenza;
- certezza, specificità e consapevolezza.

5.2 Compiti e responsabilità dei Dirigenti e dei Preposti

Sono presenti disposizioni organizzative emanate ed approvate dagli organi societari delegati che definiscono in funzione dei ruoli e delle competenze, le responsabilità dei dirigenti e dei preposti in coerenza con le disposizioni di legge vigenti in materia.

ll dirigente e il preposto deve essere informato delle responsabilità ad esso attribuite e adeguatamente formato alfine di possedere tutti i requisiti di professionalità e conoscenza esperienza richiesti dalla specifica natura delle funzioni richieste.

5.3 Organizzazione del Servizio di Prevenzione e Protezione

Sono presenti disposizioni organizzative emanate ed approvate dagli organi societari delegati che disciplinano ruoli, responsabilità e modalità di gestione del servizio di prevenzione e protezione all'interno dell'organizzazione,in coerenza con le disposizioni di legge vigenti in materia.

ln particolare devono essere rispettati:

- i requisiti e gli skill specifici del Responsabile del servizio di prevenzione e protezione;

- le competenze minime, il numero, i compiti e le responsabilità dei lavoratori addetti ad attuare le misure diemergenza, prevenzione incendi e primo soccorso;
- il processo di nomina e la relativa accettazione da parte del Medico Competente.

6. Attivita' di monitoraggio e verifica

Viene garantito il monitoraggio sistematico e continuo dei dati/indicatori che rappresentano la misura dell'efficacia e efficienza aziendale nella gestione della sicurezza e nella prevenzione.

A tale proposito sono individuati specifici indicatori di performance relativamente alle attività di gestione del Sistema di Prevenzione e Protezione.

Tali dati sono raccolti annualmente dal Datore di lavoro in collaborazione con il RSPP, presentati in occasione del−la Riunione Periodica e del Riesame della Direzione ai rappresentanti dei lavoratori per la sicurezza e trasmessi all'Organismo di Vigilanza.

ll Datore di Lavoro procede anche ad un'analisi sistematica di tali dati per la individuazione di eventuali azioni preventive o correttive.

Periodicamente il Datore di lavoro effettua, unitamente al RSPP, una verifica sistematica relativamente a:

- lo stato di attuazione delle misure adottate atte a mitigare il rischio per la salute e sicurezza dei lavoratori della loro efficacia
- la conformità alle prescrizioni legali

I risultati di tale verifica sono trasmessi all'Organismo di Vigilanza.

ll Sistema di monitoraggio e verifica è assicurato dalla procedura PO 17 "Audit interni", la quale definisce le attività e le responsabilità relative alla conduzione delle attività di audit, per assicurare che lo svolgimento degli stessi avvenga in modo programmato, pianificato e documentato, allo scopo di valutare se gli elementi del Sistema di Gestione siano attuati e risultino idonei a conseguire gli obbiettivi di prefissati.

La procedura si applica alle verifiche ispettive condotte dal Responsabile del Sistema di Gestione o da persone da lui demandate, dal RSPP e dal Medico Competente, presso tutte le funzioni aziendali e presso organizzazioni esterne (cantieri clienti), influenti sulla qualità e sulla sicurezza dei servizi prestati. inoltre, a livello operativo, è stata elaborata la procedura PO 10 "Gestione dei controlli", la quale definisce le modalità di controllo delle attività di processo interne (controllo in produzione).

Tali attività sono effettuate dal RSPP. Rientrano nelle attività di verifica ispettiva: sopralluoghi/controlli documentati da parte del RSPP, sopralluoghi documentati del medico competente, verifiche documentate sulla conformità legislativa al D.Lgs. 81/08 e s.m.i., verifiche documentate sulla conformità al Sistema 18001:2007. Queste ultime due verifiche sono svolte una volta all'anno dal personale incaricato dal Datore di Lavoro e dall'Ente di Certificazione.

7. I flussi informativi

La Società ha definito apposite modalità al fine di assicurare una corretta gestione delle comunicazioni attinenti lasicurezza, sia quelle provenienti e dirette all'esterno sia quelle interne tra i differenti livelli e settori dell'azienda.

I flussi informativi sono gestiti dall'azienda tramite la procedura PO 15 – Comunicazione, partecipazione ed consultazione.

Tale procedura definisce le modalità operative e le Responsabilità per:

- divulgare alle parti interessate le informazioni relative ai servizi erogati e rilevanti sui rischi connessi alle attività aziendali;
- raccogliere, registrare e rispondere alle segnalazioni delle parti interessate (Clienti, fornitori, ecc..) riguardanti le problematiche sull'erogazione del servizio e relative alla salute e sicurezza;
- assicurare la partecipazione e consultazione del personale aziendale in materia di salute e sicurezzasul lavoro e nei casi di gestione di anomalie e/o situazioni di emergenza rilevate durante il servizio.

Si applica a tutte le comunicazioni interne ed esterne riguardanti:

- salute e sicurezza da e verso le parti interessate;
- la gestione dei rapporti con il Cliente in termini di comunicazioni relative ai servizi erogati;
- comunicazioni rivolte o provenienti dall'esterno (possibili portatori di interesse quali Enti Locali, Organi di Controllo, clienti, fornitori, ecc).

7.1 Comunicazioni esterne

L'azienda ha adottato un sistema per gestire le comunicazioni relative alla sicurezza e all'igiene del lavoro provenienti dall'esterno, attraverso la definizione delle responsabilità e delle modalità di ricevimento, registrazione e dirisposta a tali comunicazioni.

ll processo di gestione delle comunicazioni ricevute dall'esterno (dal pubblico, dalle istituzioni, dagli organismi di controllo, etc.) è definito in modo tale da:

- garantire che le comunicazioni siano inoltrate alle funzioni responsabili dì definire le eventuali azioni conseguenti
- registrare le decisioni prese, attuare le eventuali azioni e verificarle
- archiviare le registrazioni che documentino l'intero processo.

Ogni soggetto che riceve una comunicazione dall'esterno in materia di sicurezza e igiene del lavoro deve comunicarla al RSPP, il quale provvede ad una prima valutazione e, sulla base della criticità, decide se coinvolgere o menoi soggetti delegati per l'attuazione delle azioni necessarie.

Tutte le comunicazioni giunte e la documentazione delle relative azioni intraprese sono archiviate da RSPP in un apposito raccoglitore.

7.2 Comunicazioni interne

La Società ha definito un sistema di comunicazioni interne che assicura che le informazioni relative alla sicurezza fluiscano "dall'alto verso il basso", ma anche "dal basso verso l'alto" ed orizzontalmente rispetto alle varie parti dell'organizzazione.

Lo scambio di informazioni tra i differenti livelli e settori aziendali è attuato attraverso l'individuazione di referentiinterni e di idonei strumenti di comunicazione.

Gli strumenti di comunicazione interna possono variare in funzione del tipo di informazione che è necessario fornire avendo però sempre presente che il requisito indispensabile è che le informazioni siano fornite usando una forma ed un modo che le rendano comprensibili alle persone che le devono ricevere.

Rientrano tra le comunicazioni interne tutte le segnalazioni che provengono dal personale in materia di salute e sicurezza al RSPP o al Capo Servizio, nello svolgimento quotidiano del loro lavoro. Tali segnalazioni vengono gesti−te come descritto in PO 15.

7.3 Coinvolgimento del personale

La Società è convinta che il processo di prevenzione e miglioramento della sicurezza debba vedere coinvolto tutto il personale aziendale.

A tale fine ogni lavoratore è incoraggiato a segnalare al proprio responsabile di funzione o direttamente al RSPPeventuali anomalie o proposte di miglioramento.

Tali segnalazioni sono raccolte dal RSPP che provvede ad effettuarne un'analisi ed è responsabile di mettere in at−to le eventuali azioni conseguenti; la decisione presa in merito è registrata da RSPP.

ll RSPP organizza anche le riunioni periodiche sulla sicurezza prevista dalle norme vigenti e redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione.

7.4 Comunicazioni con l'Organismo di Vigilanza (OdV)

ll Datore di lavoro, sentito il RSPP, deve inviare all'Organismo di Vigilanza un report informativo, con cadenza trimestrale, comprendente almeno:

- descrizione degli incidenti/infortuni eventualmente occorsi
- risultati delle attività di monitoraggio e verifica effettuate
- stato di attuazione del programma di miglioramento
- segnalazioni ricevute
- risultati di eventuali accertamenti degli organismi di controllo

ln caso di infortuni che abbiano causato (o avrebbero potuto causare) lesioni gravi il RSPP avverte tempestivamente l'Organismo di Vigilanza.

8. Regolamentazione delle singole attivita' sensibili

8.1 Valutazione dei rischi e programma di miglioramento

Relativamente all'attività sensibile di "Valutazione dei rischi e definizione e gestione degli interventi di migliora− mento", è stata definita una procedura che disciplina l'attività di aggiornamento della valutazione dei rischi (PO 16 "lndividuazione e gestione dei rischi" e di definizione delle modalità con le quali l'organizzazione individua e gestisce gli obiettivi di miglioramento in materia di sicurezza (PO 01 "Riesame della Direzione"), coerentemente con quanto stabilito nel codice etico aziendale.

Le procedure si applicano a tutte le misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza individuate da ciascun livello e funzione dell'organizzazione e verificare

il raggiungimento degli obiettivi stabiliti e che l'intero sistema risulti sempre appropriato, adeguato ed efficace.

Mediante il "Programma annuale di miglioramento" (MO 10.3), l'azienda si pone degli obiettivi di miglioramento sulla salute e sicurezza, predisponendo un bilancio previsionale che prevede la destinazione di risorse per l'attuazione del programma stesso, individuando i responsabili dell'attuazione degli obiettivi e le modalità, non− ché le tempistiche di sorveglianza sullo stato di avanzamento.

8.2 Aggiornamento normativo e verifica di conformità legislativa

Relativamente all'attività sensibile di "Aggiornamento normativo e verifica di conformità normativa", è stata definita una procedura che disciplina l'attività di accesso, identificazione, valutazione e applicazione delle prescrizioni legali in materia di sicurezza e di acquisizione e conservazione di tutta la documentazione e le certificazioni obbligatorie per legge (PO 02 "Gestione dei documenti e registrazioni").

La procedura ha lo scopo di garantire la corretta gestione (accesso, identificazione, valutazione e applicazione) delle prescrizioni legali stabilite a livello nazionale e locale, nonché delle eventuali prescrizioni di altro tipo eventualmente sottoscritte dall'azienda. Ciò al fine di garantire il recepimento da parte dell'organizzazione e la conoscenza da parte delle funzioni interessate delle prescrizioni applicabili.

La procedura definisce modalità e responsabilità in merito a:

- la raccolta, gestione, aggiornamento ed archiviazione delle prescrizioni legali riferite all'azienda;
- l'identificazione delle disposizioni normative che disciplinano gli aspetti di sicurezza che hanno origine dalle attività di Mondialpol S.R.L.;
- l'accesso alle disposizioni normative e alla loro archiviazione;
- la gestione degli adempimenti richiesti e di verifica della conformità legislativa;
- garantire l'aggiornamento sulle novità in materia di legislazione sicurezza;
- permessi licenze o altre forme di autorizzazione;
- accordi contrattuali;
- comunicazione delle azioni conseguenti alle funzioni interessate;

La procedura gestisce, oltre a quanto sopra descritto, i documenti di origine interna e esterna relativi alla Salute e sicurezza sul lavoro.

La responsabilità di tale attività è affidata al RSPP, il quale gestisce:

- la documentazione relativa agli appalti in essere con la clientela presso cui si svolge attività continuativa di piantonamento fisso. Nel registro si gestisce l'elenco dei documenti e l'aggiornamento della documentazione in possesso di Mondialpol S.R.L. e del committente stesso.
- i documenti di origine interna relativi alle valutazioni dei rischi e alla documentazione ad esse allegata. Nel registro si gestisce l'elenco dei documenti presenti ed elaborati in Mondialpol Security con le revisioni e le relative scadenze.

8.3 Gestione delle Emergenze

Relativamente all'attività sensibile di gestione delle emergenze, al fine di garantire l'individuazione delle potenziali emergenze, l'efficace coordinamento in fase di risposta a eventuali incidenti e situazioni di emergenza e la capacità di prevenire o attenuare le conseguenze degli eventi incidentali, è stata definita una procedura (PO 20 "Gestione emergenze") che disciplina le attività di:

- definizione delle responsabilità e modalità per l'individuazione delle emergenze;
- definizione, redazione, riesame, approvazione e simulazione periodica del "Piano di emergenza interno";
- formazione e addestramento alle emergenze;
- manutenzione e verifica dei presidi e delle dotazioni per le emergenze.

La procedura si applica a tutte le situazioni di emergenza e ai potenziali incidenti derivanti dalle attività dell'azienda che possano determinare un rischio per la sicurezza e salute dei lavoratori e dei visitatori: ditte appaltatrici e/o personale esterno.

8.3 Sorveglianza Sanitaria

Relativamente all'attività sensibile di sorveglianza sanitaria, al fine di assicurare la sorveglianza sanitaria dei propri dipendenti, secondo quanto previsto dalla normativa vigente è stata definita una procedura (PO 21 "Sorveglianza sanitaria"). Scopo della procedura è stabilire le responsabilità e le

modalità operative per lo svolgimento della sorveglianza sanitaria, ove necessaria, cui sottoporre i lavoratori facente parte dell'Organizzazione.

