

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO**
ai sensi del Decreto Legislativo 8 giugno 2001 n. 231
di
**COMPAGNIE FRANCAISE D'ASSURANCE POUR LE
COMMERCE EXTERIEUR S.A.**

Approvato dal Preposto della Sede Secondaria (Country Manager) il 31/10/2023

Versione 5 – luglio 2023

1

SOMMARIO

Premessa	14
Finalità del Modello	15
Struttura del Modello	16
Destinatari del Modello	17
PARTE GENERALE	19
1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231	19
1.1. IL D.LGS. 231/2001 E LA NORMATIVA DI RIFERIMENTO	19
1.2. I REATI CHE DETERMINANO LA RESPONSABILITA' AMMINISTRATIVA	21
1.3 LE SANZIONI A CARICO DELL'ENTE	21
1.4 L' ESONERO DA RESPONSABILITA'	22
1.5 LE LINEE GUIDA ANIA	25
2. LA RESPONSABILITA' DA REATO NEI GRUPPI DI IMPRESE	26
3. LE VICENDE MODIFICATIVE DELL'ENTE	33
4 LA COSTRUZIONE DEL MODELLO	34
4.1 L'INDIVIDUAZIONE DELLE AREE A RISCHIO	34
4.2 ANALISI DEL SISTEMA DI CONTROLLO INTERNO	34
4.3 STESURA DELLA PARTE SPECIALE DEL MODELLO	39
4.4 GAP ANALYSIS	40
4.5 MANUTENZIONE ED AGGIORNAMENTO DEL MODELLO	40
5 COFACE SA E L'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO	40
5.1. PREMESSA: DESCRIZIONE DI COFACE SA E DELLE AREE DI ATTIVITÀ	40
5.2 STRUTTURA ORGANIZZATIVA, DI GESTIONE E DI CONTROLLO DI COFACE SA	42
5.3 INDIVIDUAZIONE DELLE ATTIVITÀ A RISCHIO E DEFINIZIONE DEI PROTOCOLLI: METODOLOGIA DI LAVORO	43
5.3.1. PRIMA FASE: RACCOLTA E ANALISI DI TUTTA LA DOCUMENTAZIONE ESSENZIALE	43
5.3.2. SECONDA FASE: IDENTIFICAZIONE DELLE ATTIVITÀ A RISCHIO	43
5.3.3. TERZA FASE: INDIVIDUAZIONE E ANALISI DEGLI ATTUALI PRESIDI AL RISCHIO	44

5.3.4. QUARTA FASE: GAP ANALYSIS	44
5.3.5. QUINTA FASE: DEFINIZIONE DEI PROTOCOLLI	44
5.4. AGGIORNAMENTO DEL MODELLO.....	45
6. L'ORGANISMO DI VIGILANZA.....	46
6.1. STRUTTURA E COMPOSIZIONE DELL'ORGANISMO DI VIGILANZA.....	46
a) Autonomia e indipendenza	46
b) Professionalità	47
c) Onorabilità.....	47
d) Continuità d'azione	48
6.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA.....	49
6.3. REPORTING DELL'ORGANISMO DI VIGILANZA	52
6.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA.....	52
6.4.1. Flussi informativi verso gli Organi societari ed i Vertici aziendali.....	52
6.4.2. Flussi informativi verso l'Organismo di Vigilanza	53
6.4.3. Whistleblowing protection (protezione delle segnalazioni).....	53
7. IL SISTEMA SANZIONATORIO	56
7.1. STRUTTURA E FUNZIONE DEL SISTEMA SANZIONATORIO	56
7.1.1 Violazione del Modello: le condotte rilevanti	58
7.1.2. Principi generali di commisurazione delle sanzioni.	60
7.1.3. Sanzioni applicabili ai Dipendenti	60
a) Biasimi verbali, biasimi scritti, multe e sospensioni.....	61
b) Licenziamento	61
7.1.4. Sanzioni applicabili ai Dirigenti	62
7.1.5. Misure nei confronti degli Agenti	63
7.1.6. Sanzioni a carico dei Consulenti, agenti, collaboratori e soggetti terzi.	63
6.1.6. Sanzioni nei confronti degli Amministratori e del Preposto della Sede Secondaria.	64
6.1.7. Misure applicabili nei confronti dei membri dell'Organismo di Vigilanza.....	64
7.2. PROCEDURA PER L'ACCERTAMENTO DELLA VIOLAZIONE, CONTESTAZIONE DISCIPLINARE E IRROGAZIONE DELLE SANZIONI	64
7.2.1 Dovere di segnalazione degli illeciti e procedura disciplinare	65
8. INFORMAZIONE E FORMAZIONE DEL PERSONALE	66
8.1 Premessa.....	66
8.2 Formazione e comunicazione ai destinatari	66
8.3 Comunicazione al pubblico.....	67
PARTE SPECIALE.....	68
1. PREMESSE.....	68
1.1. I presidi messi in atto allo scopo di ostacolare il compimento di condotte illecite	69

1.2. I comportamenti a carico dei destinatari.....	71
1.3. L'attività dell'Organismo di Vigilanza	72
I REATI PRESUPPOSTO RILEVANTI PER COFACE SA.....	75
A) REATI IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ARTT. 24 E 25 D.LGS. 231/2001).....	75
1.1. Malversazione a danno dello Stato o della Unione Europea (art. 316 <i>bis</i> Cod. Pen.) 75	75
1.2. Indebita percezione di erogazioni in danno dello Stato o della UE (art. 316 <i>ter</i> Cod. Pen.) 75	75
1.3. Truffa aggravata in danno dello Stato o di altro ente pubblico o delle Comunità Europee (art. 640, comma 2, n. 1 Cod. Pen.).....	76
1.4. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 <i>bis</i> Cod. Pen.)	76
1.5. Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 <i>ter</i> Cod. Pen.)	76
1.6 Frode nelle pubbliche forniture (art. 356 Cod. Pen.).....	77
1.7. Concussione (art. 317 Cod. Pen.)	77
1.8. Corruzione per l'esercizio della funzione (Art. 318 Cod. Pen.)	77
1.9. Corruzione per un atto contrario ai doveri d'ufficio (Art. 319 Cod. Pen.)	78
1.10. Corruzione in atti giudiziari (Art. 319 <i>ter</i> Cod. Pen.)	78
1.11. Induzione indebita a dare o promettere utilità (Art. 319 <i>quater</i> Cod. Pen.)	79
1.12. Corruzione di persona incaricata di un pubblico servizio (Art. 320 Cod. Pen.)	79
1.13. Pene per il corruttore (Art. 321 Cod. Pen.)	79
1.14. Istigazione alla corruzione (Art. 322 Cod. Pen.)	79
1.15. Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati Esteri (Art. 322 <i>bis</i> Cod. Pen.)	79
1.16. Traffico di influenze illecite (art. 346-bis Cod. Pen.)	80
1.17. Peculato (art. 314 comma 1 Cod. Pen.)	81
1.18. Peculato mediante profitto altrui (art. 316 Cod. Pen.).....	81
1.19. Abuso d'ufficio (art. 323 Cod. Pen.).....	81
2. LE ATTIVITA' A RISCHIO REATO	81
2.1 Possibili modalità attuative.	83
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	84
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	85
4.1. Protocolli Generici.....	85
4.2. Protocolli Specifici:	85
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	86
B) DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24-BIS D.LGS. 231/2001).....	86

Delitti informatici	87
1.1 Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 <i>bis</i> Cod. Pen.)	88
1.2 Accesso abusivo ad un sistema informatico (art. 615 <i>ter</i> Cod. Pen.)	89
1.3 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 <i>quater</i> Cod. Pen.)	90
1.4. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 <i>quinquies</i> Cod. Pen.)	90
1.5. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 <i>quater</i> Cod. Pen.)	90
1.6. Installazione, diffusione e installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 <i>quinquies</i> Cod. Pen.)	91
1.7 Danneggiamento di informazioni, dati e programmi informatici (art. 635 <i>bis</i> Cod. Pen.)	91
1.8 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 <i>ter</i> Cod. Pen.)	91
1.9 Danneggiamento di sistemi informatici o telematici (art. 635 <i>quater</i> Cod. Pen.)	91
1.10 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 <i>quinquies</i> Cod. Pen.)	92
1.11 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 <i>quinquies</i> Cod. Pen.)	92
2. LE ATTIVITA' A RISCHIO REATO	92
2.1 Possibili modalità attuative.	93
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	93
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	93
4.1. Protocolli Generici	93
4.2. Protocolli Specifici:	95
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	95
C) DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER).....	96
1.1 Associazione per delinquere (art. 416 Cod. Pen.)	96
1.2 Associazione di tipo mafioso anche straniera (art. 416 <i>bis</i> Cod. Pen.)	97
1.3 Scambio elettorale politico-mafioso (art. 416 <i>bis</i> Cod. Pen.)	97
1.4. Sequestro di persona a scopo di estorsione (art. 630 Cod. Pen.)	98
1.5. Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 309/1990)	98
2. LE ATTIVITA' A RISCHIO REATO	98
2.1 Possibili modalità attuative.	99
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	99
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	100