L'obiettivo è altresì quello di definire una corretta pianificazione e attuazione della sorveglianza sanitaria, ai sensi della normativa vigente in materia di salute e sicurezza negli ambienti di lavoro.

La presente procedura è applicabile a tutti i lavoratori di Mondialpol S.R.L. secondo "Protocollo sanitario" del medico competente.

Tale procedura disciplina le attività di:

- definizione del protocollo sanitario;
- attuazione degli accertamenti sanitari;
- attivazione o modifica del protocollo sanitario in caso di nuovi assunti e cambi mansione;
- nomina e definizione dei compiti del Medico Competente.

8.4 Formazione, Informazione e Addestramento

Relativamente all'attività sensibile di "Formazione e informazione", è stata definita una procedura per regolamentare le attività di formazione, informazione e addestramento da erogare al personale dipendente e neoassunto o in fase di assunzione o in occasione del cambio di mansione.

La procedura PO 18 "Gestione informazione, formazione e addestramento" ha lo scopo di regolamentare le attività di informazione, formazione e addestramento del personale di Mondialpol S.R.L. al fine di garantirne la qualificazione personale, la consapevolezza del ruolo aziendale e la sensibilizzazione, in considerazione di tutti gli aspetti di salute e sicurezza nei luoghi di lavoro in accordo con quanto prescritto dalle leggi nazionali e comunitarie vigenti.

l contenuti della procedura specificano modalità e responsabilità in merito a:

- l'individuazione delle necessità di informazione, formazione e addestramento;
- la pianificazione e attuazione della formazione;
- la registrazione delle attività formative;
- la verifica della loro efficacia;
- l'informazione e sensibilizzazione del personale sull'igiene e la sicurezza del lavoro

8.5 Gestione degli infortuni

E' stata definita una procedura per regolamentare la raccolta e l'analisi dei dati in occasione di infortuni occorsi all'interno dell'azienda al fine di garantire la tracciabilità degli incidenti, e delle situazioni potenzialmente danno− se, l'attività di rilevazione e registrazione degli stessi e la loro investigazione.

La procedura Po 12 "Gestione delle non conformità" ha lo scopo di definire le modalità con cui Mondialpol S.R.L. gestisce le non conformità ed i reclami provenienti dalle parti interessate sia interne sia esterne in campo sicurezza, individuando le responsabilità e le modalità di gestione delle azioni correttive, ritenute necessarie al fine di eliminare non conformità riscontrate che presentano caratteristiche di ripetitività e delle azioni preventive volte alla minimizzazione dei rischi di insorgenza di non conformità non ancora manifestate.

Tale procedura, inoltre, prevede la definizione di responsabilità e modalità operative per la:

- registrazione incidenti, dei near miss e degli infortuni;
- individuazione delle possibili cause;
- la definizione di eventuali azioni migliorative per evitarne il ripetersi.

8.6 Rapporto con i fornitori

Relativamente all'attività sensibile di gestione dei contratti di appalto e opera, è stata regolamentata, all'interno di un apposita procedura PO 22 "Gestione dei lavori in appalto", la gestione delle attività in appalto o d'opera, definendo, per ogni figura responsabile, i compiti e le attività da mettere in atto per la tutela della sicurezza e della salute di tutto il personale interessato, durante gli interventi eseguiti da imprese appaltatrici o lavoratori autonomi all'interno dell'azienda, in conformità a quanto disposto dalla normativa vigente.

La procedura viene applicata nel caso di lavori in appalto o contratti d'opera effettuati all'interno dell'azienda da ditte appaltatrici, cooperative, lavoratori autonomi.

L'azienda nella gestione del rapporto con i fornitori definisce modalità e responsabilità per:

- qualificare i fornitori in relazione ai loro requisiti tecnico−professionali (mediante la PO 05 "Gestione acquistie qualificazione dei fornitori";
- valutare i rischi derivanti dalle interferenze;
- fornire le informazioni sui rischi e le misure di prevenzione ed emergenza;

- definire trasmettere le norme di comportamento;
- vigilare sull'operato dei fornitori.

8.7 Acquisto impianti, macchine e attrezzature

Per garantire una corretta gestione dell'attività sensibile di "Acquisto di impianti macchine e attrezzature" è stata definita una procedura che stabilisce le modalità operative per l'acquisto di macchine, impianti e componenti di sicurezza utilizzate in azienda per quanto riguarda gli aspetti di sicurezza e igiene del lavoro (PO 05 "Gestione acquisti e qualificazione fornitori").

La procedura prevede la definizione di responsabilità e modalità operative per il corretto adempimento delle prescrizioni previste dalla legislazione vigente in materia di salute e sicurezza, nei rapporti con le imprese appaltatricio lavoratori autonomi.

La procedura si applica a tutti i fornitori dei prodotti e servizi, sotto elencati, ritenuti influenti sulla qualità e sulla sicurezza aziendale.

- Apparecchiature di sorveglianza;
- Automezzi e relativi allestimenti;
- Apparecchiature di comunicazione;
- Apparecchiature e dotazioni di servizio;
- Apparecchiature di comunicazione;
- Divise e DPl delle Guardie;
- Carburanti e lubrificanti per gli automezzi di servizio;
- Manutenzione di automezzi, apparecchiature e dotazioni di sicurezza;
- Manodopera per l'installazione di apparecchiature di sorveglianza;
- Consulenza sulla salute e sicurezza;
- Sorveglianza sanitaria;
- Dotazioni di sicurezza (estintori, luci emergenza, cassetta di primo soccorso, ecc..).

8.9 Modifica di strutture, impianti e processi

Per questo processo "sensibile" è stata definita una procedura per garantire la valutazione preliminare delle modifiche ad attività, macchine, impianti, layout e strutture, al fine di assicurare che queste modifiche non aumenti−no i rischi.

La procedura PO 23 "Gestione modifiche" ha lo scopo di garantire che le esigenze poste dalla politica in materia di salute e sicurezza e dalle leggi e regolamenti applicabili siano considerate all'atto della progettazione di nuove strutture, nuovi impianti e nuovi processi, introduzione di nuove sostanze o preparati, nuove mansioni, al fine di effettuare preliminarmente una valutazione degli aspetti di salute e sicurezza connessi e di minimizzare gli eventuali impatti negativi sui pericoli e rischi per la S&SL.

La presente procedura si applica alla fase di introduzione in Mondialpol S.R.L. di nuove strutture, nuovi impianti e nuovi processi o nuove mansioni che potrebbero portare a qualsiasi cambiamento aventi effetti o impatti sui suoi pericoli e sui rischi per la salute e sicurezza dei lavoratori, analizzando i pericoli ed i rischi potenziali.

8.8 Manutenzioni

L'azienda ha definite modalità e responsabilità del processo di manutenzione, attraverso il quale garantisce che le proprie macchine, attrezzature e impianti siano mantenuti nelle originarie condizioni di efficienza e di sicurezza, così come per prevenire l'insorgenza di condizioni che possano creare un incremento delle condizioni di rischio.

Tale procedura PO 09 "Controllo del servizio" si applica alle manutenzioni delle macchine ed attrezzature, degli impianti (compresi quelli per la prevenzione e protezione), dei mezzi aziendali e dei locali e infrastrutture.

Vengono specificate le modalità relative a:

- esecuzione e registrazione delle verifiche periodiche su attrezzature e impianti che possono generare incidenti;
- esecuzione e registrazione delle verifiche periodiche sui presidi di prevenzione e protezione.

8.9 Verifica dei luoghi di lavoro

Con riferimento all'attività sensibile di "Controllo e verifica dei luoghi di lavoro", sono state formalizzate le responsabilità specifiche di ciascuna figura preposta alla quale si delega l'attività di sorveglianza dei luoghi di lavoro e/o delle attrezzature e definite le modalità di comunicazione di

eventuali anomalie i destinatari di queste e le responsabilità per la definizione e l'attuazione delle misure correttive.

8.10 Gestione dei Dispositivi di Protezione Individuale

Per garantire una corretta gestione dell'attività sensibile di acquisto e gestione dei DPl è stata definita la procedura PO 19 "Gestione dei DPl aziendali"

La procedura stabilisce le responsabilità e le modalità operative per l'identificazione e gestione dei dispositivi di protezione individuale ed assicurare che ogni lavoratore abbia a disposizione i DPl previsti, sulla base della valuta−zione dei rischi e delle mansioni svolte.

ln essa sono indicate le responsabilità e modalità operative per:

- scelta dei DPl;
- distribuzione e manutenzione dei DPl;
- informazione sull'utilizzo;
- vigilanza sull'utilizzo da parte dei lavoratori.

9. Procedure di riferimento

Al fine di evitare la proliferazione di procedure specifiche si è deciso di adottare nel modello le procedure già in uso descritte dai seguenti strumenti aziendali, che qui si intendono tutti richiamati e compresi:

- Manuale della qualità in conformità alla Norma Europea UNI EN ISO 9001:2015 "Sistemi di Gestione per la qualità – Requisiti", ed in conformità alla Norma Nazionale UNI 10891:2000 "Istituti di Vigilanza Privata- Requisiti";
- Il Regolamento interno sulle modalità di esecuzione dei servizi offerti dall'Istituto di vigilanza privata "Mondialpol S.R.L." approvato dalla Questura di Palermo;
- Il Documento di Valutazione dei Rischi (DVR) ai sensi dell'art.28 comma 2 D.Lgs. 81/08 e s.m.i.;
- Manuale della Centrale Operativa redatto in conformità alla Norma Italiana UNI CEI EN 50518:2020 "Centro di monitoraggio e di ricezione di allarme";
- Il Funzionigramma approvato del 2 febbraio 2023;
- Il Manuele delle procedure aziendali "MPA" del 3 settembre 2021.

Dalla su riportata documentazione sono state analizzate e richiamate nel presente modello le seguenti procedure così classificate in un quadro sinottico:

MODELLO ORGANIZZATIVO E DI GESTIONE 231 PARTE SPECIALE	MANUALE DELLE PROCEDURE	MANUALE DELLA CENTRALE OPERATIVA	REGOLAMENTO INTERNO	DVR
PO 01 Riesame della Direzione	*PIANIFICAZIONE*		SI	Analisi autorizzativa e documentale
PO 02 Gestione dei documenti e	*GESTIONE DELLA DOCUMENTAZIONE*	• *Gestione dei Dati .*		
PO03 Gestione delle offerte e dei contratti	*ACQUISIZIONE CLIENTE / COMMITTENTE*			
PO 05 Gestione acquisti e Qualificazione dei fornitori	*SELEZIONE VALUTAZIONE E APPROVVIGIONAMENTO DA FORNITORI*	• *Gestione fornitori*		
PO 09 Controllo del servizio	*PIANIFICAZIONE E PROGETTAZIONE DEL SERVIZIO - SERVIZI DI VIGILANZA FISSA, ISPETTIVA, ANTIRAPINA - SERVIZI FIDUCIARI (PORTIERATO) - SERVIZIO DI SICUREZZA SUSSIDIARIA - TRASPORTO VALORI E SCORTE*	• *Gestione del Data Base ;* • *Entrata ed uscita dall'ARC (Gestione e controllo degli accessi ai locali della C.O.);*	SI	
PO 10 Gestione dei controlli	*RADIOALLARME, TELEALLARME, VIDEOSORVEGLIANZA E PRONTO INTERVENTO H24*	• *Gestione dei segnali ;*	SI	Metodologie seguite per la valutazione
PO 12 Gestione delle non conformità	*GESTIONE NON CONFORMITA'*	• *Test sulle apparecchiature tecniche dell'ARC ;*		
PO 15 Comunicazione, partecipazione e consultazione	ANALISI DEI DATI E CUSTOMER SATISFACTION - GESTIONE RECLAMI CLIENTE	• *Gestione dei Reclami ;*		
PO 16 Individuazione gestione dei rischi			SI	Valutazione dei rischi
PO 17 Audit Interni	*VERIFICHE ISPETTIVE INTERNE*			
PO 18 Gestione Informazione formazione addestramento	*GESTIONE DELLE RISORSE UMANE*			Informazione, formazione ed addestramento
PO 19 Gestione dei DPI aziendali			SI	
PO 20 Gestione Emergenze	*GESTIONE DELLE REGISTRAZIONI*	• *Procedure di Evacuazione ;* • *Continuità operativa e Gestione delle Emergenze ;*	SI	
PO 21 Sorveglianza sanitaria				Organizzazione della sicurezza
PO 22 Gestione dei lavori in appalto	*SELEZIONE VALUTAZIONE E APPROVVIGIONAMENTO DA FORNITORI*	• *Gestione fornitori*		
PO 23 Gestione Modifiche	*GESTIONE DELLE AZIONI CORRETTIVE -* GESTIONE DELLE AZIONI PREVENTIVE			Programmadi attuazione degli interventi

Parte Speciale 5: I Reati Ambientali

Le origini comunitarie della tutela penale dell'ambiente

L'Unione europea ha dato da sempre una spinta determinante al processo di costruzione del diritto penale dell'ambiente. La consapevolezza che l'inquinamento costituisce un fenomeno globale, infatti, ha imposto l'adozione di provvedimenti di carattere sovranazionale.