4.1. Protocolli Generici.....	100
4.2. Protocolli Specifici:	101
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	101
D) FALSITA' IN MONETE, IN CARTE DI CREDITO, IN VALORI DI BOLLO E SEGNI DI RICONOSCIMENTO (ART. 25-BIS D.LGS. 231/2001)	101
1.1 Spendita di monete falsificate ricevute in buona fede (Art. 457 Cod. Pen.).....	101
1.2 Uso di valori di bollo contraffatti o alterati	102
2. LE ATTIVITA' A RISCHIO REATO	102
2.1 Possibili modalità attuative.	102
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	102
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	103
4.1. Protocolli Generici.....	103
4.2. Protocolli Specifici:	103
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	103
E) DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO (ART. 25-BIS 1 D.LGS. 231/2001) ...	104
1.1 Turbata libertà dell'industria o del commercio (art. 513 c.p.)	104
1.2 Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.).....	104
2. LE ATTIVITA' A RISCHIO REATO	105
2.1 Possibili modalità attuative.	105
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	105
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	105
4.1. Protocolli Generici.....	105
4.2. Protocolli Specifici:	106
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	106
F) I REATI SOCIETARI (ART. 25 TER)	106
1.1. False comunicazioni sociali (art. 2621 Cod. Civ.)	107
1.2. False comunicazioni sociali delle società quotate (art. 2622 Cod. Civ.).....	107
1.3. Impedito controllo (Art. 2625 Cod. Civ.).....	108
1.4. Indebita restituzione dei conferimenti (Art. 2626 Cod. Civ.)	109
1.5. Illegale ripartizione degli utili e delle riserve (Art. 2627 Cod. Civ.).....	109
1.6. Illecite operazioni sulle azioni o quote sociali o della società controllante (Art. 2628 Cod. Civ.)	110
1.7. Operazioni in pregiudizio dei creditori (Art. 2629 Cod. Civ.).....	111
1.8. Omessa comunicazione del conflitto d'interessi (Art. 2629 bis Cod. Civ.).....	111
1.9. Formazione fittizia del capitale (Art. 2632 Cod. Civ.).....	112
1.10. Indebita ripartizione dei beni sociali da parte dei liquidatori (Art. 2633 Cod. Civ.) ..	112
1.11. Illecita influenza sull'assemblea (Art. 2636 Cod. Civ.).....	113
1.12. Aggiotaggio (Art. 2637 Cod. Civ.)	113

1.13. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (Art. 2638 Cod. Civ.)	113
1.14. False o omesse dichiarazioni per il rilascio del certificato preliminare (Art. 54 D.lgs. 19/2023)	114
1.15. Corruzione tra privati (art. 2635 c. c.)	114
1.16. Istigazione alla corruzione tra privati (art. 2635 bis Cod. Pen.)	114
2. LE ATTIVITA' A RISCHIO REATO	115
2.1 Possibili modalità attuative.	116
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	117
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	117
4.1. Protocolli Generici	117
4.2. Protocolli Specifici:	118
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	118
G) ABUSI DI MERCATO (ART. 25-SEXIES D.LGS. 231/2001)	119
1.1 Manipolazione del mercato (Art. 185 D.lgs. 58/1998)	119
1.2. Abuso o comunicazione illecita di informazioni privilegiate (Art. 184 D.lgs. 58/1998)	119
2. LE ATTIVITA' A RISCHIO REATO	121
2.1 Possibili modalità attuative.	121
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	121
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	122
4.1. Protocolli Generici	122
4.2. Protocolli Specifici:	122
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	122
H) REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO (ART. 25-SEPTIES D.LGS. 231/2001)	123
1.1 Omicidio colposo (art. 589 Cod. Pen.)	123
1.2 Lesioni colpose gravi o gravissime (art. 590 Cod. Pen.)	123
2. LE ATTIVITA' A RISCHIO REATO	124
2.1 Possibili modalità attuative.	124
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	125
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	125
4.1. Protocolli Generici	125
4.2. Protocolli Specifici:	126
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	126

I) REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ DI AUTORICICLAGGIO E TERRORISMO (ARTT. 25-OCTIES E 25-QUATER D.LGS. 231/2001)

.....	128
1.1 Ricettazione (art. 648 Cod. Pen.)	128
1.2 Riciclaggio (art. 648-bis Cod. Pen.).....	128
1.3 Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter Cod. Pen.)	129
1.4 Autoriciclaggio (art. 648-ter.1 Cod. Pen.)	129
1.5. Associazioni sovversive (Art. 270 Cod. Pen.)	130
1.6. Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (Art. 270 bis Cod. Pen.).....	130
1.7. Assistenza agli associati (Art. 270 ter Cod. Pen.).....	130
1.8. Arruolamento con finalità di terrorismo anche internazionale (Art. 270 quater Cod. Pen.).....	130
1.9. Addestramento ad attività con finalità di terrorismo anche internazionale (Art. 270 quinquies Cod. Pen.)	130
1.10. Attentato per finalità terroristiche o di eversione (Art. 280 Cod. Pen.).....	131
2. LE ATTIVITA' A RISCHIO REATO	131
2.1 Possibili modalità attuative.	131
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	132
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	132
4.1. Protocolli Generici.....	132
4.2. Protocolli Specifici:	134
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	134
J) INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES D.LGS. 231/2001)	134
1.1. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Art. 377 bis Cod. Pen.).....	134
2. LE ATTIVITA' A RISCHIO REATO	135
2.1 Possibili modalità attuative.	135
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	135
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	135
4.1. Protocolli Generici.....	135
4.2. Protocolli Specifici:	136
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	136
K) REATI AMBIENTALI (ART. 25-UNDECIES D.LGS. 231/2001).....	136
1.1. Inquinamento ambientale (art. 452 bis Cod. Pen.)	136

1.2. Disastro ambientale (art. 452 <i>quater</i> Cod. Pen.).....	137
1.3. Delitti colposi contro l'ambiente (art. 452 <i>quinquies</i> Cod. Pen.)	138
1.4. Attività di gestione di rifiuti non autorizzata (art. 256 D.lgs. 152/2006).....	138
1.5. Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 D.lgs. 152/2006)	138
1.6. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 D.lgs. 152/2006)	139
1.7. Traffico illecito di rifiuti (art. 259 D.lgs. 152/2006).....	139
1.8. Attività organizzate per il traffico illecito di rifiuti (art. 452- <i>quaterdecies</i> Cod. Pen.).....	140
1.9. Sistema informatico di controllo della tracciabilità dei rifiuti	140
1.10. Sanzioni (art. 279 co. 5 D.lgs., 152/2006).....	141
1.11. Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3 co. 6 L. 549/1993)	141
2. LE ATTIVITA' A RISCHIO REATO	141
2.1 Possibili modalità attuative.	141
3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO	142
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	142
4.1. Protocolli Generici.....	142
4.2. Protocolli Specifici:	142
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	143
L) IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES D.LGS. 231/2001).....	143
1.1. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 bis D.lgs. 286/1998).....	143
2. LE ATTIVITA' A RISCHIO REATO	144
2.1 Possibili modalità attuative.	144
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	144
4.1. Protocolli Generici.....	144
4.2. Protocolli Specifici:	145
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	145
M) REATI TRIBUTARI (ART. 25-QUINQUEDECIES D.LGS. 231/2001).....	146
1.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. 74/2000)	146
1.2. Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)	146
1.3. Dichiarazione infedele (art. 4 D. Lgs. 74/2000)	147
1.4. Omessa dichiarazione (art. 5 D. Lgs. 74/2000)	148
1.5. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D. Lgs. 74/2000).....	148
1.6. Occultamento o distruzione di documenti contabili (art. 10 D. Lgs. 74/2000)	149

1.7. Inedita compensazione (art. 10 <i>quater</i> D. Lgs. 74/2000).....	149
1.8. Sottrazione fraudolenta al pagamento di imposte (art. 11 D. Lgs. 74/2000).....	150
2. LE ATTIVITA' A RISCHIO REATO	150
2.1 Possibili modalità attuative.	151
4 I PROTOCOLLI PER MITIGARE IL RISCHIO	151
4.1. Protocolli Generici.....	151
4.2. Protocolli Specifici:	151
5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA	152

ELENCO ALLEGATI PARTE GENERALE

- [Allegato 1](#) – Visura Camerale;
- [Allegato 2](#) – Codice di Condotta COFACE;
- [Allegato 3](#) – Organigramma Aziendale;
- [Allegato 4](#) – Decreto Legislativo 231/2001;
- [Allegato 5](#) – Linee Guida Confindustria (giugno 2021);
- [Allegato 6](#) – Elenco Reati Presupposto 231 aggiornato al 22/03/2023;
- [Allegato 7](#) – Procedura di Whistleblowing;
- [Allegato 7-bis](#) – Procedura Ombudsman

ELENCO ALLEGATI PARTE SPECIALE

- [Allegato A](#) – Procedure prevenzione reati ex artt. 24 e 25 D.lgs. 231/2001;
- [Allegato A-bis](#) – Codice Anticorruzione;
- [Allegato A-ter](#) – Gifts & Benefits Procedure;
- [Allegato B](#) – Procedure prevenzione reati ex art. 24-bis D.lgs. 231/2001;
- [Allegato C](#) – Procedure prevenzione reati ex art. 24-ter D.lgs. 231/2001;
- [Allegato D](#) – Procedure prevenzione reati ex art. 25-bis D.lgs. 231/2001;
- [Allegato E](#) – Procedure prevenzione reati ex art. 25-bis 1 D.lgs. 231/2001;
- [Allegato F](#) – Procedure prevenzione reati ex art. 25-ter D.lgs. 231/2001;
- [Allegato G](#) – Procedure prevenzione reati ex art. 25-sexies D.lgs. 231/2001;
- [Allegato H](#) – Procedure prevenzione reati ex art. 25-septies D.lgs. 231/2001;
- [Allegato I](#) – Procedure prevenzione reati ex artt. 25-octies e 25-quater D.lgs. 231/2001;
- [Allegato J](#) – Procedure prevenzione reati ex art. 25-decies D.lgs. 231/2001;
- [Allegato K](#) – Procedure prevenzione reati ex art. 25-undecies D.lgs. 231/2001;
- [Allegato L](#) – Procedure prevenzione reati ex art. 25-duodecies D.lgs. 231/2001;

- [Allegato M](#) – Procedure prevenzione reati ex art. 25-quinquedecies D.lgs. 231/2001;
- [Allegato N](#) – Procedura KYC – Know Your Customers procedure;
- [Allegato O](#) – Procedura KYS – Know Your Supplier procedure;
- [Allegato P](#) – Procedura IFRS 17;
- [Allegato Q](#) – Procedura IFRS 15;
- [Allegato R](#) – Procedura IFRIC 23;
- [Allegato S](#) – Procedura “Costi e Disposizioni per la Gestione di Sinistri di Recupero”;
- [Allegato T](#) – Procedura “Calcolo Imposte Differite”;
- [Allegato U](#) – Procedura “Operazioni in Valuta Estera”;
- [Allegato V](#) – “Cybersecurity Process”;
- [Allegato W](#) – “Data Management Policy”;
- [Allegato X](#) – “Claims Group Rules on dual use items”;
- [Allegato Y](#) – “Sanctioned Companies and Countries under Sanctions”;
- [Allegato Z](#) – “Cash Management Group Rules”.

DEFINIZIONI

Nel presente documento e nei relativi allegati, le seguenti espressioni hanno il significato ivi indicato:

- “**Compagnie française d’assurance pour le commerce extérieur S.A.**” (di seguito “**Coface SA**” o “**Società**” o “**Compagnia**”): Società oggetto del presente Modello, come meglio individuata sub [Allegato 1](#).
- “**Area a rischio di reato**”: l’area o la funzione aziendale nell’ambito della quale sono svolte le attività a rischio commissione reati presupposto ex D.lgs. 231/2001.
- “**Attività a rischio di reato**” o “**Attività sensibile**”: il processo, l’operazione, l’atto, ovvero l’insieme di operazioni e atti, che possono costituire occasione o strumento di realizzazione dei reati/illeciti di cui al D. Lgs. 231/2001.
- “**Clienti**”: società e soggetti privati ai quali la società offre i servizi e le prestazioni di cui all’oggetto sociale.
- “**Codice di Condotta COFACE**”: il documento, parte integrante del presente Modello, approvato da Coface SA e contenente i valori, i principi e le linee di comportamento che ispirano la politica societaria e l’operatività dell’ente, la cui violazione da parte dei Destinatari è sanzionata ([Allegato 2](#))

- **“Conflitti di interesse”**: è la situazione in cui un interesse personale di uno dei Destinatari può interferire e/o prevalere su quello societario.
- **“Decreto 231” o “Decreto” o “D. Lgs. 231/2001”**: 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 le sue successive modificazioni e/o integrazioni, come allegato sub [Allegato 4](#).
- **“Destinatari”**: tutti i soggetti tenuti al rispetto del presente Modello, di cui fa parte integrante il Codice di Condotta COFACE. A titolo meramente esemplificativo e non esaustivo, sono da considerarsi destinatari, i dipendenti della Società, i componenti dell’Organo Amministrativo, i consulenti esterni e chiunque, a qualunque titolo, presti la propria attività lavorativa in favore di Coface SA.
- **“Enti”**: soggetti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica, con esclusione dello Stato, degli enti pubblici territoriali, altri enti pubblici non economici nonché enti che svolgono funzioni di rilievo costituzionale.
- **“Incaricato di pubblico servizio”**: la definizione di incaricati di un pubblico servizio può essere ricavata dall’art. 358 c.p., il quale li definisce come *“coloro i quali, a qualunque titolo, prestano un servizio pubblico. Per servizio pubblico deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”*. Essa, quindi, si differenzia da un pubblico ufficiale, in quanto non è dotata di poteri autoritativi e certificativi.

A titolo meramente esemplificativo, rivestono la qualifica di incaricato di pubblico servizio i seguenti soggetti: esattori di ENEL, lettoristi dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento della corrispondenza, dipendenti del Poligrafico dello Stato, guardie giurate che conducono furgoni portavalori.

- **“Istituzioni Pubbliche”**: sono, a titolo esemplificativo e non esaustivo le amministrazioni dello Stato (compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative), le aziende e le amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di Commercio, industria, artigianato e agricoltura, gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale. La funzione pubblica è rivestita anche dai membri della Commissione Europea, del Parlamento Europeo, della Corte di Giustizia dell’Unione Europea e della Corte dei Conti europea, dai funzionari e dagli agenti assunti a contratto a norma dello statuto dei funzionari dell’Unione europea, dalle persone comandate dagli Stati membri o da qualsiasi ente

pubblico o privato presso l'Unione Europea che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle comunità europee, i membri o gli addetti a enti costituiti sulla base dei trattati che istituiscono l'Unione Europea.

- **“Linee Guida”**: le linee guida pubblicate dalle associazioni di categoria per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex Decreto 231. Nello specifico, ai fini della predisposizione e adozione del presente Modello sono state prese in considerazione quelle emanate da Confindustria in data 07.02.2002, aggiornate nel marzo 2014 e nel giugno 2021 come allegate sub [Allegato 5](#), nonché le Linee Guida ANIA (Associazione Nazionale fra le Imprese Assicuratrici) emanate nel 2002 e successivamente aggiornate nel 2006 e nel 2008.
- **“Modello di organizzazione, gestione e controllo ai sensi del Decreto 231”** o **“Modello 231”** o **“Modello”**: il Modello di organizzazione, gestione e controllo adottato dal Preposto della Sede Secondaria di Coface SA, ai sensi degli articoli 6 e 7 del Decreto, al fine di prevenire la consumazione dei “reati presupposto” individuati dal D.lgs. 231/2001, da parte del Personale Apicale o del Personale sottoposto ad altrui direzione, nonché dei Destinatari in generale, così come descritto dal presente documento e dai relativi allegati;
- **“Organismo di Vigilanza”** o **“OdV”**: l'Organismo previsto dall'art. 6 del Decreto, avente il compito di vigilare sull'efficacia e sull'effettività del Modello di organizzazione, gestione e controllo, nonché sull'aggiornamento dello stesso.
- **“P.A.”**: la Pubblica Amministrazione. Rientrano nel concetto di Pubblica Amministrazione le Istituzioni Pubbliche, i Pubblici Ufficiali e gli Incaricati di pubblico servizio.
- **“Protocollo specifico”**: la misura organizzativa fisica e/o logica, prevista dal Modello per governare i profili di rischio individuati in relazione alla commissione dei reati presupposto di cui al Decreto.
- **“Protocollo generico”**: l'insieme di regole e di principi di controllo e di comportamento previsti dal Modello per governare genericamente i profili di rischio di realizzazione di tutti i Reati di cui al Decreto.
- **“Pubblico Ufficiale”**: ai sensi dell'art. 357 Cod. Pen.: *“Agli effetti della legge penale sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa”. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”*.
- **“Reati”** o **“Reato”**: sono quelle condotte idonee a costituire il presupposto dell'illecito amministrativo attribuibile all'Ente e a fondare, di conseguenza, la responsabilità

amministrativa derivate da reato in capo all'Ente stesso ex D.lgs. 231/2001 e sue successive modificazioni e integrazioni ([Allegato 6](#))

- **“Sistema Disciplinare”**: l’insieme delle misure sanzionatorie applicabili in caso di violazione delle regole procedurali e comportamentali previste dal Modello, nel rispetto di quanto previsto dal CNNL di riferimento e dallo Statuto dei Lavoratori.
- **“Statuto dei Lavoratori”**: la Legge 20 maggio 1970, n. 300, recante le *“Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale nei luoghi di lavoro e norme sul collocamento”*, pubblicata in Gazzetta Ufficiale n. 131 del 27 maggio 1970, e successive modificazioni e integrazioni.