Già nel 1998 il Consiglio d'Europa, decise di adottare una Convenzione per la tutela dell'ambiente attraverso il diritto penale (mai entrata in vigore per il ridotto numero di ratifiche), che rappresenta tuttavia il primo strumento internazionale che ha previsto la criminalizzazione da parte degli Stati membri dell'UE di una serie di condotte produttive di danno o pericolo per l'ambiente. Invero, scopo ultimo della Convenzione era imporre agli Stati l'introduzione nei codici penali di fattispecie di reato di pericolo, anticipando, così, la soglia di tutela del bene, nonché la predisposizione di una responsabilità a titolo di colpa, quanto meno in riferimento ai casi di colpa grave.

Nel 2001 la Commissione europea, visto il tentativo mal riuscito nel 1998,predispose un testo per una direttiva in materia, mentre il Consiglio dei Ministri dell'Unione europea il 27 gennaio 2003 assunse la decisione quadro 2003/80/GAI, nota per esser stata oggetto di ricorso da parte della Commissione europea per un conflitto di competenza istituzionale, risolto dalla sentenza della Corte di Giustizia del 13 settembre 2005, Causa C-176/03, nella quale i giudici europei confermarono che una decisione in materia di protezione dell'ambiente mediante il diritto penale avrebbe dovuto avere come fondamento giuridico il trattato CE e non il trattato sull'Unione europea (trattato UE).

Va ricordato inoltre che la Commissione Europea ha emanato la Direttiva 2004/35/CE con la quale ha inteso fornire un contributo determinante nella costruzione di un sistema normativo condiviso in tema di responsabilità per danni all'ambiente, pur senza introdurre fattispecie penali, ma prescrivendo obblighi e responsabilità a carico degli operatori economici in caso di causazione di danni.Ma l'atto decisamente più significativo è rappresentato dalla Direttiva 2008/99/CEsulla tutela penale dell'ambiente del 19 novembre 2008.

Per le attività svolte dalla MONDIALPOL tale fattispecie di reato rappresenta un rischio irrilevante.

Parte Speciale 6: I Delitti Informatici e il Trattamento illecito dei dati

Considerazioni generali

La Legge n. 48/2008 ha integrato nuovamente l'area dei reati presupposto in presenza dei quali scatta la responsabilità degli enti: all'art. 24-bis, figurano alcuni dei comportamenti che rappresentano minacce alla sicurezza informatica e che,nel nostro ordinamento, sono qualificati come condotte penalmente rilevanti.

La sicurezza informatica si interfaccia con la tutela dei dati personali al punto che,lo stesso Codice Privacy (D.lgs. n.196/03), in tema di tutela dei dati personali, stabilisce obblighi specifici e generali che si sostanziano nella necessità, da parte del titolare del trattamento dei dati, di implementare una serie di misure minime di sicurezza identificate direttamente dalla normativa, oltreché misure idonee e preventive da identificare in base ad un'accurata analisi dei rischi.

Le misure minime di sicurezza, di cui all'Allegato B al Codice Privacy, stabiliscono il livello minimo di protezione dei dati e la loro adozione è conditio sine qua non per lo svolgimento delle attività di trattamento dei dati.

All'interno dell'azienda, i rischi correlati al crimine informatico sono di grande rilevanza; si pensi che la maggior parte dei processi aziendali sono informatizzati e per di più esternalizzati; l'assistenza tecnica od i servizi di cloud computing ne sono un chiaro esempio.

A questo proposito, il d.lgs. 231 prevede che tra l'autore materiale del reato e l'ente non debba intercorrere necessariamente un rapporto di lavoro subordinato,rilevando la subordinazione alla direzione o vigilanza di uno dei soggetti in posizione apicale, la quale è rinvenibile anche nei rapporti con i collaboratori esterni/consulenti.

Questi ultimi devono essere nominati responsabili del trattamento, come nel caso dell'amministratore di sistema in outsourcing, del fornitore di servizi cloud o del manutentore del sito web aziendale e come tali devono attenersi, secondo quantoprescritto dallo stesso Codice Privacy all'art. 29, alle istruzioni loro fornite dal titolare. È rinvenibile in tali rapporti quel vincolo di subordinazione alla vigilanza e direzione dei soggetti apicali, richiesto dall'art. 5 del D.lgs. 231, per l'insorgeredella responsabilità amministrativa dell'ente.

In particolare, le aziende devono valutare ex ante l'affidabilità di tali consulenti/fornitori nonché prevedere, nei contratti conclusi con gli stessi, un'apposita clausola che regoli le conseguenze delle violazioni alle norme del D.lgs. 231/01.

La prevenzione dei reati informatici, al fine di evitare di incorrere nella citata responsabilità, passa attraverso la predisposizione di misure di sicurezza fisica, logica ed organizzativa. La sensibilizzazione della dirigenza e dei dipendenti, la loro formazione, le azioni di monitoraggio ed audit sono solo alcuni dei punti chiave per assicurare l'azienda dalle gravi ripercussioni previste dal D.lgs.231/01.
Per difendersi l'azienda ha vari strumenti che riducono il rischio di commissione di reati ed illeciti, i più efficaci dei quali sono l'adozione di un valido ed efficace modello di organizzazione e gestione e di una privacy policy.
Il rispetto della normativa privacy, prevedendo l'applicazione di misure minime di sicurezza, consente appunto di prevenire la commissione dei reati presupposti previsti dal D.lgs. 231/01; le policy ed i modelli organizzativi sono efficaci ed assumono valore esimente, solamente se concretamente attuati e se portati a conoscenza di dipendenti e stakeholder.

L'art. 24 bis D.lgs. 231/2001 - Delitti informatici e trattamento illecito di dati

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

Il significato dell'art. 24 bis: fattispecie e conseguenze

LA CONDOTTA TIPICA

L'accesso abusivo punisce la condotta di chi si introduce abusivamente – ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'accesso – inun sistema informatico o telematico, protetto da misure di sicurezza, rimanendovicontro la volontà di chi ha diritto di escluderlo.

Due sono pertanto le condotte penalmente rilevanti: l'intrusione in un sistema protetto ed il mantenimento nello stesso contro la volontà espressa o tacita di chiha il diritto di esclusione. Di conseguenza si parla di accesso abusivo sia nel casoin cui il soggetto, pur legittimato all'utilizzo del sistema, entri in ambienti informatici a cui non è autorizzato ad accedere, sia nel caso in cui lo stesso, puressendo abilitato, acceda o si mantenga nel sistema violando le condizioni ed i limiti fissati dal titolare per delimitarne oggettivamente l'accesso, restando invecedel tutto irrilevanti le finalità che hanno mosso l'agente.

Perché il reato si configuri il sistema deve essere protetto da misure di sicurezza.Occorre dunque dimostrare che siano stati adottati dei meccanismi di selezione dei soggetti abilitati all'accesso del sistema informatico che possono essere di tipo logico (es. firewall, password, codici d'accesso, dati biometrici), fisico (es. sistemi di videosorveglianza, porte blindate) od organizzativo (es. accesso ai locali vietato al personale impiegatizio). E' sufficiente che il soggetto agisca con la coscienza e la volontà di introdursi nell'altrui sistema protetto ovvero di rimanervi contro la volontà di chi ha diritto diescluderlo, mentre non rilevano in alcun modo le finalità (curiosità, ricerca di informazioni riservate, intento vandalico o manipolativo) per cui il soggetto agisce. Oggetto di tutela è il "domicilio informatico" quale spazio fisico e ideale, estensione della sfera di riservatezza della persona (sia fisica che giuridica).

SOGGETTO AGENTE

E' un reato che può essere compiuto da chiunque abbia accesso al sistema, percui può essere realizzato tanto dall'utente generico quanto dall'amministratore disistema (magari in outsourcing). Dal momento che non esistono delle aree o funzioni maggiormente a rischio si rileva la necessità di una vigilanza "trasversale".

IL PRESUPPOSTO 231

Posto che ai sensi del d.lgs.231/01 il reato deve essere commesso "nell'interesse o vantaggio" dell'azienda per fondare una responsabilità della stessa, si avrà accesso abusivo, rilevante in chiave 231, a titolo esemplificativo, allorquando il soggetto (apicale o sottoposto) acceda abusivamente al sistema di un'azienda concorrente al fine di conoscerne il portafoglio clienti o per acquisire, a scopo di spionaggio industriale, la documentazione relativa ai suoi prodotti. Si avrà altresì accesso abusivo anche quando il soggetto acceda abusivamente ai propri sistemi informatici, ad esempio per manipolarne i dati al fine di ottenere un vantaggio in ordine agli adempimenti contabili e di bilancio. Come in generale, costituiscono attività "sensibili" (i.e. a rischio di commissione di reato) tutti gli accessi ai sistemi informatici/telematici.

LA PREVENZIONE DEL MODELLO ORGANIZZATIVO

Tra i protocolli da adottare per prevenire la commissione di questa tipologia di reato, fondamentale è il ricorso ad adeguate policies (supportate da corrispondenti procedure) che andranno a disciplinare la gestione degli account e dei profili di autorizzazione, la gestione della rete aziendale e di internet nonché l'utilizzo della posta elettronica.

LE SANZIONI

La sanzione prevista è quella pecuniaria da cento a cinquecento quote (in grado dunque di arrivare sino ad € 774.500) nonché, laddove ricorrano le condizioni di cui agli artt. 9, 12 e 13, d.lgs. 231/01, le sanzioni interdittive dell'interdizione dall'esercizio dell'attività, della sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito e del divieto di pubblicizzare beni o servizi.

I reati presupposto

Art. 615-ter c.p. - Accesso abusivo ad un sistema informatico o telematico.

«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico,la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni».

L'oggetto giuridico tutelato dalla norma è, secondo la teoria predominante, il "domicilio informatico".

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo,attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Cass. 3067/1999).

Il sistema informatico, dovendo svolgere una funzione - mediante tecnologie informatiche - è dunque tale se gestisce o elabora dati, mentre tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare datiin vista dello svolgimento di una funzione non è "sistema informatico".

La mera copiatura dei contenuti di un sito, realizzata semplicemente dallavisualizzazione del sito senza introduzione nella "memoria interna" del sito o neiprogrammi che ne consentono il funzionamento, non concreta interazioni con il sistema informatico come definito dalla

giurisprudenza; peraltro, si segnala che la norma in questione è stata introdotta al fine di reprimere il fenomeno degli hacker, cosa ben diversa dalla consultazione / visualizzazione / copiatura del contenuto di una pagina web.

Dirimente ai fini della configurabilità del reato è la presenza o meno delle cd. misure di sicurezza nel sistema informatico / telematico.

Sono tali quelle protezioni (che possono essere apposte sia a livello di apparecchiature (hardware) che di programmi (software) che integrano quei peculiari meccanismi operativi che impediscono un libero accesso al sistema e, quindi, la presa di cognizione di informazioni e dati ivi rinvenibili) a terzi estranei(ad esempio, codice alfanumerico di accesso, chiave di avviamento, eccetera.

L'apposizione di siffatte misure protettive del sistema informatico o telematico costituisce, infatti, l'estrinsecazione della voluntas excludendi manifestata dal titolare del relativo ius.

L'accesso ad un sistema non protetto, pertanto, risulta atipico e penalmente lecito ma non anche civilisticamente, dovendosi, a tale riguardo, ulteriormente verificare in concreto un danno ingiusto risarcibile ex articolo 2043 CC.

La Corte di Cassazione ha aderito all'orientamento interpretativo estensivodell'art. 615-ter parte seconda e stabilito la configurabilità del reato "nel caso in cui il soggetto legittimato all'accesso per motivi di servizio o di ufficio s'introduca per motivi diversi".

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

«Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunquerivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, ilcontenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni seil fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

- da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso deipoteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi esercita anche abusivamente la professione di investigatore privato».

Tale norma mira a impedire l'intercettazione fraudolenta, ravvisabile ogniqualvolta l'agente prenda conoscenza delle comunicazioni in maniera occulta e senza essere legittimato.

La Cassazione ha statuito che integra la violazione di cui all'art. 617-quater, comma 2 c.p., la condotta di chi diffonda al pubblico una trasmissione televisivainterna, trasmessa da punto a punto (cd "fuori onda") su un canale riservato a comunicazioni di servizio e intercettata in modo fraudolento. Il caso si riferiva a Striscia la notizia che aveva "intercettato" dei fuori onda e poi trasmessi nel corsodella propria trasmissione.

Art. 617-quinquies c.p. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche.

«Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater».

Tale norma è volta a sanzionare la semplice predisposizione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Va segnalata una pronuncia del GIP presso il Tribunale di Milano secondo cui integra il reato di cui all'art. 617- quinquies c.p. e non il reato di cui all'art. 615- quater c.p. la condotta di chi installa su uno sportello bancomat, in sostituzione del pannello originario, una apparecchiatura composta da una superficie plastificata, con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat, quando non vi sia prova certa dell'avvenuta captazione di almeno un codice identificativo.

L'attività illecita d'intercettazione, infatti, nel silenzio dell'art. 617- quinquies c.p.,deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico qual è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso

ad un sistema attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione.

Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici.

«Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora,cancella, altera o sopprime informazioni, dati o programmi informatici altrui èpunito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635ovvero se il fatto è commesso con abuso della qualità di operatore del sistema,la pena è della reclusione da uno a quattro anni e si procede d'ufficio».

Art. 635 c.p. - Danneggiamento

"Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a un anno o con la multa fino a lire seicentomila. La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso con violenza alla persona o con minaccia; (omissis) L'art. 635-bis non si limita ad ampliare ed integrare la norma sul danneggiamento(art. 635 c.p.), con riguardo ai dati ed ai programmi, ossia alle componenti immateriali di un sistema informatico, ma predispone altresì una tutela rafforzata di tutti i beni informatici, prevedendo un trattamento più rigoroso, sia sotto il profilosanzionatorio che sotto il profilo della procedibilità, anche di fatti che erano pacificamente riconducibili alla fattispecie tradizionale, in quanto aventi ad oggetto cose materiali: il sistema informatico o telematico, ovvero il supporto materiale delle informazioni.

Oggetto di danneggiamento può essere innanzitutto il sistema informatico, eventualmente collegato a distanza con altri elaboratori, come nel caso dei sistemi telematici e l'aggressione può riguardare tanto il sistema nel suo complesso quanto una o più delle sue componenti materiali, quali il video, la tastiera, etc.

Il danneggiamento, inoltre, può riguardare anche i dati e i programmi informaticinonché le informazioni contenute nel sistema. L'art. 635 bis richiede che i beni informatici oggetto di aggressione siano «altrui»:il problema del significato da attribuire a tale termine sembra destinato adassumere rilevanza pratica proprio in relazione alla nuova figura di danneggiamento informatico, stante la diffusa prassi di procurarsi la disponibilità di hardware e di software attraverso contratti di

locazione (anziché di compravendita), solitamente accompagnati dalla contestuale conclusione di un contratto di assistenza e/o manutenzione con lo stesso fornitore.

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

«Salvo che il fatto costituisca più grave reato, chiunque commette un fatto direttoa distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la penaè della reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata».

La prevenzione dei reati presupposto in MONDIALPOL

Nell'espletamento di tutte le operazioni attinenti alla gestione e all'utilizzo dei sistemi informativi aziendali, i Dipendenti e gli Organi Sociali devono adottare e rispettare:

1. il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;
2. le norme inerenti la gestione e l'utilizzo dei sistemi informativi di MONDIALPOL;
3. il sistema disciplinare;
4. in generale, la normativa applicabile.

Si precisa che MONDIALPOL ha delegato ad un provider terzo la gestione dei sistemi informativi aziendali, l'implementazione, il monitoraggio e la corretta applicazione delle relative procedure di controllo, disciplinando compiutamente gli aspetti relativi a condizioni e modalità di erogazione del servizio all'interno di uno specifico contratto di service (si veda al riguardo anche quanto espressamente previsto dal successivo paragrafo).

In virtù degli accordi contrattuali in essere tra le parti, al fine di presidiare l'attività sensibile in oggetto, il service provider, su indicazioni specifiche di MONDIALPOL, adotta tutte le misure di cui al successivo paragrafo, garantendo piena conformità dei servizi erogati rispetto ai criteri stabiliti all'interno dei contratti ed essendo pertanto responsabile di eventuali inadempienze.

PRINCIPI GENERALI DI COMPORTAMENTO

La presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali (in via diretta) e dei lavoratori dipendenti e dei consulenti di MONDIALPOL (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente oindirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del d.lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente parte speciale. La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di:
    1. impegnarsi a non rendere pubbliche tutte le informazioni loro assegnate per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password, anche se superata, necessaria per l'accesso ai sistemi dell'Azienda);
    2. attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione (uscita dal sistema o blocco dell'accesso tramite password);
    3. accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere, entro le scadenze indicate dal Responsabile ICT Governance, alla modifica periodica della password;
    4. astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;
    5. assicurare la veridicità delle informazioni contenute in qualsivoglia atto e/o documento informatico. Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:
        a) intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;

b) installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile ICT Governance;

c) accedere alla rete aziendale, attraverso una connessione alternativa rispetto a quella messa a disposizione da parte dell'Azienda, al fine di eludere il sistema di accesso protetto implementato;

d) accedere in maniera non autorizzata ai sistemi informativi di terzi, né alterarne in alcun modo il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner,fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse di MONDIALPOL, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativainternazionale e locale relativa, in particolare, a comportamenti configurantiipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dalDecreto);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionalee locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto)e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da partedegli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e localerelativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es. clausole risolutive espresse, penali).

Le "attività sensibili relative ai delitti informatici e di trattamento illecito di dati" ai fini del d.lgs. 231/2001

Le attività sensibili individuate, in riferimento ai Delitti informatici e di trattamentoillecito di dati richiamati dall'art. 24-bis del d.lgs. 231/2001, sono le seguenti:

- Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato "Gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici" e "Invio telematico di atti, documenti e scritture").

Principi generali di controllo

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzaticome segue:

- SEGREGAZIONE DELLE ATTIVITÀ: si richiede l'applicazione del principio diseparazione delle attività tra chi autorizza, chi esegue e chi controlla;
- ESISTENZA DI PROCEDURE/NORME/CIRCOLARI: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- POTERI AUTORIZZATIVI E DI FIRMA: i poteri autorizzativi e di firma devono:

i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese;

ii) essere chiaramente definiti e conosciuti all'interno della Società;

- TRACCIABILITÀ: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

Principi di riferimento specifici relativi alle regolamentazione delle singole attività sensibili

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al capitolo 5, nel disciplinare le Fattispecie di attività sensibili di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

Utilizzo di risorse e informazioni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore

La regolamentazione dell'attività deve prevedere:

- l'implementazione di un approccio di governance dei sistemi informativi aziendali improntato al rispetto degli standard di sicurezza attiva e passiva, voltia garantire l'identità degli utenti e la protezione, la confidenzialità, l'integrità e la disponibilità dei dati. In particolare MONDIALPOL ha implementato un sistema centralizzato per la gestione delle componenti software, che, pertanto, non possono essere aggiornate o modificate in alcun modo da parte del singolo utente;
- la possibilità di accedere ai sistemi informativi solo previa opportuna identificazione da parte dell'utente, a mezzo username e password assegnati originariamente dall'Azienda. Per i sistemi di identificazione e accesso MONDIALPOL ha definito un iter tale per cui ogni utente ha necessità di inserire una password - costituita da un codice alfanumerico con un numero minimo di caratteri - per "loggarsi" e accedere ai sistemi;
- l'obbligo di cambiamento della password, a seguito del primo accesso, e la periodicità di modifica della suddetta password a seconda della frequenza di utilizzo e della criticità dei dati cui si accede per mezzo della stessa. In particolareil sistema informativo di MONDIALPOL prevede che ciascun utente modifichi la propria password periodicamente e comunque non oltre 60 giorni dalla registrazione. Qualora l'utente non provveda alla modifica di propria iniziativa, il sistema è strutturato in modo da inviare in automatico alert preliminari alcuni giorni prima che la password scada. Decorso anche questo termine, il sistema obbliga l'utente al cambio password per poter accedere al sistema; il monitoraggio, con frequenza periodica, di tutti gli accessi e le attività svolte sullarete aziendale nei limiti e con le modalità di cui alla vigente normativa.

MONDIALPOL prevede una lista con un elenco dettagliato di siti inaccessibili ai propri utenti;

- la registrazione e la verifica di tutti gli accessi e le attività svolte sulla rete aziendale da remoto, nei limiti e con le modalità di cui alla vigente normativa. In particolare gli utenti autorizzati da MONDIALPOL hanno la possibilità di accedere alla rete da remoto tramite check-point VPN - previa espressa autorizzazione del Responsabile gerarchico, oppure utilizzando esclusivamente la mail, con l'autorizzazione del Responsabile gerarchico e dopo aver seguito un corso sulla sicurezza informatica;

Inoltre il Responsabile del Personale comunica tutte le assunzioni e le cessazioni, nonché tutti i passaggi di stato/mansioni che possono impattare sulla gestione delle utenze informatiche, in modo che vengano attivate tutte le utenzenecessarie. Si sottolinea che, al fine di abilitare le utenze, è necessaria l'autorizzazione del diretto superiore dell'utente richiedente.

La cessazione dei rapporti lavorativi comportano la disattivazione delle utenze. E' previsto in ogni caso che, decorsi 60 giorni dalla data di ultimo utilizzo, le utenze vengano comunque disattivate; l'adeguata formazione di ogni risorsa sui comportamenti da tenere per garantirela sicurezza dei sistemi informativi e sulle possibili conseguenze, anche penali, che possono derivare dalla commissione di un illecito.

I controlli dell'organismo di vigilanza

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguitodelle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività di MONDIALPOL potenzialmente a rischio di compimento dei Delitti informatici e di trattamento illecito di dati che sono state incluse nel piano di lavoro approvato dall'Organismo stesso, in funzione della valutazione del rischio assegnata in sede di predisposizione del Modello e nel corso dei suoi successivi aggiornamenti (si veda al riguardo l'Allegato 1 al presente documento). Tali controlli sono diretti a verificare la conformità dei comportamenti in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le Fattispecie di attività sensibili. L'Organismo di Vigilanza riferisce di detti controlli all'Organismo di Gestione.

Parte Speciale 7: Privacy e Data Protection - GDPR

Inquadramento generale della normativa

Il General Data Protection Regulation (GDPR), ovvero il Regolamento UE n. 679/2016 sulla protezione dei dati personali (o Regolamento sulla privacy), è entrato in vigore Il 24 maggio 2016, per divenire pienamente applicabile dal 25 maggio 2018, abrogando la Direttiva 95/46/CE.5

Il testo affronta anche il tema dell'esportazione di dati personali al di fuori dell'UEe obbliga tutti i Titolari del trattamento dei dati (anche con sede legale fuori dall'Unione Europea) che trattano dati di residenti nell'unione europea ad osservare ed adempiere agli obblighi previsti. Gli obiettivi principali della Commissione europea nel GDPR sono quelli di restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali unificando e rendendo omogenea la normativa privacy dentrol'UE.[1] Dal 25 maggio 2018, il GDPR andrà a sostituire la direttiva sulla protezione dei dati (ufficialmente Direttiva 95/46/EC)[2] istituita nel 1995, abrogherà le norme del Codice per la protezione dei dati personali (dlgs.n. 196/2003) che risulteranno con esso incompatibili. Ciò potrà generare confusioneper alcuni ma si attende una normativa italiana "di raccordo" che metta ordine einserisca le norme del Codice privacy non incompatibili all'interno dell'impianto normativo del Regolamento. Con Direttiva UE 2016/680, in aggiunta a questo nuovo regolamento sarà applicata una disciplina speciale e in parte derogatrice per i trattamenti dei dati da parte dell'Autorità Giudiziaria e di tutte le forze di polizia; in ragione della caratteristica dell'istituto della direttiva europea talitrattamenti dei dati (Autorita' Giudiziaria e forze di polizia) continueranno ad essere differenti da Stato a Stato ed oggetto di una legislazione separatanazionale. Alcune novità del GDPR impongono un'attenta pianificazione fin da subito,potendo comportare modifiche organizzative significative e investimenti di naturatecnologica. Inoltre il GDPR rovescia completamente la prospettiva della disciplina di riferimento, istituendo un quadro normativo tutto incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di"accountability"). La nuova disciplina impone a tale soggetto di garantire il rispettodei principi in essa contenuti, ma anche di essere in grado di comprovarlo, adottando una serie di strumenti che lo stesso GDPR indica.

5 Le fonti principali di questo paragrafo sono le seguenti:

http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati
https://www.digital4.biz/executive/law4digital/gdpr-tutto-quello-che-avreste-voluto-sapere-ma-non-avete-osato-chiedere_436721510206.htm

In primis, il registro delle attività di trattamento, che deve contenere una serie di informazioni, tra cui le finalità del trattamento, la descrizione delle categorie di interessati e di dati personali che vengono trattati, oltre che l'indicazione delle misure di sicurezza adottate. La tenuta del registro costituisce un adempimento di fondamentale importanza nell'ottica del principio di accountability, in quanto permette di monitorare in maniera approfondita le operazioni di trattamento all'interno dell'organizzazione. Esso costituisce dunque sia uno strumento operativo di lavoro con cui censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un sano "ciclo di gestione" dei dati personali, siaun vero e proprio documento di carattere probatorio mediante il quale il Titolare del trattamento può dimostrare di aver adempiuto alle prescrizioni del Regolamento.
A tal fine, può risultare utile indicare nel registro una serie di elementi non espressamente imposti dall'art. 30 del GDPR, ma comunque importanti per tenertraccia delle operazioni di trattamento effettuate. Tra questi, ad esempio, la base giuridica del trattamento (ricompresa tra gli elementi che devono essere contenuti nell'informativa da consegnare all'interessato), o gli applicativi e/o database utilizzati, la cui elencazione può risultare necessaria per mappare con esattezzale misure di sicurezza implementate/da implementare, oltre che per condurre efficacemente la valutazione dei rischi.
Quest'ultima assume carattere imprescindibile per poter stabilire quali misure tecniche e organizzative adottare in azienda per garantire un livello di sicurezzaappropriato al rischio stesso. La nuova normativa, infatti, abbandona il concetto di "misure minime" del Codice Privacy, sostituendolo con quello di "misure adeguate". Tale maggiore discrezionalità, tuttavia, è accompagnata, come soprapreciSato, dall'onere in capo al Titolare del trattamento di poter dimostrare le ragioni che hanno portato a una determinata decisione.
Titolare del trattamento che potrà nominare un Data Protection Officer (DPO), ovvero una figura specialistica e altamente qualificata che supporti l'applicazionedegli obblighi della nuova normativa, e funga da punto di contatto con le Autoritàdi controllo e gli interessati. La designazione del DPO è

obbligatoria solo in alcuni casi (trattamenti effettuati su larga scala, posti in essere da un'Autorità pubblica/organismo pubblico, o che ricomprendono categorie particolari di dati personali). Tuttavia costituisce una buona prassi anche per le aziende che sarebbero esenti da tale adempimento.
In sostanza, l'ampio spettro di novità introdotte dal GDPR impone di definire un piano di adeguamento alla nuova normativa, coinvolgendo le diverse funzioni aziendali coinvolte in operazioni di trattamento di dati personali. È fondamentale sfruttare appieno il periodo transitorio a disposizione, per garantire la conformità alle nuove disposizioni entro il 25 maggio 2018.