PREMESSA

“La Viscontea Compagnia di Assicurazione e Riassicurazione S.p.A.” viene costituita il 23/11/1987, con l’iniziale obiettivo di inserirsi nel mercato assicurativo dei rami Credito e Cauzione. Dopo aver raggiunto in entrambi tali settori una posizione di assoluto rilievo, nel 1994 la Società entra a far parte del Gruppo assicurativo francese COFACE SA, leader internazionale nell’assicurazione e nella gestione dei crediti commerciali, mutando nel 2002 ragione sociale in Viscontea Coface S.p.A., ed assumendo poi, a far data dal gennaio 2006, la denominazione di Coface Assicurazioni S.p.A.

Nel dicembre 2010 Coface Service S.p.A., società che fino ad allora aveva prestato servizi accessori all’attività assicurativa, quali ad esempio la gestione dei servizi informatici, è stata fusa per incorporazione in Coface Assicurazioni S.p.A. In data 31/10/2012, a seguito del completamento di un processo di fusione per incorporazione iniziato con l’acquisizione da parte della già controllante Coface S.A. dell’intero capitale sociale di Coface Assicurazioni S.p.A., quest’ultima cessa di esistere assumendo contestualmente la denominazione di Compagnie française d’assurance pour le commerce extérieur S.A. con Sede Secondaria e Rappresentanza Generale per l’Italia in Milano, di seguito “Coface SA”.

Il marchio Coface è presente in Italia, oltre che con la società di assicurazioni, anche con Coface Italia S.r.l., quest’ultima attiva nell’ambito dei settori di ricerca e raccolta di informazioni commerciali, e di recupero dei crediti sia per conto della clientela assicurata che per conto terzi. Nell’esercizio della sua attività d’impresa la Sede Secondaria Italiana utilizza una consolidata e competente rete di intermediari assicurativi, e si avvale - per la distribuzione dei propri prodotti - anche della collaborazione di brokers e di istituti di credito.

Il presente Modello di Organizzazione e Gestione e Controllo è adottato dalla Sede Secondaria italiana di Compagnie française d’assurance pour le commerce extérieur. Quanto alla struttura aziendale, si rinvia all’organigramma aziendale¹ ([Allegato 3](#)) ove trovano dettagliata descrizione

¹ Cfr. <https://www.coface.it/A-proposito-di-Coface/Coface-in-Italia/Coface-in-Italia>

sia l'organizzazione dell'Ente nel suo complesso, che le specifiche aree operative e le funzioni da esse svolte.

Il presente documento rappresenta il Modello di Organizzazione, Gestione e Controllo ex Decreto Legislativo 231/2001 adottato da Coface SA, in cui sono individuate le attività aziendali ritenute a rischio commissione reati-presupposto, nonché le procedure e i protocolli finalizzati a limitare e prevenire il rischio di consumazione di tali illeciti penali.

La Società, al fine di garantire trasparenza e correttezza nella conduzione degli affari e nelle attività aziendali, ha ritenuto, infatti, necessario implementare un sistema di controllo interno, atto alla prevenzione e limitazione della commissione di reati connessi all'attività aziendale.

La presente edizione del Modello è la quinta versione adottata dalla Società ed è stata approvata dal Preposto della Sede Secondaria, in data 31/10/2023.

FINALITÀ DEL MODELLO

La scelta di Coface SA di provvedere all'elaborazione di un Modello 231 riflette la più ampia politica d'impresa della Società, che persegue le seguenti finalità principali:

- prevenire e limitare i rischi connessi all'attività aziendale, con particolare attenzione alle eventuali condotte illecite che potrebbero comportare una responsabilità amministrativa derivante da reato della Società;
- confermare l'impegno della Società nel contrastare qualsiasi comportamento illecito che possa consumarsi al suo interno o nel suo interesse, condannando le condotte di tal genere;
- sensibilizzare tutti coloro che operano in nome e per conto della Società, nelle aree individuate a "rischio", affinché, nello svolgimento delle proprie attività e mansioni, assumano un comportamento conforme al Modello 231, tale da prevenire la commissione dei reati presupposto;
- comunicare ed informare i Destinatari che, la violazione delle disposizioni del Modello 231 e la commissione dei reati presupposto, comporta, l'applicazione di sanzioni disciplinari, secondo quanto previsto dal sistema sanzionatorio, adottato della Società, le cui regole e sanzioni integrano e non sostituiscono le norme di legge e le clausole della pattuizione collettiva. Eventuali condotte di tal guisa, inoltre, determineranno anche l'irrogazione di sanzioni pecuniarie ed interdittive a carico della Società;
- consentire alla Società, grazie a un'azione di stretto controllo e monitoraggio sulle aree a rischio e sulle attività sensibili rispetto alla potenziale commissione di reati rilevanti ai fini del Decreto e all'implementazione di strumenti ad hoc, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Decidendo di adottare un Modello di Organizzazione, Gestione e Controllo, Coface SA ha dunque voluto creare uno strumento tramite il quale fosse possibile sovrapporre i processi e le regole aziendali alle fattispecie di reato previste dal Decreto, in modo da costruire un efficace sistema di prevenzione ed un efficiente piano di controllo per il monitoraggio dei rischi relativi alla commissione di tali illeciti.

Tale sistema di verifica e controllo è stato realizzato grazie ad una preventiva opera di mappatura dei reati, delle attività e delle procedure aziendali esistenti, nonché delle circolari e degli ordini di servizio emanati nel corso degli anni dalla Compagnia. Ciò ha consentito di evidenziare quali attività aziendali fossero potenzialmente a rischio di illecito, e di programmare gli interventi occorrenti e necessari al perfezionamento del Sistema di Controllo Interno della Compagnia.

L'applicazione di tale criterio nel continuo dell'attività aziendale ha consentito e consente adeguamenti mirati delle procedure interne a supporto delle operatività quotidiane.

Tale struttura si innesta nel più generale apparato di cui la Compagnia si è dotata con l'istituzione, rispettivamente nel 2002, 2006 e 2008 delle funzioni di Internal Auditing, Risk Management, Compliance: tali funzioni di controllo sono a vario titolo incaricate di monitorare e valutare l'efficacia ed efficienza del sistema di controllo nonché le relative necessità di adeguamento, di identificare e valutare i rischi maggiormente significativi, quali ad esempio quelli le cui conseguenze possono minare la solvibilità dell'impresa o costituire un serio ostacolo alla realizzazione degli obiettivi aziendali, ovvero quelli di incorrere in sanzioni per violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza o di norme di autoregolamentazione.

Al fine di adempiere ai compiti di controllo e verifica cui sono preposte, tali funzioni svolgono le rispettive attività di verifica sulla base di una dettagliata programmazione su base annuale; esse sono, inoltre, tenute a rendere informative periodiche alle figure apicali della Compagnia e, in applicazione degli standard della Sede, a trasmettere a quest'ultima regolari report informativi e di analisi.

È di tutta evidenza, dunque, come l'attività di verifica ed il monitoraggio svolti in applicazione del presente Modello e focalizzati sui rischi di commissione degli illeciti previsti dal Decreto, si innesti nel più ampio quadro aziendale di controllo e prevenzione dei rischi globalmente intesi.

STRUTTURA DEL MODELLO

Il presente documento si compone di una Parte Generale e di una Parte Speciale.

La Parte Generale fornisce un quadro sintetico dei contenuti del Decreto e della normativa di riferimento, richiamando le fattispecie di reato che possono determinare la responsabilità amministrativa in capo ad un ente, le possibili sanzioni e le condizioni necessarie affinché vi sia l'esenzione della responsabilità dell'Ente, nonché una descrizione della struttura organizzativa della Società e delle attività svolte per la costruzione, diffusione e aggiornamento del Modello.

La Parte Speciale contiene i Protocolli ovvero un insieme di regole e di principi di controllo e di comportamento ritenuti idonei a governare le aree a rischio di potenziale commissione dei reati presupposto (elenco disponibile sub [Allegato 6](#)).

Più in dettaglio, nella Parte Speciale sono individuate le categorie di reato che, sulla base dell'attività sociale e all'esito dell'attività di Risk Assessment, sono state valutate a rischio consumazione e, per ciascuna di esse, sono individuate le aree aziendali in cui, potenzialmente,

gli illeciti penali potrebbero essere perpetrati. Sono indentificati, dunque, le regole di condotta e i protocolli specifici che i Destinatari del Modello 231 dovranno rispettare nell'adempimento delle proprie attività.

Le regole contenute nel Modello si integrano con quelle del Codice di Condotta COFACE ([Allegato 2](#)) pur presentando il primo, per le finalità che esso intende perseguire, in attuazione delle disposizioni riportate nel Decreto, un obiettivo diverso rispetto ai secondi. Si specifica, infatti, che:

- il **Codice di Condotta COFACE** è un documento adottato in via autonoma dalla Società, contenente l'insieme dei principi e dei valori che ispirano l'attività aziendale, nonché dei principi etici su cui si fonda l'intero operato della Società;
- il **Modello** risponde a specifiche prescrizioni contenute nel D. Lgs. 231/2001, finalizzate a prevenire la commissione dei reati che possono comportare l'attribuzione della responsabilità penale - amministrativa in capo alla Società.

DESTINATARI DEL MODELLO

Il presente Modello si applica a tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione o controllo della Società, nonché ai soci e a tutto il personale dipendente di Coface SA.

Tali soggetti sono:

- il Rappresentante della Sede Secondaria (Country Manager), i Direttori, i Procuratori Speciali, i Responsabili di Funzione;
- i Dirigenti e tutti i Dipendenti che operano sotto la direzione e la vigilanza di uno dei soggetti di cui al punto precedente.

Al fine di garantire un'efficace ed effettiva prevenzione dei reati, sono Destinatari del presente Modello anche i collaboratori esterni, sia persone fisiche (a titolo esemplificativo: consulenti, professionisti, agenti etc.) sia persone giuridiche che, mediante contratto, prestino la propria collaborazione a Coface SA per la realizzazione delle proprie attività.

Allo stesso modo, devono considerarsi Destinatari del presente Modello 231 e del Codice di Condotta COFACE tutti coloro i quali intrattengono con la Compagnia rapporti stabili e continuativi, come le Agenzie componenti la Rete di Distribuzione e Vendita dei prodotti di Coface SA.

Ed invero, tali soggetti, per quanto non appartenenti alla struttura organizzativa aziendale ed essendo quindi entità autonome e distinte rispetto alla Società, svolgono la propria attività lavorativa dell'interesse e/o vantaggio di Coface SA e, pertanto, dovranno conformarsi ai principi ed ai valori fondamentali dettati dalla Società e ai protocolli previsti dal presente Modello 231.

L'eventuale commissione in ambito agenziale di fattispecie delittuose previste dal D.lgs. 231/2001, potrebbe determinare l'insorgere della responsabilità amministrativa in capo a Coface

SA, soprattutto laddove venga accertato che la stessa non abbia adottato specifiche precauzioni utili a limitare e prevenire condotte criminose.

Per tutte queste ragioni, come sarà poi meglio specificato nella Parte Speciale, qualunque azienda intenda sottoscrivere con la Società un rapporto agenziale, o qualsiasi altra tipologia contrattuale, deve assumere l'obbligo di prendere visione e conoscenza nel Modello di Organizzazione, Gestione e Controllo.

Il rispetto del Modello è garantito mediante l'apposizione di una specifica clausola contrattuale che obblighi il contraente ad attenersi ai principi del Modello societario nello svolgimento dell'attività che riguarda l'impresa. Eventuali violazioni nel Modello 231 ad opera di soggetti terzi, potranno comportare come conseguenza la risoluzione del contratto, nonché nei casi di più grave entità ipotesi di risarcimento danno in favore della stessa. Per tali ragioni, le violazioni od elusioni del Modello poste in essere da tali soggetti, come meglio analizzato nel prosieguo di tale Parte Generale e nell'allegata Procedura di Whistleblowing, potranno essere oggetto di Segnalazioni, destinate all'Organismo di Vigilanza e/o all'Organo Amministrativo.

PARTE GENERALE

1. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

1.1. IL D.LGS. 231/2001 E LA NORMATIVA DI RIFERIMENTO

Il Decreto Legislativo n. 231 dell'8 giugno 2001 ([Allegato 4](#)), attuando la legge delega 29 settembre 2000, n. 300, ha introdotto la c.d. “*responsabilità amministrativa*” delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica (enti), adeguando la normativa italiana, in materia di responsabilità delle persone giuridiche, alle convenzioni internazionali vigenti in materia:

- Convenzione di Bruxelles del 26 luglio 1995 sulla tutela finanziaria delle Comunità europee;
- Convenzione di Bruxelles del 26 maggio 1997 alla lotta contro la corruzione;
- Convenzione OCSE del 17 settembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali.

Prima dell'introduzione di tale disciplina legislativa, gli enti collettivi non erano soggetti, secondo la legge nazionale, a responsabilità di tipo c.d. “*penale-amministrativo*” e solo le persone fisiche (ovvero Amministratori, Dirigenti, etc. degli enti) potevano essere perseguite, in caso di commissione di reati nell'interesse dell'ente di appartenenza, senza alcuna sanzione in danno alla Società stessa.

Con l'adozione del Decreto, il legislatore italiano ha ottemperato agli obblighi previsti dalla normativa comunitaria, prevedendo profili di responsabilità “*penale-amministrativa*” delle persone giuridiche e il corrispondente sistema sanzionatorio, che colpisce la criminalità d'impresa in modo più diretto ed efficace.

L'istituzione della c.d. “*responsabilità amministrativa derivante da reato*” delle società muove dalla considerazione empirica secondo cui le condotte illecite commesse all'interno dell'ente, lungi dallo scaturire da un'iniziativa privata del singolo, di sovente rientrano nell'ambito di una diffusa politica aziendale e conseguono a decisioni di vertice dell'ente medesimo.

Sulla natura della responsabilità imputabile alla Società, scaturente dalla consumazione di un reato presupposto, nel suo interesse o a suo vantaggio, va evidenziato come la Giurisprudenza ultima abbia affermato che si tratti di un “*Tertium genus di responsabilità*” che “*coniuga i tratti essenziali del sistema penale e di quello amministrativo, nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle della massima garanzia*”.

L'accertamento dell'illecito amministrativo spetta, ai sensi e per gli effetti dell'art. 36 D.lgs. 231/2001 al Giudice penale, competente per i reati presupposto dal quale esso dipende. La scelta del Legislatore di affidare tale accertamento al Giudice penale è conseguenza della maggiore tutela che il processo penale fornisce all'imputato (persona fisica o giuridica), rispetto al rito civilistico (Es. Assunzione della prova in contraddittorio tra le parti, oralità ed immediatezza, principio del *favor rei*).

La responsabilità degli enti si estende anche ai reati commessi all'estero, nei casi e alle condizioni previste dagli Artt. 7, 8, 9 e 10 c.p., purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

I criteri di attribuzione della responsabilità all'Ente sono **(i)** la commissione di uno dei reati tassativamente individuati dal Decreto da parte di soggetti apicali dell'ente o ad essi sottoposti, **(ii)** nell'*“interesse o a vantaggio della società”*.

Laddove l'autore del reato abbia agito nell'interesse esclusivo proprio o di terzi l'ente non ne risponde, trattandosi di una situazione di manifesta estraneità della persona giuridica rispetto al fatto di reato.

In riferimento ai soggetti autori del reato, il Legislatore, all'articolo 5 del Decreto, individua due categorie:

- a) **Soggetti apicali**, ossia *“persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo degli stessi”*;
- b) **Soggetti sottoposti**, ossia *“persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)”. In particolare, rientrano in tale categoria: i) i dipendenti, ossia i soggetti che hanno con l'Ente un rapporto di lavoro subordinato, nonché ii) tutti quei prestatori di lavoro che, pur non essendo dipendenti dell'Ente, abbiano con esso un rapporto tale da far ritenere sussistente un obbligo di vigilanza da parte dei vertici dell'Ente medesimo, quali, a titolo meramente esemplificativo, i c.d. parasubordinati in genere, gli agenti, i consulenti e i collaboratori.*

Il Decreto è improntato ad una scelta di tipo “funzionalistico”, invece che una di tipo “nominalistico”, riservando, cioè, l'attenzione alla concreta attività svolta dai soggetti, piuttosto che alla qualifica formalmente rivestita all'interno dell'ente e, in tal senso, i soggetti richiamati dall'articolo 5 sono infatti coloro i quali svolgono funzioni inerenti alla gestione e al controllo dell'ente o di sue articolazioni.