Le regole da applicare

Scopo

Il regolamento si applica ai dati dei residenti nell'Unione Europea. Inoltre, a differenza dell'attuale direttiva, il regolamento si applica anche a società, aziende,imprese ed enti con sede legale fuori dall'UE che trattano dati personali di residenti nell'Unione Europea. Ciò anche a prescindere dal luogo o dai luoghi ovesono collocati i server e le banche dati. Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico ("le autoritàcompetenti per gli scopi di prevenzione, indagine, individuazione e persecuzionedi reati penali o esecuzione di provvedimenti penali"). Secondo la CommissioneEuropea "i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque cosa: nomi, foto, indirizzi email, dettagli bancari, interventi su siti webdi social network, informazioni mediche o indirizzi IP di computer."

Responsabilità

Il principio di responsabilità legato al trattamento dei dati personali resta ancorato(come nel Codice per la protezione dei dati personali) ad un concetto di responsabilità per esercizio di attività pericolosa con una valutazione ex ante in concreto ed una sostanziale inversione dell'onere della prova. Per non risponderedel danno commesso derivante dal trattamento dei dati personali occorre sostanzialmente provare di aver fatto tutto il possibile per evitarlo. Il Regolamentoaggancia e sviluppa questo tipo di responsabilità verso il concetto di Accountability (art. 5 co. 2). Occorre osservare i principi applicabili al trattamentodei dati personali di cui all'articolo 5 adempiendo alle relative obbligazioni ed essere in grado di comprovarlo.

Obblighi

I requisiti per le informative agli interessati rimangono e in parte sono ampliati. Essi devono includere il tempo di mantenimento dei dati personali e occorre fornire i contatti di chi controlla i dati e del funzionario preposto alla protezione dei dati. È stato introdotto il diritto di contestazione delle decisioni automatizzate, compresa la profilazione (Articolo 22). I cittadini hanno ora il diritto di contestare e contrastare decisioni che hanno impatto su di loro e che sono state realizzate unicamente in base ai risultati di un algoritmo. Tale diritto, fatta eccezione per dati personali intesi ad identificare in modo univoco una persona fisica (Articolo 9 comma 1), non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa inoltre misure adeguate a tutela dei diritti, della libertà e dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

I principi di Privacy by Design and by Default (Articolo 25) richiedono che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per prodotti e servizi.
Le impostazioni di privacy sono configurate su un livello alto in modo predefinito.

La risk analysis in materia di protezione dei dati personali

Le valutazioni di impatto in materia di protezione dei dati (art. 35) devono essereeffettuate nei casi in cui si verifichino rischi specifici per i diritti e le libertà dei soggetti dei dati. La valutazione e la riduzione del rischio sono richieste insiemead un'approvazione preventiva da parte delle autorità per la protezione dei dati (DPA, Data Protection Authority) per rischi elevati. I Responsabili per la protezione dei dati (Articoli 37) sono tenuti a verificare l'osservanza delle norme del Regolamento da parte dei titolari e nel caso di valutazioni di impatto, se richiesto dal titolare, sono tenuti a consultarsi con esso

Il consenso

Un valido consenso deve essere esplicitamente dato per la raccolta dei dati e peri propositi per i quali sono usati (Articolo 7; definito in Articolo 4). Pertanto se la richiesta viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro (Articolo 7). Condizione di validità delconsenso è che le finalità per cui viene richiesto siano esplicite, legittime,adeguate e pertinenti (Articolo 5). nel caso in cui il consenso al trattamento dei propri dati personali per una o più specifiche finalità sia stato espresso da minori esso è valido solo se il minore ha almeno 16 anni. L'età viene ridotta a 13 anni solo se lo stato membro ha previsto con legge una diversa età purché non inferiore a questa. Qualora il minore abbia un'età inferiore ai 16 o 13 anni, il consenso al trattamento deve essere dato da un genitore o da chi eserciti la potestà, e deve essere verificabile (Articolo 8). I controllori dei dati devono esserein grado di provare il consenso ("opt-in") e il consenso può essere ritirato o modificato con l'introduzione di limitazioni nel trattamento (art. 18).

La sicurezza dei dati

La sicurezza dei dati raccolti è garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio. A tal fine il titolare e il responsabile del trattamento garantiscono che chiunque faccia accesso ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri (Articolo 32). A garanzia dell'interessato il Regolamento UE 2016/679 regolamenta anche il caso di trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale (Articolo 44 ess) e prevede che l'interessato venga prontamente informato in presenza di una violazione che metta a rischio i suoi diritti e le sue libertà (Articolo 33).

Il DPO (Data Protection Officer)

Qualora l'elaborazione sia effettuata da un'autorità pubblica, fatto salvo per le corti o le autorità giudiziarie indipendenti agenti nella loro competenza giudiziaria, o qualora, nel settore privato, l'elaborazione sia effettuata da un controllore le cuiattività principali consistono di operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico dei soggetti dei dati, una persona

esperta dilegislazione e pratiche relative alla protezione dei dati deve assistere colui che li controlla o li gestisce al fine di verificare l'osservanza interna al regolamento. Il responsabile per la protezione dei dati è una figura simile, ma non identica, al funzionario preposto all'osservanza, in quanto ci si aspetta che il primo abbia una buona padronanza dei processi informatici, della sicurezza dei dati (inclusa la gestione dei ciber-attacchi) e di altre questioni di coerenza aziendale riguardanti il mantenimento e l'elaborazione di dati personali e sensibili. Ricorda molto l'Odv (organismo di vigilanza) della legge n. 231 del 2001 sulla responsabilità penale delle persone giuridiche e il responsabile anticorruzioni per la sua autonomia, indipendenza e assenza di conflitti di interesse. L'insieme di competenze richieste si estende al di là della comprensione dell'osservanza legale di leggi e regolamenti sulla protezione dei dati e comporterà una grande preparazione e professionalità. Il monitoraggio dei Data protection office sarà onere del regolatore e non del consiglio di amministrazione dell'organizzazione che assume il funzionario. La nomina di un responsabile per la protezione dei dati all'interno di una grande organizzazione rappresenterà una sfida sia per il consiglio di amministrazione, sia per lo stesso responsabile. Considerati lo scopo e la natura della nomina, sono in gioco una miriade di questioni legate alla governance e a fattori umani che le organizzazioni e le aziende dovranno affrontare. Inoltre, chi detiene l'incarico dovrà creare un proprio team di supporto e sarà anche responsabile del proprio sviluppo professionale continuativo, dal momento che, come "mini-regolatore" ad ogni effetto, dovrà essere indipendente dall'organizzazione che lo ha assunto.

Violazioni dei dati (Data Breach – art. 33 e 34)

Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe didati all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto aconoscenza. I resoconti delle fughe di dati non sono soggetti ad alcuno standard"de minimis" e debbono essere riferite all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore. In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

Sanzioni

Possono essere comminate le seguenti sanzioni:

- un'ammonizione scritta in casi di una prima mancata osservanza non intenzionale.

- accertamenti regolari e periodici sulla protezione dei dati
- una multa fino a 10 milioni di euro, o fino al 2% del volume d'affari globaleregistrato nell'anno precedente nei casi previsti dall'Articolo 83, Paragrafo4 o fino a 20 milioni di euro o fino al 4% del volume d'affari nei casi previstidai Paragrafi 5 e 6.

Diritti degli interessati

Diritto alla cancellazione, limitazione e rettifica

Il cosiddetto diritto all'oblio è stato sostituito da un più limitato diritto alla cancellazione nella versione del GDPR adottata dal Parlamento Europeo nel marzo del 2014. L'Articolo 17 stabilisce che il soggetto dei dati ha il diritto di richiedere la cancellazione di dati personali relativi a sé sulla base di unaqualsiasi di una serie di giurisdizioni che comprendono la mancata osservanza dell'articolo 6.1 (legalità), il quale include il caso (f) in cui gli interessi o i diritti fondamentali del soggetto dei dati richiedente la loro protezione prevalgono sui legittimi interessi del controllore. L'interessato deve poter esercitare questo suo diritto con la stessa facilità con cui ha espresso il consenso al trattamento dei suoi dati. Il responsabile del trattamento, dietro richiesta dell'interessato, dovrà comunicare all'interessato i destinatari a cui ha trasmesso la sua richiesta di cancellazione (Articolo 19). Sul responsabile del trattamento grava lo stesso onere in caso di richiesta di limitazione o di rettifica dei dati presentata dall'interessato rispettivamente ai sensi dell'art. 18 e dell'art. 16 del RegolamentoUE 2016/679.

Diritto alla portabilità

Una persona deve essere in grado di trasferire i propri dati personali da un sistema di elaborazione elettronico a un altro senza che il controllore dei dati possa impedirlo. Inoltre, i dati devono essere forniti dal controllore in un formatostrutturato e di uso comune. Il diritto alla portabilità dei dati è sancito dall'Articolo18 del GDPR. Gli esperti legali vedono nella versione finale di questa misura la creazione di un "nuovo diritto" che "si estende oltre l'ambito della portabilità dei dati tra due controllori, così come stipulato dall'Articolo 18".

Le esigenze dell'organizzazione

Data l'ampiezza del perimetro di impatto del GDPR a livello aziendale, mappare il modello attuale e identificarne in modo esaustivo i gap, in relazione a quanto richiesto dal Regolamento, richiede un approccio strutturato e comprensivo di tutte le leve su cui è possibile agire in relazione all'obiettivo di adeguamento, quali:

1. Organizzazione e ruoli. Definizione e formalizzazione del modello organizzativo, dei ruoli e delle relative responsabilità all'interno dell'azienda, in relazione all'indirizzo e alla gestione dei temi legati alla Privacy.
2. Persone, cultura e competenze. Progettazione e diffusione della culturadella protezione dei dati e delle policy di sicurezza all'interno dell'organizzazione, attraverso attività di formazione e sensibilizzazione.
3. Processi e regole. È senza dubbio una delle aree più impattate dalle richieste di adeguamento del GDPR, basti ricordare la Privacy by design,la portabilità dei dati, la gestione dei data breach, la gestione del registro dei trattamenti, la gestione dei diritti degli interessati. Sono solo alcuni deiprocessi richiesti dal Regolamento che dovranno essere disegnati, implementati e presidiati nell'organizzazione.
4. Documentazione. Definizione delle procedure del manuale di gestione della data protection, aggiornamento dei contratti con le terze parti, adeguamento e/o stesura della documentazione di base quali informative,moduli di consenso, lettere di nomina, ecc.
5. Tecnologia e strumenti. Area di rilevante importanza - tipicamente anchedal punto di vista di investimenti da prevedere in ottica di piano diadeguamento - in ambito di misure di sicurezza informatica (antivirus, disaster recovery, firewall, pseudonimizzazione dati, cifratura dati,prevenzione e rilevazione data breach, Identity Management, ecc.), di sicurezza fisica (es. controllo accessi), di adozione di tool IT GRC (Governance, Risk & Compliance).
6. Sistema di controllo. Progettazione e gestione di un cruscotto di KPI peril monitoraggio della compliance a normative esterne (es. GDPR), regolamenti interni, progettazione di reportistica ad hoc da condividere a vari livelli dell'organizzazione;
7. Cessione Rami d'Azienda e Trasferimento Dati. Definizione di specifiche cautele contrattuali e informative privacy (ex artt. 13 e 14 GDPR) in occasione della cessione del ramo d'azienda (Business 1) relativo ai contratti pubblici, al fine di garantire la liceità della migrazione dei dati

personali del personale dipendente trasferito e degli interessati (Stazioni Appaltanti) all'operatore subentrante.

L'osservanza del regolamento nel modello organizzativo

Il principio di funzionamento del sistema

In relazione ai principi descritti al paragrafo precedente, il Modello Organizzativogià implementato in azienda per la prevenzione dei reati presupposto 231, si presta efficacemente per la gestione ed il monitoraggio del Regolamento Europeo oggetto della presente Parte Speciale consentendo di essere in linea per i seguenti parametri:

- Organizzazione e ruoli: l'organigramma dinamico consente, oltre a visualizzare le funzioni ed i relativi responsabili, di monitorare il rischio specifico ed implementare le necessarie azioni correttive sulla base dellarilevazione delle non conformità
- Analisi e Gestione del Rischio: il sistema adottato nasce con lo scopo di misurare costantemente il rischio sotteso ai processi nelle attività sensibili;il Regolamento Europeo per la Protezione dei Dati Personali richiede infatti che l'azione dell'Azienda in tale ambito sia improntata ai principi di compliance e di risk management insieme; il risultato è quello di un'analisidei rischi finalizzata al rispetto delle regole
- Processi e regole: le procedure aziendali vengono sottoposte ad un costante controllo, e ad una misurazione delle performances in ottica di prevenzione del rischio; anche in tal caso giova la possibilità di attribuire non conformità ed azioni correttive
- Documentazione: il sistema adottato presenta le caratteristiche di conservazione della documentazione necessaria, che può essereutilizzata anche a fini probatori, e collegata alle schede di controllo destinate all'analisi del rischio.

L'applicazione delle regole e l'implementazione delle azioni di sistema

Le aree di processo e le schede di controllo già implementate per l'analisi del rischio degli altri reati presupposto sono state revisionate nella struttura, comprendendo le sanzioni indicate dalla normativa introdotta in tema di protezione dei dati personali. Le ipotesi di sanzione misurate con lo strumento dinamico risultano quindiproporzionalmente aumentate di gravità, nella misura in cui la fase di audit

abbia rilevato un pericolo di commissione dei reati presupposto che possono portare ad una condotta tipica.

All'applicazione del Regolamento Europeo è stata quindi dedicata una nuova Area di Processo, che permette di identificare le attività sensibili e valutare costantemente le necessarie azioni correttive, misurando la pericolosità delle singole funzioni interessate in organigramma, in relazione alle attività svolte.

Parte Speciale 8: Le Segnalazioni Anonime - WHISTLEBLOWING

1. Definizioni

Nel presente documento le seguenti espressioni hanno il significato di seguito indicato:

- "ANAC": istituita con la legge n. 190/2012 è l'autorità amministrativa indipendente la cui missione istituzionale è individuata nella prevenzione della corruzione in tutti gli ambiti dell'attività amministrativa.
- "Attività a rischio di reato": il processo, l'operazione, l'atto, ovvero l'insieme di operazioni e atti, che possono esporre la Società al rischio di sanzioni ai sensi del Decreto in funzione della commissione di un Reato.
- "CCNL": il Contratto Collettivo Nazionale di Lavoro applicabile ai dipendenti della Società.
- "Codice Etico": il documento, ufficialmente voluto e approvato dal vertice della Società quale esplicazione della politica societaria, che contiene i principi generali di comportamento - ovvero, raccomandazioni, obblighi e/o divieti - a cui i Destinatari devono attenersi e la cui violazione è sanzionata.
- "Contesto lavorativo": le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4 del D. Lgs. 24/2023, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile;
- "D. Lgs. 231/2001" o "Decreto": il Decreto Legislativo 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre

2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni ed integrazioni.

- "Destinatari": Organi statutari (il Presidente; il Collegio di Presidenza; il Consiglio di Amministrazione; il Collegio dei Sindaci), Personale della Società, Fornitori e tutti coloro che operano nell'interesse o a vantaggio della Società, con o senza rappresentanza e a prescindere dalla natura e dal tipo di rapporto intrattenuto con il soggetto preponente. I Destinatari sono tenuti al rispetto del Modello, del Codice Etico e dei Protocolli preventivi.
- "Dipendenti": tutte le persone fisiche che intrattengono con la Società un rapporto di lavoro subordinato.
- "Divulgazione pubblica" o "divulgare pubblicamente": rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.
- "Facilitatore": soggetto che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.
- "Informazioni sulle violazioni" informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2 del d. Lgs. 24/2023 (ovvero settore pubblico e settore privato), nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.
- "Linee Guida": le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001, pubblicate dalle associazioni di categoria, che sono state considerate ai fini della predisposizione ed adozione del Modello. Ai fini del presente Modello ci si è ispirati a quanto indicato dalle Linee Guida di Confindustria e quelle del Consiglio Nazionale dei Dottori Commercialisti ed Esperti contabili per gli Enti No profit.
- "Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001" o "Modello": il Modello di organizzazione, gestione e controllo ritenuto dagli Organi Sociali idoneo a prevenire i Reati e, pertanto, adottato dalla Società, ai sensi degli articoli 6 e 7 del Decreto

Legislativo, al fine di prevenire la realizzazione dei Reati stessi da parte del Personale apicale o subordinato, così come descritto dal presente documento e relativi allegati.

- "Organi Statutari": il Presidente, i Vice Presidenti, il Collegio di Presidenza, il Consiglio di Amministrazione, il Collegio dei Sindaci della Società, in funzione del senso della frase di riferimento.
- "Organismo di Vigilanza" o "OdV": l'Organismo previsto dall'art. 6 del Decreto Legislativo, avente il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo, nonché sull'aggiornamento dello stesso.
- "Personale": tutte le persone fisiche che intrattengono con la Società un rapporto di lavoro, inclusi i lavoratori dipendenti, interinali, i collaboratori, gli "stagisti", i volontari ed i liberi professionisti che abbiano ricevuto un incarico da parte della Società.
- "Personale Apicale": i soggetti di cui all'articolo 5, comma 1, lett. a) del Decreto, ovvero i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società; in particolare, il Presidente, i Vice Presidenti, i membri del Consiglio di Amministrazione e gli eventuali institori e procuratori della Società.
- "Personale sottoposto ad altrui direzione": i soggetti di cui all'articolo 5, comma 1, lett. b) del Decreto, ovvero tutto il Personale che opera sotto la direzione o la vigilanza del Personale Apicale.
- "Persona segnalante": la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.
- "Persona coinvolta": la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente.
- "Pubblica Amministrazione" o "P.A.": Per Amministrazione Pubblica si deve intendere:
    - lo Stato (o Amministrazione Statale);
    - gli Enti Pubblici: si specifica che l'Ente Pubblico è individuato come tale dalla legge oppure è un Ente sottoposto ad un sistema di controlli pubblici, all'ingerenza dello Stato o di altra Amministrazione per ciò che concerne la nomina e la revoca dei suoi amministratori, nonché l'Amministrazione dell'Ente stesso. È caratterizzato dalla partecipazione dello Stato, o di altra Amministrazione Pubblica, alle spese di gestione;

oppure dal potere di direttiva che lo Stato vanta nei confronti dei suoi organi; o dal finanziamento pubblico istituzionale; o dalla costituzione ad iniziativa pubblica. A titolo puramente esemplificativo e non esaustivo sono da considerarsi Pubbliche Amministrazioni in senso lato le seguenti Società: Ferrovie dello Stato, Autostrade S.p.A., AEM Milano, ecc.

- Pubblico Ufficiale: colui che esercita "una pubblica funzione legislativa, giudiziaria o amministrativa". Agli effetti della legge penale "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. 357 c.p.);
- Incaricato di Pubblico Servizio: colui che "a qualunque titolo presta 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

- "Protocollo": la misura organizzativa, fisica e/o logica prevista dal Modello al fine di prevenire il rischio di commissione dei Reati.
- "Reati" o il "Reato": l'insieme dei reati, o il singolo reato, richiamati dal D. Lgs. 231/2001 (per come eventualmente modificato e integrato in futuro).
- "Ritorsione": qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.
- "Segnalazione": la comunicazione scritta od orale di informazioni sulle violazioni;
- "Segnalazione esterna": la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna;
- "Segnalazione interna": la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna;

- "Seguito": l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;
- "Sistema Disciplinare": l'insieme delle misure sanzionatorie applicabili in caso di violazione delle regole procedimentali e comportamentali previste dal Modello;
- "Violazioni": comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:
    1. illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6);
    2. condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);
    3. illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nel relativo allegato al decreto legislativo n. 24/2023 ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nel relativo allegato al decreto legislativo n. 24/2023, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
    4. atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
    5. atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di

imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;

6. atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5).

2. Premessa

La Società ha conformato la propria politica al rispetto dei principi di legalità e correttezza previsti dal Codice Etico, con ciò palesando la propria estraneità a politiche o comportamenti scorretti o illeciti.

Tale politica è declinata nel Modello di organizzazione, gestione e controllo per la prevenzione del rischio di reato adottato ai sensi e per gli effetti indicati dagli articoli 6 e 7 del D. Lgs. 231/2001.

Tutti i Destinatari del Modello hanno l'obbligo di Segnalare Violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità della Società, nell'ambito delle Violazioni di cui alla presente procedura, di cui siano venuti a conoscenza nel Contesto lavorativo.

Dette Segnalazioni devono essere il più possibile circostanziate, effettuate in buona fede, sulla base della ragionevole convinzione fondata su elementi di fatto precisi e concordanti.

La presente procedura costituisce un'attuazione all'intero della Società delle più recenti previsioni normative in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali di cui al D. Lgs. n. 24/2023. Tale norma costituisce il riferimento prioritario per ogni attività di seguito contemplata.

3. Scopo

Il presente documento ha l'obiettivo di regolare il processo di gestione delle Segnalazioni, come definite al successivo capitolo 4, secondo modalità atte a garantire la tutela della riservatezza dell'identità della Persona segnalante.

La Società, con la presente procedura definisce il proprio modello di ricevimento e di gestione delle segnalazioni interne, nonché il canale interno di segnalazione, individuando misure tecniche e

organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti anche dal trattamento di dati personali effettuati per la gestione delle stesse, nel rispetto di quanto previsto dal Regolamento (UE) 2016/679 e dell'articolo 18 del decreto legislativo n. 51 del 2018.

4. Le Segnalazioni oggetto della presente procedura

La presente procedura riguarda le Segnalazioni (di seguito anche "whistleblowing") delle seguenti Violazioni (come definite nella sezione dedicata del presente documento e individuate nell'art. 2 del D. Lgs. n. 24 del 10 marzo 2023):

- illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6);
- condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni del Modello di organizzazione e gestione previsti dallo stesso Decreto e adottato dalla Società, che non rientrano nei numeri 3), 4), 5) e 6);
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nel relativo allegato al decreto legislativo n. 24/2023 ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nel relativo allegato al decreto legislativo n. 24/2023 ovvero, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
- atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i

meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;

- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5).

Le Segnalazioni possono avere ad oggetto:

- informazioni, compresi i fondati sospetti, riguardanti Violazioni commesse;
- informazioni, compresi i fondati sospetti, riguardanti Violazioni che, sulla base di elementi concreti, potrebbero essere commesse;
- elementi riguardanti condotte volte ad occultare tali violazioni.

Con specifico riferimento alle condotte di cui al numero 2) si richiamano, a titolo esemplificativo, le seguenti fattispecie:

- condotte illecite, rilevanti ai sensi del Decreto Legislativo 231/01;
- violazioni del Modello, del Codice Etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- sospetti di violazioni del Modello, del Codice Etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- operazioni societarie o di business per cui si sospetta possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto.

Le Segnalazioni di Violazioni di cui al numero 2), possono essere effettuate solo tramite il canale di Segnalazione interna (vedi cap. 6.1.1. "Segnalazione interna").

5. Ambito di applicazione

Il presente documento si applica ai Destinatari come sopra identificati nel capitolo "1. Definizioni".

Il processo di gestione della Segnalazione illustrato nel presente documento non fa riferimento a comunicazioni di carattere commerciale o a informazioni di carattere meramente delatorio che non afferiscono alle Violazioni di cui al D.lgs. 24/23, come sopra definite.

La presente procedura non si applica altresì alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della Persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate.

In linea generale, la Società esorta i propri dipendenti a risolvere eventuali controversie lavorative, ove possibile, attraverso il dialogo, anche informale, con i propri colleghi e/o con il proprio responsabile diretto.

6. Processo di gestione delle Segnalazioni

6.1. Canali di Segnalazione

6.1.1. Segnalazione interna

Ai sensi di legge, la Società ha attivato un proprio canale di segnalazione interna di cui al D. Lgs. n. 24/2023, che garantisce, la riservatezza dell'identità della Persona Segnalante, della Persona coinvolta e della persona comunque menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione.

La gestione di tale canale è affidata all'Organismo di Vigilanza della Società, con l'unica eccezione di cui si dirà di seguito (vedi par. 11 "Casi particolari").

I componenti dell'Organismo di Vigilanza sono stati debitamente autorizzati dalla Società al trattamento dei dati personali contenuti nelle Segnalazioni interne.

Le Segnalazioni possono essere effettuate attraverso le seguenti modalità:

- in forma scritta, con modalità informatiche, tramite la casella PEC all'indirizzo email: **odv@mondiapol.eu**;
- in forma scritta, attraverso posta ordinaria, all'attenzione dell'Organismo di Vigilanza con la dicitura "riservata personale", presso lo Studio Lexia Avvocati, con sede in Palermo, via Quintino Sella, 77;
- in forma orale mediante richiesta di incontro diretto con l'Organismo di Vigilanza fissato entro un termine ragionevole. In tali casi, previo consenso della Persona segnalante, la Segnalazione interna potrà essere documentata a cura del personale autorizzato mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la Persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

Per maggiori dettagli si rimanda al paragrafo 6.2.