Da sottolineare, in questa prospettiva, anche l'equiparazione – rispetto ai soggetti che ricoprono funzioni di rappresentanza, di amministrazione o di direzione dell'ente – delle persone che rivestono le medesime funzioni in una *“unità organizzativa dotata di autonomia finanziaria e funzionale”*. Si tratta, come noto, di una figura sempre più diffusa nella realtà economica attuale, soprattutto nell'ambito di società strutturate su più sedi, e ciò richiede una particolare attenzione al fine di elaborare un Modello Organizzativo che si riveli, nella prassi, realmente efficace.

Ai fini dell'affermazione della responsabilità dell'ente, oltre al verificarsi dei requisiti fin qui richiamati, che consentono di effettuare il c.d. *“collegamento oggettivo”* tra il reato commesso e l'attività dell'ente, il legislatore impone anche l'accertamento di un *“collegamento soggettivo”*, che consiste essenzialmente nella colpevolezza dell'ente per il reato realizzato. Tale presupposto soggettivo è rappresentato da una *“colpa da organizzazione”*, **intesa come carenza organizzativa rispetto ad un modello di diligenza stabilito dalla norma e, quindi,**

consistente nella **mancata adozione ovvero nel carente funzionamento del modello preventivo dei reati**.

L'art. 8 D.lgs. 231/2001, inoltre, afferma il principio di "Autonomia della responsabilità dell'ente", disponendo che sussiste la sua responsabilità anche quando:

- a) l'autore del reato non sia identificato o non sia imputabile;
- b) il reato si estingue per causa diversa dall'amnistia.

1.2. I REATI CHE DETERMINANO LA RESPONSABILITA' AMMINISTRATIVA

In virtù dei principi di tassatività e tipicità che caratterizzano il D.lgs. 231/2001 e l'interno sistema penale, la responsabilità degli Enti è limitata alle sole fattispecie di reato tassativamente indicate nel decreto stesso, o in leggi speciali che fanno riferimento allo stesso articolato normativo, non potendosi operare applicazioni analogiche o estensive di illeciti non espressamente individuati del Decreto, a nulla rilevando l'afferenza o lo stretto collegamento a settori normativi penali, in parte ricompresi nel novero dei suddetti reati.

Nel corso degli anni il catalogo dei reati "presupposto" si è notevolmente ampliato e, attualmente, il Decreto prevede diverse "famiglie" di reato ([Allegato 6](#)).

Peraltro, come si avrà modo di meglio precisare in seguito, non tutti i reati di cui all'[Allegato 6](#) sono stati considerati rilevanti rispetto all'attività svolta dall'Coface SA

1.3 LE SANZIONI A CARICO DELL'ENTE

Il sistema sanzionatorio previsto dal D. Lgs. 231/01 è articolato in quattro tipi di sanzione, cui può essere sottoposto l'ente in caso di condanna ai sensi del Decreto:

- **Sanzione pecuniaria:**
è sempre applicata qualora il giudice ritenga l'Ente responsabile. Essa viene calcolata tramite un sistema basato su quote, che vengono determinate dal Giudice nel numero e nell'ammontare: il numero delle quote, da applicare tra un minimo e un massimo, che varia a seconda della fattispecie, dipende dalla gravità del reato, dal grado di responsabilità dell'ente, dall'attività svolta per eliminare o attenuare le conseguenze del reato o per prevenire la commissione di altri illeciti; l'ammontare della singola quota va invece stabilito, tra un minimo di € 258,00 e un massimo di € 1.549,00, a seconda delle condizioni economiche e patrimoniali dell'Ente.
- **Sanzioni interdittive:**
le sanzioni interdittive si applicano, in aggiunta alle sanzioni pecuniarie, soltanto se espressamente previste per il reato per cui l'Ente viene condannato, e solo nel caso in cui ricorra almeno una delle seguenti condizioni:
 - i) l'Ente ha tratto dal reato un profitto rilevante, e il reato è stato commesso da un Soggetto Apicale, o da un Soggetto Sottoposto qualora in questo caso la

- commissione del reato sia stata determinata o agevolata da gravi carenze organizzative;
- ii) in caso di reiterazione degli illeciti.

Le sanzioni interdittive previste dal Decreto sono così individuabili:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Eccezionalmente applicabili in via definitiva, le sanzioni interdittive sono temporanee (durata non inferiore a tre mesi e non superiore a due anni, tranne nei casi previsti dall'art. 25 comma 5 D.lgs. 231/01) ed hanno ad oggetto la specifica attività dell'Ente cui si riferisce l'illecito. Esse possono essere applicate anche in via cautelare, prima della sentenza di condanna qualora sussistano gravi indizi della responsabilità dell'Ente e fondati e specifici elementi che facciano ritenere concreto il pericolo di ulteriore commissione di illeciti della stessa indole di quello per cui si procede.

- **Confisca:**
con la sentenza di condanna è sempre disposta la confisca del prezzo o del profitto del reato (confisca ordinaria) o di beni o altre utilità di valore equivalente (confisca per equivalente).
Il profitto del reato è stato definito come il vantaggio economico di diretta e immediata derivazione causale dal reato, e concretamente determinato al netto dell'effettiva utilità conseguita dal danneggiato nell'ambito di un eventuale rapporto contrattuale con l'Ente; è stato inoltre specificato che da tale definizione debba escludersi qualsiasi parametro di tipo aziendalistico, per cui il profitto non può essere identificato con l'utile netto realizzato dall'Ente (tranne che nel caso, normativamente previsto, di commissariamento dell'ente).
- **Pubblicazione della sentenza di condanna:**
può essere disposta quando l'Ente è condannato ad una sanzione interdittiva; consiste nella pubblicazione della sentenza una sola volta, per estratto o per intero, in uno o più giornali indicati dal giudice nella sentenza, nonché mediante affissione nel Comune ove l'ente ha la sede principale, ed è eseguita a spese dell'ente.

1.4 L'ESONERO DA RESPONSABILITÀ

Gli artt. 6 e 7 del Decreto prevedono l'esenzione dalla responsabilità amministrativa qualora l'ente si sia dotato di un effettivo ed efficace Modello di Organizzazione, Gestione e Controllo, idoneo a prevenire reati della specie di quello verificatosi. Resta ferma la responsabilità penale personale di chi ha commesso il reato.

Sul punto va chiarito, dunque, come la finalità del Modello 231 sia quella di rendere esente la società da eventuale responsabilità *penale-amministrativa* derivante da reato, senza in alcun modo incidere sulla responsabilità personale dell'autore del reato.

In qualsiasi caso, è evidente come i protocolli e le procedure, individuate nella Parte Speciale del Modello 231, se osservate dai Destinatari, limiteranno la loro possibilità di incorrere in condotte penalmente rilevanti ai sensi del D.lgs. 231/2001.

Dalle norme citate, emerge una differenza di disciplina e di regime probatorio tra i reati commessi dai soggetti in posizione apicale e quelli posti in essere dai sottoposti.

L'art. 6 del Decreto prevede infatti che **l'Ente non risponde dei reati commessi dai soggetti in posizione apicale, qualora l'Ente sia in grado di dimostrare che:**

- a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e sull'osservanza dei modelli, nonché di curare il loro aggiornamento, sia stato affidato ad un Organismo di Vigilanza dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- c) le persone fisiche abbiano commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- d) non vi sia stata un'omessa o insufficiente vigilanza da parte dell'Organismo di cui alla lettera b).

Ai sensi dell'art. 7, per i reati commessi da soggetti sottoposti all'altrui direzione, **l'ente risponde solo se la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza** (in questo caso l'onere della prova è a carico dell'accusa). **In ogni caso, si presuppongono osservati tali obblighi se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.**

Con riferimento al requisito dell'efficacia, l'art. 6 comma 2 del Decreto statuisce che il Modello debba:

- a) individuare le attività nel cui ambito possono essere commessi i reati presupposto (ovvero la c.d. "*mappatura delle attività a rischio*");
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati presupposto;
- d) prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del Modello.

La Legge 179/2017, inoltre, introducendo il comma 2 bis all'art. 6, modificato, poi, dal D.lgs. 24/2023, ha previsto che, i Modelli devono sempre prevedere un canale di segnalazione interno che consenta ai Destinatari dello stesso di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su

elementi di fatto precisi e concordanti, o di violazioni del Modello di Organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Come previsto dalla recente normativa, destinatario della Segnalazione deve essere un soggetto o un ufficio all'uopo deputato, dotato di specifiche conoscenze e competenze nel settore.

Nel caso di specie, Coface SA ha attribuito tale funzione all'Organismo di Vigilanza.