6.1.2. Segnalazione esterna

La Persona segnalante può altresì presentare una segnalazione esterna all'Autorità Nazionale Anti Corruzione (ANAC) al ricorrere delle seguenti condizioni:

- la segnalazione interna presentata secondo i termini previsti dalla presente procedura non ha avuto alcun seguito;
- la Persona segnalante ha fondati e comprovati motivi per ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito, ovvero la stessa possa determinare il rischio di ritorsione;
- la Persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Il canale di segnalazione esterno istituito dall'ANAC garantisce, alla stregua del canale interno sopramenzionato definito dalla Società, la riservatezza dell'identità del segnalante, del contenuto della segnalazione, del segnalato e di persone eventualmente coinvolte.

Le segnalazioni esterne sono effettuate in forma scritta tramite la piattaforma informatica messa a disposizione da ANAC sul proprio sito web nella sezione dedicata al "Whistleblowing". La segnalazione potrà essere realizzata anche in forma orale attraverso linee telefoniche o sistemi di messagistica vocale, ovvero su richiesta del Segnalante, mediante un incontro diretto fissato entro un termine ragionevole; le modalità di accesso a tali canali sono specificati dall'ANAC sul proprio sito web.

6.1.3. Divulgazione pubblica

Alla Persona segnalante è, altresì, garantita la possibilità di effettuare una divulgazione pubblica in presenza di una delle seguenti condizioni:

- aver previamente effettuato una segnalazione interna e/o esterna e non aver ricevuto riscontro nei termini previsti dalla presente procedura in merito alle misure previste o adottate per dare seguito alla segnalazione;
- avere fondato motivo per ritenere che la Violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- avere fondato motivo di ritenere che la Segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso

concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

6.2. Invio della Segnalazione interna

Colui che desidera effettuare una Segnalazione interna scritta può inoltrarla allegando l'apposito modulo di cui l'Allegato 1.

Il Modulo fornisce alla Persona segnalante un percorso guidato, strutturato attraverso una serie di domande e di richieste di elementi a supporto, volte a descrivere in maniera chiara, precisa e circostanziata la situazione oggetto della Segnalazione.

Le Segnalazioni devono essere fondate su elementi di fatto precisi e concordanti. La Persona segnalante è invitata ad allegare tutta la documentazione comprovante i fatti segnalati, astenendosi dall'intraprendere autonome iniziative di analisi e approfondimento.

6.3. Ricezione e analisi della Segnalazione interna

Le Segnalazioni sono gestite, in primo luogo, dall'Organismo di Vigilanza, che tratta le Segnalazioni interne ricevute in maniera riservata, adottando modalità di verifica idonee a tutelare l'identità della Persona segnalante nonché quella delle Persone coinvolte.

<u>Verifica preliminare</u>

Tutte le Segnalazioni interne ricevute sono oggetto di una verifica da parte dell'Organismo di Vigilanza al fine di comprendere se la comunicazione ricevuta sia corredata dalle informazioni necessarie per verificarne preliminarmente la fondatezza e per poter avviare le successive attività di approfondimento.

L'OdV si impegna a rilasciare alla Persona segnalante avviso di ricevimento entro 7 giorni dal ricevimento della Segnalazione interna.

L'OdV dà diligente seguito alle Segnalazioni ricevute, mantenendo interlocuzioni con la Persona segnalante, a cui richiede, se necessario, informazioni.

Ferma restando la riservatezza delle informazioni ricevute, nelle attività di verifica preliminare, l'OdV potrà avvalersi del supporto di altre strutture della Società o di consulenti specializzati, in base alle specifiche competenze richieste in relazione al contenuto della Segnalazione oggetto di verifica.

Al termine della verifica preliminare, l'OdV può archiviare le Segnalazioni interne:

- non circostanziate;
- quelle che, in base alla descrizione dei fatti e alle informazioni fornite dalla Persona segnalante, non consentano di ottenere un quadro sufficientemente dettagliato da poter avviare ulteriori approfondimenti per accertarne la fondatezza;
- quelle manifestamente infondate.

Nella fase di istruttoria e verifica, l'OdV:

- garantisce l'imparzialità, l'equità e l'accuratezza dell'analisi e valutazione della Segnalazione interna;
- assicura la confidenzialità delle informazioni raccolte e la riservatezza del nominativo della Persona segnalante, ove fornito;
- si impegna a non utilizzare le Segnalazioni interne oltre quanto necessario per dare adeguato seguito alle stesse. L'OdV non potrà rivelare l'identità della Persona segnalante e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità, senza il consenso espresso della Persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle Segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del Regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al D.lgs. 196/03.

<u>Segnalazioni che non superano la verifica preliminare</u>

Le Segnalazioni interne che non superano la fase preliminare vengono archiviate a cura dell'OdV in un apposito spazio logico che garantisca con strumenti di crittografia, la riservatezza dell'identità del segnalante, accessibile solo ai componenti dell'OdV.

In ogni caso l'OdV annota la Segnalazione interna e le attività effettuate a seguito della sua ricezione nel Libro Segnalazioni e Istruttorie sempre garantendo la riservatezza dell'identità del Persona segnalante e delle Persone coinvolte. Il Libro Segnalazioni e Istruttorie deve essere conservato a cura dell'OdV stesso e reso accessibile soltanto ai soggetti autorizzati dalla Società.

Segnalazioni che superano la verifica preliminare

Qualora la verifica preliminare eseguita dall'OdV abbia stabilito che la Segnalazione interna, adeguatamente circostanziata e corredata da evidenze di cui è stato possibile dedurne la fondatezza, integra una condotta perseguibile anche solo disciplinarmente, si provvede a:

- dare immediata e motivata informativa alle funzioni/organi preposti all'applicazione del sistema sanzionatorio e disciplinare, di cui al capitolo 7 "Sistema sanzionatorio e disciplinare", affinché questi possano autodeterminarsi in merito all'azione disciplinare da intraprendere anche nel rispetto dei principi di specificità, immediatezza e immutabilità della contestazione qualora le Persone coinvolte siano lavoratori della Società. Nell'ambito della propria autodeterminazione tali funzioni/organi possono svolgere ulteriori indagini e verifiche richiedendo il supporto dell'OdV che permane l'unico interlocutore della Persona segnalante e ne garantisce l'anonimato. Laddove, a seguito di ulteriori indagini e verifiche tali funzioni/organi:
    a. ritengano la condotta non contestabile, ne danno immediata comunicazione all'OdV affinché quest'ultimo possa archiviare la Segnalazione nei modi sopra descritti (si veda par. Segnalazioni che non superano la verifica preliminare) e informare la Persona segnalante circa lo stato della procedura;
    b. decidano di procedere con la contestazione, assieme a questa deve essere fornita alla Persona coinvolta idonea informativa privacy ai sensi dell'art. 14 del GDPR e comunque entro un mese dall'avvio del trattamento.
- informare l'organo di gestione e/o di controllo per le valutazioni di rispettiva competenza.
- formalizzare un report finale al termine delle attività di indagine il cui destinatario è l'organo o la funzione depositaria dell'azione disciplinare e/o delle azioni correttive finalizzate ad evitare in futuro situazioni analoghe (anche ai sensi dell'art. 7, comma 4, del D. Lgs. 231/2001).

L'OdV si impegna a processare le Segnalazioni interne ricevute entro un tempo ragionevole ed a fornire un riscontro in merito alla Persona segnalante (attraverso la casella PEC o altro strumento indicato dalla Persona segnalante o con questa concordato) entro:

- tre mesi dalla data dell'avviso di ricevimento,

o, in mancanza di tale avviso,

- entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione.

7. Sistema sanzionatorio e disciplinare

7.1. Attivazione del Sistema Sanzionatorio e disciplinare

Nei casi in cui, dalle indagini realizzate le Violazioni oggetto della Segnalazione interna siano risultate fondate, l'organo/funzione preposto all'attivazione del Sistema sanzionatorio decide quale tipologia di sanzione comminata ai soggetti che hanno commesso.

A seconda della qualificazione della Persona coinvolta e dell'inquadramento eventuale giuslavoristico, il Sistema Disciplinare è attivato da:

- Presidente qualora sia un dipendente o un soggetto terzo (fornitore, volontario, ecc.);
- Consiglio di Amministrazione un componente del Collegio Sindacale;
- Collegio Sindacale, qualora sia il Presidente, uno dei Vice Presidenti o un Amministratore.

La sanzione può essere graduata in funzione della gravità del fatto, nel rispetto delle normative di volta in volta applicabili (ad es. normativa giuslavoristica in caso di lavoratori della Società).

Nel caso in cui la Persona segnalante sia corresponsabile delle Violazioni, è previsto un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la Violazione commessa e con la disciplina applicabile.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non può essere rivelata senza il suo consenso espresso. Il consenso libero, specifico, inequivocabile e informato della Persona segnalante deve essere raccolto in forma scritta e conservato a cura dell'OdV nella documentazione relativa alla Segnalazione.

Nell'ambito del procedimento disciplinare, l'identità della Persona segnalante, in assenza di consenso, non può essere comunque rivelata ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla Segnalazione, anche se conseguenti alla stessa.

Qualora invece la contestazione sia fondata in tutto o in parte sulla Segnalazione e la conoscenza dell'identità della Persona segnalante sia indispensabile per la difesa della Persona coinvolta, l'OdV, laddove non abbia già raccolto il consenso della Persona segnalante, informa quest'ultima, mediante comunicazione scritta, delle ragioni su cui si fonda la necessità di rivelare la sua identità o altre

informazioni dalle quali possa potenzialmente evincersi, al fine di per dare completo seguito alla gestione della Segnalazione, ovvero ai fini del procedimento disciplinare.

In caso di diniego del consenso da parte della Persona segnalante alla comunicazione della sua identità, l'OdV archivia la Segnalazione interna senza darvi ulteriore seguito.

La presente procedura lascia impregiudicata la responsabilità penale e disciplinare della Persona segnalante nell'ipotesi di Segnalazione calunniosa o diffamatoria ai sensi del codice penale e dell'art. 2043 del codice civile.

È altresì sanzionato il comportamento di chi effettua con dolo o colpa grave Segnalazioni che si rivelano infondate.

Sono fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali le Segnalazioni interne manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione della presente procedura.

Pertanto, quando è accertata, anche con sentenza di primo grado, la responsabilità penale della Persona segnalante per i reati di diffamazione o di calunnia, ovvero la responsabilità civile, nei casi di dolo o colpa grave, le tutele previste nella presente procedura non sono garantite e alla Persona segnalante è irrogata una sanzione disciplinare cui al presente capitolo.

8. Tutele della Persona segnalante e applicazione delle misure di protezione

È vietata nei confronti della Persona segnalante qualsiasi forma di Ritorsione.

Ai sensi di legge, il divieto di Ritorsione e, comunque, le misure di protezione normativamente previste nei confronti della Persona segnalante, si applicano anche:

- ai Facilitatori;
- alle persone del medesimo Contesto lavorativo della Persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una Divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della Persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una Divulgazione pubblica, che lavorano nel

medesimo Contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;

- agli enti di proprietà della Persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo Contesto lavorativo delle predette persone.

Le misure di protezione trovano applicazione quando al momento della Segnalazione (interna e/o esterna), o della denuncia all'autorità giudiziaria o contabile o della Divulgazione pubblica, la Persona segnalante:

- aveva fondato motivo di ritenere che le informazioni sulle Violazioni fossero vere e afferissero a violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'integrità del Patronato, di cui siano venute a conoscenza nel Contesto lavorativo;
- ha effettuato la Segnalazione (interna e/o esterna) o Divulgazione pubblica secondo quanto previsto dalla normativa alle stesse applicabile ai sensi del D. Lgs. 24/2023.

I motivi che hanno indotto la persona a Segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

Le condizioni previste per la protezione si applicano anche nei casi di Segnalazione (interna e/o esterna) o denuncia all'autorità giudiziaria o contabile o Divulgazione pubblica anonime, se la Persona segnalante è stata successivamente identificata e ha subito ritorsioni, nonché nei casi di segnalazione presentata alle istituzioni, agli organi e agli organismi competenti dell'Unione Europea, in conformità alle condizioni di cui alla presente procedura (nonché dell'articolo 6 del D. lgs. 24/2023).

L'adozione di Ritorsioni nei confronti delle Persone segnalanti può essere comunicata all'ANAC, che a sua volta informerà l'Ispettorato nazionale del lavoro per i provvedimenti di propria competenza.

Gli atti assunti in violazione del divieto di Ritorsione sono nulli e la Persona segnalante che sia stata licenziata a causa della Segnalazione (interna e/o esterna) di Divulgazione pubblica o di denuncia ha diritto a essere reintegrata sul posto di lavoro.

Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati nei confronti della Persona segnalante si presume che gli stessi siano stati posti in essere a causa della Segnalazione

(interna e/o esterna), della Divulgazione pubblica o della denuncia. A norma di legge, l'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla Segnalazione (interna e/o esterna), alla Divulgazione pubblica o alla denuncia è a carico del soggetto che li ha posti in essere (es. Datore di Lavoro).

Inoltre, in caso di domanda risarcitoria presentata all'autorità giudiziaria dalla Persona segnalante se questa dimostra di aver effettuato una Segnalazione (interna e/o esterne), una Divulgazione pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno, si presume, salvo prova contraria, che il danno ne sia conseguenza.

8.1. Limitazioni della responsabilità

Ai sensi di legge, non è punibile la Persona segnalante che riveli o diffonda informazioni sulle Violazioni coperte dall'obbligo di segreto, diverso da quello di cui all'articolo 1, comma 3 del D. lgs. 24/2023, o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero riveli o diffonda informazioni sulle Violazioni che offendono la reputazione della Persona coinvolta o denunciata, quando, al momento della rivelazione o diffusione, vi fossero fondati motivi per ritenere che la rivelazione o diffusione delle stesse informazioni fosse necessaria per svelare la Violazione, e la Segnalazione (interna e/o esterna), la Divulgazione pubblica o la denuncia all'autorità giudiziaria o contabile sia stata effettuata nel rispetto di quanto previsto dal D. Lgs. 24/2023.

In tali casi, è esclusa altresì ogni ulteriore responsabilità, anche di natura civile o amministrativa.

Salvo che il fatto costituisca reato, la Società o la Persona segnalante non incorrono in alcuna responsabilità, anche di natura civile o amministrativa, per l'acquisizione delle Informazioni sulle Violazioni o per l'accesso alle stesse.

In ogni caso, la responsabilità penale e ogni altra responsabilità, anche di natura civile o amministrativa, non è esclusa per i comportamenti, gli atti o le omissioni non collegati alla Segnalazione (interna e/o esterna), alla denuncia all'autorità giudiziaria o contabile o alla Divulgazione pubblica o che non sono strettamente necessari a rivelare la Violazione.

9. Conservazione e Archiviazione

L'OdV è informato delle eventuali sanzioni irrogate a fronte delle Segnalazioni interne ed esterne. Le funzioni aziendali competenti archiviano la documentazione inerente al processo sanzionatorio e disciplinare.

L'OdV provvede pertanto ad archiviare la documentazione relativa alla Segnalazione interna, ricevuta tramite canale informatico, e alla sua istruttoria in un apposito spazio logico che garantisca con strumenti di crittografia, la riservatezza dell'identità del segnalante.

L'eventuale documentazione cartacea, nonché il Libro Segnalazioni e Istruttorie tenuto dall'OdV deve essere conservato a cura dell'OdV stesso e reso accessibile soltanto ai soggetti autorizzati dalla Società.

Le Segnalazioni interne ricevute sono conservate per il tempo necessario al trattamento delle stesse e, comunque, non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del d.lgs. 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del Regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

A valle di tali termini, l'OdV può mantenere un Registro delle Segnalazioni nel quale devono essere anonimizzati i dati personali relativi alla Persona segnalante, alle Persone coinvolte, indicate come possibili responsabili delle condotte illecite, nonché a coloro che sono a vario titolo coinvolti nella Segnalazione interna, al fine di dare in futuro prova dell'adeguata gestione delle Segnalazioni di Violazioni, quale requisito di un'efficace attuazione del Modello di prevenzione del rischio di reato ai sensi dell'art. 6 D. Lgs. 231/2001 e conseguente assenza di colpa organizzativa.

10. Reporting

L'OdV rende conto annualmente del corretto funzionamento dei sistemi interni di Segnalazione, riportando nella propria relazione le informazioni aggregate sulle risultanze dell'attività svolta e sul seguito dato alle Segnalazioni interne ricevute.

Nella redazione di tale rendiconto, l'OdV è tenuto a rispettare quanto previsto dalla disciplina sulla tutela dell'identità della Persona segnalante e dalla normativa applicabile in materia di protezione dei dati personali.

11. Casi particolari

Laddove la Segnalazione interna riguardi un componente dell'Organismo di Vigilanza, si segue la procedura standard di cui sopra e il componente oggetto di segnalazione si asterrà dal partecipare ai lavori e alle decisioni dell'OdV.

Nel caso in cui la Segnalazione interna abbia ad oggetto più componenti dell'OdV, deve essere trasmessa al Collegio di Presidenza, tramite consegna al Presidente del CdA dell'eventuale documentazione a supporto.

Il Presidente, sentito anche il Consiglio di Amministrazione e il Collegio Sindacale, dopo aver valutato collegialmente se la Segnalazione interna sia corredata dalle informazioni necessarie per verificarne preliminarmente la fondatezza e poter avviare le successive attività di approfondimento, dà seguito alla stessa eseguendo l'istruttoria anche avvalendosi delle competenze aziendali e, se del caso, di consulenti specializzati, sempre nel rispetto della riservatezza normativamente prevista in materia nonché dal presente documento.

L'istruttoria segue l'iter descritto nella presente procedura.

La decisione in ogni caso spetta al Consiglio di Amministrazione che la formalizza attraverso delibera scritta.

12. Delibere dell'OdV

Il funzionamento dell'OdV è disciplinato all'interno del Regolamento dallo stesso adottato.

In caso di ricezione di una Segnalazione, la convocazione dell'OdV deve avvenire tempestivamente, indicativamente entro 3 giorni dalla notizia del ricevimento della Segnalazione e comunque in un termine utile per garantire il riscontro al Persona segnalante entro 7 giorni.

13. Divulgazione della procedura

La presente procedura è esposta e resa facilmente visibile nei luoghi di lavoro e conoscibile, nonché accessibile anche ai Destinatari che non frequentano i luoghi di lavoro della Società, anche per il tramite della sua pubblicazione in una sezione dedicata del sito internet della Società.

ALLEGATO 1 - MODULO DI SEGNALAZIONE

MODULO DI SEGNALAZIONE WHISTLEBLOWING

Si raccomanda di allegare tutta la documentazione che si ritenga possa essere utile a corroborare la Segnalazione; qualora la Segnalazione avvenga verbalmente, tale documentazione può essere consegnata direttamente.

DATI DELLA PERSONA SEGNALANTE

Nome e Cognome

_____

Struttura di appartenenza e qualifica

_____

Canali di contatto prescelti (p.e.c, indirizzo mail privato, numero di telefono, etc)

_____

La Persona segnalante ha un interesse privato collegato alla Segnalazione? Si No

Specificare la natura dell'interesse privato collegato alla Segnalazione

_____
_____
_____
_____
_____
_____
_____
_____

La Persona segnalante è corresponsabile delle violazioni che segnala? Si No

Interni	

Descrizione del fatto oggetto di segnalazione

_____
_____
_____
_____
_____
_____

Altri soggetti che possono riferire sui fatti oggetto di Segnalazione

Interni	

Altri soggetti ai quali è stata inoltrata la Segnalazione del fatto? Si No

Specificare quali soggetti e quando

_____
_____
_____
_____
_____
_____

Data _____ **Firma**_____

ALLEGATO 2: INFORMATIVA PRIVACY PER LA PERSONA SEGNALANTE

ai sensi dell'art. 13 del Regolamento (UE) 2016/679 relativa al trattamento di dati personali nell'ambito della segnalazione di violazioni di cui al d.lgs.24/23

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito "GDPR") e della normativa applicabile in materia di protezione dei dati personali La informiamo che i dati personali forniti in qualità di Persona Segnalante (di seguito anche "Interessato") attraverso il presente "Modulo di Segnalazione" o comunque forniti in caso di segnalazione interna di una violazione ai sensi del D.lgs. 24/2023, saranno trattati, nel rispetto della normativa sopra richiamata e conformemente ai principi di correttezza, liceità e trasparenza da personale autorizzato da INAS CISL ai sensi dell'articolo 29 del GDPR e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali (D.lgs. 196/2003)

1. Titolare del trattamento e Responsabile della protezione dei dati

Titolare del trattamento dei dati personali è Mondialpol s.p.a. (di seguito anche "Società" o "Titolare", in persona del Legale Rappresentante pro tempore, con sede legale Blocco A, Zona industriale Centro Servizi ASI, 90018 Termini Imerese PA;

2. Finalità del trattamento e base giuridica

I dati personali sono trattati per la gestione delle segnalazioni interne di presunte violazioni, ovvero di comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, definiti dall'art. 2 co. 1 lett. a) del d.lgs. 24/23, delle quali la Persona Segnalante sia venuta a conoscenza in ragione del proprio rapporto di collaborazione con il Titolare. I dati personali trattati sono quelli contenuti nella segnalazione interna, e/o in atti e documenti a questa allegati che si riferiscono alla Persona Segnalante.

I dati personali possono essere altresì trattati per lo svolgimento delle necessarie attività istruttorie volte a verificare la fondatezza di quanto segnalato, nonché, se del caso, per l'adozione di adeguate misure correttive e l'introduzione di opportune azioni disciplinari e/o giudiziarie nei confronti dei responsabili delle violazioni. La base giuridica che legittima il trattamento dei dati personali è rappresentata dall'adempimento di un obbligo legale al quale è soggetto il Titolare (Art. 6 comma 1, lett. c) del GDPR), e nello specifico, previsto dal D.lgs. 165/2001, dal D.lgs. 231/2001, dalla L. 179/2017 e dal D.lgs. 24/2023. Il trattamento potrà eventualmente riguardare anche dati particolari e dati relativi a condanne penali e reati qualora inclusi nella segnalazione secondo quanto disposto dagli articoli 9 e 10 del GDPR.

3. Categorie di destinatari dei dati

I dati personali forniti saranno trattati dai componenti dell'Organismo di Vigilanza (OdV), in qualità di soggetti autorizzati al trattamento dal Titolare, al fine di dare seguito e riscontro alle segnalazioni ricevute, in ottemperanza a quanto previsto dal D. Lgs 24/2023 e dal Modello di Organizzazione, Gestione e Controllo ai sensi dell'art. 6 del D. Lgs. 231/01.

Nel caso in cui la Società affidi ad un soggetto terzo l'incarico di gestione del canale di segnalazione, i suddetti dati personali saranno tratti da tale soggetto in qualità di Responsabile del trattamento designato dal Titolare ai sensi dell'art. 28 del GDPR. Tali dati saranno trattati esclusivamente per il tramite di personale espressamente autorizzato e nel rispetto di quanto previsto dal D.lgs. n. 24/2023.

I dati personali non saranno soggetti a diffusione ma potranno essere trasmessi all'Autorità Giudiziaria Nessuno dei dati raccolti sarà trasferito verso Paesi Terzi, intesi quali Paesi non appartenenti allo Spazio Economico Europeo (SEE). Qualora la segnalazione sia esterna e venga presentata, come previsto dagli artt. 6 e 7 del d.lgs. 24/2023, all'Autorità Nazionale Anticorruzione (ANAC), le informazioni relative al trattamento dei dati personali verranno fornite dall'Autorità stessa mediante gli appositi canali.

4. Criteri dei tempi di conservazione

Le segnalazioni interne e la relativa documentazione saranno conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente d.lgs. 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del GDPR e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018. Decorso il periodo massimo di cinque anni le informazioni riferite alla segnalazione potranno essere conservate dalla Società al fine di garantire e preservare il proprio diritto di difesa e dare prova, ove richiesto, della corretta gestione delle segnalazioni ricevute. In tal caso i dati personali della Persona segnalante saranno anonimizzati.

5. Modalità di trattamento dei dati

Il trattamento dei dati personali verrà effettuato esclusivamente da personale espressamente autorizzato, con modalità tali da garantire la riservatezza dell'identità della Persona Segnalante e del contenuto delle segnalazioni interne e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d'integrità e riservatezza, anche accidentali. Al fine di garantire la riservatezza della Persona Segnalante per tutta la durata della gestione della segnalazione interna, l'identità della stessa sarà conosciuta dai soggetti espressamente autorizzati alla gestione delle segnalazioni. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del c.c. ovvero, ove applicabile, nell'ambito del procedimento penale e nei modi e limiti di quanto previsto dall'art. 329 c.p.p., l'identità della Persona Segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità della Persona Segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.

6. Conferimento dei dati

Il conferimento dei dati personali è facoltativo. Il mancato conferimento potrebbe tuttavia pregiudicare l'istruttoria della segnalazione: le segnalazioni anonime, infatti, verranno prese in considerazione solo ove si presentino adeguatamente circostanziate e rese con dovizia di particolari, in modo da far emergere fatti e situazioni connessi a contesti determinati.

7. Diritti degli interessati

I diritti di cui agli articoli 15-22 del GDPR possono essere esercitati, nei limiti di quanto previsto dall'art. 2-undecies, co. 3, del d.lgs. n. 196/2003, rivolgendosi al Titolare o al DPO mediante i contatti sopra indicati. In particolare, i diritti sopra individuati non possono essere esercitati con richiesta al Titolare o al DPO, ovvero con reclamo ai sensi dell'articolo 77 del GDPR all'Autorità Garante, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte. L'esercizio dei suddetti diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo dal Titolare, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi della Persona Segnalante, della Persona coinvolta o delle persone a vario titolo coinvolti nelle segnalazioni. In tali casi, ai sensi dell'art. 2-undecies, co. 3, del decreto legislativo n. 196/2003 l'Interessato ha facoltà di esercitare i succitati diritti tramite l'Autorità Garante con le modalità di cui all'art. 160 del predetto decreto legislativo. Nei casi in cui si ritenga che il trattamento dei dati personali avvenga in violazione di quanto previsto dal GDPR, è possibile proporre reclamo all'Autorità Garante, come previsto dall'art. 77 del GDPR stesso (con esclusione delle limitazioni all'esercizio dei diritti sopra riportate e previste dall'art. 2-undecies, co. 3, del d.lgs. n. 196/2003), o di adire le opportune sedi giudiziarie (art. 79 del GDPR).