Ulteriore importante novità introdotta dal D.lgs. 24/2023 è l'estensione delle misure di protezione, previste già in favore del Segnalante, anche ad altri soggetti quali:

- Liberi professionisti e consulenti;
- Volontari e tirocinanti;

- Facilitatori, da intendersi coloro i quali assistano il Segnalante nel processo di segnalazione ed operanti nel medesimo contesto lavorativo;
- Persone del medesimo contesto lavorativo del Segnalante e a lui legate da uno stabile legame affettivo o di parentela entro il quarto grado;
- Colleghi del Segnalante che lavorano del medesimo contesto lavorativo e che hanno con egli un rapporto abituale e corrente;
- Enti di proprietà del Segnalante o della persona che ha sporto denuncia o per i quali le stesse persone lavorano, nonché gli enti che operano del medesimo contesto lavorativo delle predette persone.

Quanto all'effettività del Modello, questa è legata alla sua efficace attuazione che richiede a norma dell'art. 7, comma 4 del Decreto 231:

- a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività (aggiornamento del Modello);
- b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

I Modelli di Organizzazione, Gestione e Controllo, secondo quanto previsto dall'art. 6, comma 3 del Decreto *“possono essere adottati (...) sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati”*².

² Occorre, tuttavia, sottolineare che le indicazioni contenute nelle linee guida predisposte dalle Associazioni di categoria rappresentano solo un quadro di riferimento e non esauriscono le cautele che possono essere adottate dai singoli enti nell'ambito dell'autonomia di scelta dei modelli organizzativi ritenuti più idonei.

Per la predisposizione del proprio Modello 231 di Organizzazione, Gestione e Controllo, Coface SA ha espressamente tenuto conto, oltre che delle disposizioni del Decreto e delle sue successive modifiche, anche della Relazione ministeriale accompagnatoria e del Decreto ministeriale 201/2003, recante il regolamento di esecuzione del Decreto, delle Linee guida predisposte da Confindustria in data 7 marzo 2002 e relativi aggiornamenti ([Allegato 5](#)), nonché delle Linee Guida ANIA (Associazione Nazionale fra le Imprese Assicuratrici), di seguito esplicate.

1.5 LE LINEE GUIDA ANIA

Il Decreto Legislativo 231/2001 prevede all'art. 6 la possibilità di adottare modelli "sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti". Tale indicazione è resa dal legislatore con la finalità di promuovere il recepimento dei principi espressi dal Decreto e, nel contempo, di incentivare le associazioni di categoria all'elaborazione di documenti metodologici, di per sé non vincolanti, ma utili alle imprese al fine di adottare il proprio modello organizzativo.

Come indicato la Compagnia ha dunque elaborato il presente Modello ispirandosi alle Linee Guida ed ai Suggerimenti Operativi emanati per il settore assicurativo da ANIA (Associazione Nazionale fra le Imprese Assicuratrici) nel 2002 e successivamente aggiornati nel 2006 e nel 2008, e con i quali l'associazione ha individuato sia la procedura da seguire per l'adozione dei modelli, sia alcuni dei possibili strumenti di rilevazione e prevenzione delle fattispecie di reato descritte nel Decreto.

Nello specifico ANIA ha proposto i seguenti passaggi operativi per la costruzione del modello:

- descrizione della fattispecie criminosa prevista dal Decreto e sua applicabilità al settore assicurativo;
- individuazione, per ciascuna fattispecie, delle aree e delle funzioni aziendali cosiddette "a rischio", ossia potenzialmente esposte alla commissione di illeciti;
- identificazione delle attività aziendali dal cui compimento è ipotizzabile la commissione del reato descritto (c.d. attività sensibili);
- previsione di un sistema di controllo interno idoneo a prevenire e ridurre al minimo il rischio di commissione di reati ed atto a perseguire:
 - l'efficacia e l'efficienza dei processi aziendali;
 - l'attendibilità delle informazioni aziendali, siano esse interne o rese all'esterno;
 - la conformità dell'attività aziendale alle leggi, ai regolamenti, ed alle norme e disposizioni interne alla Compagnia.

Con particolare riferimento a tale sistema di controllo, ANIA evidenzia altresì la necessità che lo stesso recepisca criteri e principi quali la verificabilità, coerenza e congruenza di ogni operazione aziendale, la separazione delle funzioni, la documentazione dei controlli, l'adozione di un adeguato sistema sanzionatorio per la violazione delle regole aziendali indicate nel Modello (e nelle procedure, raccomandazioni, disposizioni operative da esso discendenti), e la costituzione di un'OdV caratterizzato da autonomia, indipendenza, professionalità e continuità

d'azione, ed incaricato della costante attività di monitoraggio sul funzionamento, sull'osservanza e sull'efficacia del Modello.

Le predette indicazioni, senz'altro utili quale supporto nell'elaborazione del Modello, non hanno – e non potrebbero peraltro avere – carattere vincolante per gli aderenti. Con l'adozione del Modello, ciascuno di essi è infatti chiamato a calare nella propria realtà operativa e gestionale, peculiare per definizione, i principi generici contenuti nel Decreto e rielaborati dall'associazione di categoria.

Tale il motivo per cui il modello adottato da Coface SA pur – come detto – ispirandosi alle indicazioni rese da ANIA, se ne discosta al fine di adeguare nel miglior modo possibile la propria realtà operativa alle finalità del Decreto.

2. LA RESPONSABILITA' DA REATO NEI GRUPPI DI IMPRESE

Premesse

Il Decreto 231, incentrato su una visione “monistica” dell'Ente non disciplina espressamente gli aspetti connessi alla responsabilità derivante dall'appartenenza ad un gruppo di imprese, nonostante il fenomeno dei gruppi d'impresa rappresenti una soluzione organizzativa diffusa nel sistema economico italiano per diverse ragioni, tra cui l'esigenza di diversificare l'attività e ripartire i rischi.

Inoltre, alla maggiore complessità organizzativa che contraddistingue il gruppo può accompagnarsi una maggiore difficoltà nella costruzione di sistemi di prevenzione dei reati rilevanti ai sensi del Decreto 231.

Occorre pertanto interrogarsi sull'operatività dei Modelli Organizzativi in relazione a reati commessi da società appartenenti a un gruppo.

Nel nostro ordinamento, pur mancando una disciplina generale del gruppo, esistono alcuni indici normativi, quali il controllo e il collegamento (art. 2359 c.c.) e la direzione e coordinamento (art. 2497 c.c.) di società, che confermano la rilevanza del fenomeno delle imprese organizzate in forma di gruppo.

Tuttavia, l'ordinamento giuridico considera unitariamente il gruppo solo nella prospettiva economica, mentre, dal punto di vista giuridico, le società che ne fanno parte sono autonome ed indipendenti, benché l'attività di ognuna sia, il più delle volte, espressione di una politica aziendale comune, dettata dalla *holding*. Non trattandosi, dunque, di una *unicum*, il gruppo non può considerarsi diretto centro di imputazione della responsabilità da reato e non è inquadrabile tra i soggetti indicati dell'art. 1 del Decreto 231. Lo schermo della distinta personalità giuridica delle società che lo compongono rimane un dato insuperabile.

Pertanto, non si può affermare una responsabilità diretta del gruppo ai sensi del Decreto 231.

Al contrario, gli enti che compongono il gruppo possono rispondere in dipendenza dei reati commessi nello svolgimento dell'attività di impresa. È dunque più corretto interrogarsi sulla responsabilità da reato nel gruppo.

Dunque, problema fondamentale è stabilire in presenza di quali presupposti il reato commesso nell'ambito di una società del gruppo possa determinare la responsabilità penale-amministrativa delle restanti consociate ed, in particolare, della capogruppo.

In secondo luogo, occorre chiarire quali accorgimenti organizzativi possono essere adottati dalle imprese organizzate in forma di gruppo - in primo luogo la holding - per non incorrere in responsabilità a seguito del reato commesso dagli esponenti di un'altra società del gruppo.

La responsabilità della holding per il reato commesso nella controllata

Affinché possa configurarsi la responsabilità della capogruppo, per il reato commesso nell'ambito della controllata, è necessario, in primis, che nella consumazione del reato concorra una persona fisica che agisca in rappresentanza o per conto della holding stessa (Es. situazione che potrebbe determinarsi nel caso in cui vi sia una coincidenza dei vertici aziendali tra le diverse consociate), perseguendo l'interesse di quest'ultima.

Sussiste, dunque, al verificarsi di tali condizioni, una responsabilità ascendente della capogruppo.

Va precisato come sia necessario un interesse o vantaggio specifico, concreto ed attuale della holding e non un generico "interesse di gruppo", sul mero presupposto che vi sia sempre un ritorno di utilità a favore della controllante.

Perché anche un'altra società del gruppo sia ritenuta responsabile da reato, occorre quindi che l'illecito commesso nella controllata abbia recato una specifica e concreta utilità - effettiva o potenziale e non necessariamente di carattere patrimoniale - alla controllante o a un'altra società del gruppo.

Vi sarà estensione alla *holding* della responsabilità da reato ascrivibile ad una o più società controllate, anche nel caso in cui l'amministratore della capogruppo venga riconosciuto come amministratore di fatto della controllata.

Solo se i soggetti apicali della capogruppo si ingerissero in modo sistematico e continuativo nella gestione della controllata, così da rendere apparente l'autonomia giuridica di quest'ultima, i vertici della holding potrebbero qualificarsi come amministratori della stessa. In questo caso, peraltro, si verserebbe nella ipotesi del cd. gruppo apparente, ben distante dalla fisiologica realtà dei gruppi, ove la holding indica la strategia unitaria, ma le scelte operative spettano ai vertici della controllata.

Infine, il controllo societario o l'attività di direzione e coordinamento non possono creare di per sé una posizione di garanzia in capo ai vertici della controllante, tale da fondarne la responsabilità per omesso impedimento dell'illecito commesso nell'attività della controllata (art. 40, comma 2, c.p.). Non c'è alcuna disposizione che preveda in capo agli apicali della controllante l'obbligo giuridico e i poteri necessari per impedire i reati nella controllata.

Nelle società del gruppo, giuridicamente autonome, le funzioni di gestione e controllo sono svolte dai relativi amministratori (art. 2380-bis c.c.), i quali potranno legittimamente discostarsi dalle indicazioni provenienti dalla holding, senza incorrere in responsabilità verso quest'ultima.

Va segnalato, inoltre, come le Controllate siano tenute e dissociarsi e distaccarsi da direttive provenienti dalla Capogruppo, laddove esse potrebbero generare il rischio di consumazione di condotte illecite e di reati presupposto.

Ogni società del gruppo è da considerarsi come entità a sé stante e, pertanto, in nessun caso può e deve subire un condizionamento diretto da parte delle restanti consociate o della Capogruppo.

Infine, l'articolo 2497 c.c., in tema di direzione e coordinamento, non individua in capo alla controllante alcun potere peculiare, che non sia spiegabile alla luce del controllo azionario di cui dispone.

In conclusione, non esiste una posizione di garanzia in capo ai vertici della holding, relativa all'impedimento della commissione di illeciti nell'ambito delle società controllate.

Ferme le considerazioni finora svolte, la holding/controlante potrà essere ritenuta responsabile per il reato commesso nell'attività della controllata, al verificarsi di tali condizioni

- 1) sia stato commesso un reato presupposto nell'interesse o vantaggio immediato e diretto, oltre che della controllata, anche della controllante;
- 2) persone fisiche collegate in via funzionale alla controllante abbiano partecipato alla commissione del reato presupposto recando un contributo causalmente rilevante in termini di concorso (v. da ultimo Cass., II Sez. Pen., Sent. n. 52316/2016), provato in maniera concreta e specifica. Ad esempio, possono rilevare:
 - direttive penalmente illegittime, se i lineamenti essenziali dei comportamenti delittuosi, realizzati dai compartecipi siano desumibili in maniera sufficientemente precisa dal programma fissato dai vertici;
 - coincidenza tra i membri dell'organo di gestione della holding e quelli della controllata (cd. interlocking directorates) ovvero più ampiamente tra gli apicali: aumenta il rischio di propagazione della responsabilità all'interno del gruppo, perché le società potrebbero essere considerate soggetti distinti solo sul piano formale.

La responsabilità discendente - dalla controllante alla controllata

Ulteriore ipotesi di propagazione della responsabilità amministrativa all'interno di un Gruppo è la cosiddetta responsabilità discendente, che vede la sua trasmissione dalla Holding alle controllate.

Tale fattispecie potrebbe verificarsi allorché il reato, commesso nell'ambito della capogruppo, sia consumato nell'interesse o vantaggio, esclusivo e specifico, della controllata.

L'adozione di Modelli organizzativi idonei a prevenire reati-presupposto della responsabilità da reato nel contesto dei gruppi

Al fine di bilanciare, da un lato, l'autonomia delle singole società e, dall'altro, l'esigenza di promuovere una politica di gruppo anche nella lotta alla criminalità di impresa, è opportuno che

l'attività di organizzazione per prevenire reati-presupposto della responsabilità da reato degli enti tenga conto di alcuni accorgimenti.

Innanzitutto, ciascuna società del gruppo, in quanto singolarmente destinataria dei precetti del Decreto 231, è chiamata a svolgere autonomamente l'attività di valutazione e gestione dei rischi e di predisposizione e aggiornamento del proprio Modello Organizzativo. Tale attività potrà essere condotta anche in base a indicazioni e modalità attuative previste da parte della holding in funzione dell'assetto organizzativo e operativo di gruppo. Peraltro, ciò non dovrà determinare una limitazione di autonomia da parte delle società controllate nell'adozione del Modello.

L'adozione da parte di ogni società del gruppo di un proprio autonomo Modello determina due fondamentali conseguenze:

1. consente di elaborare un Modello realmente calibrato sulla realtà organizzativa della singola impresa. Infatti, solo quest'ultima può realizzare la puntuale ed efficace ricognizione e gestione dei rischi di reato, necessaria affinché al Modello sia riconosciuta l'efficacia esimente di cui all'articolo 6 del decreto 231;
2. conferma l'autonomia della singola società del gruppo e, perciò, ridimensiona il rischio di una risalita della responsabilità in capo alla controllante o di una sua discesa nei confronti della Controllate.

È fondamentale, inoltre, che ciascuna società appartenente al gruppo nomini un proprio Organismo di Vigilanza.

Solo un OdV costituito nell'ambito del singolo ente può infatti dirsi "organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo" (art. 6, comma 1, lett. b, Decreto 231).

Se, al contrario, la vigilanza fosse esercitata da un Organismo unico costituito presso la controllante, si rischierebbe di fondare una posizione di garanzia di fonte negoziale in capo ai vertici della holding. Soprattutto se all'unico Organismo di vigilanza fossero attribuiti incisivi poteri di controllo sull'attività anche delle società del gruppo, in un eventuale successivo giudizio si potrebbe agevolmente sostenere l'omesso intervento dei vertici della holding, nonostante la consapevolezza delle lacune organizzative della controllata e dell'inclinazione criminosa presente al suo interno.

Per evitare una risalita alla responsabilità della controllante per i reati commessi nella controllata, è anche opportuno evitare che i medesimi soggetti rivestano ruoli apicali presso più società del gruppo (cd. interlocking directorates). Infatti, il cumulo di cariche sociali potrebbe avvalorare la tesi del concorso dei vertici di più società del gruppo nella commissione del reato presupposto.

Fin qui si sono evidenziate, in negativo, le soluzioni organizzative che espongono gli enti del gruppo, in particolare la holding, a responsabilità per il reato commesso all'interno della controllata. Ma, chiarito questo, gli enti raggruppati possono senz'altro raccordare i propri sforzi organizzativi al fine di contrastare più efficacemente fenomeni di criminalità di impresa.

Ad esempio, nell'esercizio dei poteri di direzione e coordinamento e agendo nel rispetto dei principi di corretta gestione societaria e imprenditoriale del gruppo, la controllante può sollecitare l'adozione ed efficace attuazione da parte di tutte le società del gruppo di propri modelli organizzativi. Non dovrà, ovviamente, ingerirsi nella attività di elaborazione o revisione dei modelli, né diramare indicazioni in termini precettivi e vincolanti, limitandosi piuttosto a inviti o indicazioni di massima.

La capogruppo potrà indicare, tra l'altro, una struttura del codice di comportamento, principi comuni del sistema disciplinare e dei protocolli attuativi. Queste componenti del Modello dovranno, tuttavia, essere autonomamente implementate dalle singole società del gruppo e calate nelle realtà aziendali di ciascuna, prevedendo - ove opportuno - principi etico-comportamentali specificamente determinati in relazione al settore di attività dell'ente e ai reati per esso rilevanti. Quest'ultimo accorgimento vale anche nel caso di gruppo multifunzionale, malgrado le maggiori difficoltà che possono porsi, vista la diversificazione delle attività svolte dalle singole imprese che vi operano.

Nel caso di Codici Etici di Gruppo, è opportuno che ciascuna società, integri, nell'alveo della propria regolamentazione interna (ad es. attraverso addenda o protocolli), un proprio Codice Etico, individuando i valori e i principi espressamente correlati all'ambito di specifica operatività e all'effettiva esposizione ai rischi-reato contemplati dal Decreto 231.

Fermo restando quanto precede, si evidenzia che - sulla base delle esperienze sino a oggi maturate - nella prassi operativa possono presentarsi talune problematiche, riconducibili a profili di competenze specialistiche e di dimensionamento organizzativo che connotano tipicamente le società del gruppo, con possibili riflessi in termini di efficacia del complessivo Modello di governance in materia 231, valutato a livello di gruppo. Infatti, il presidio delle tematiche 231, soprattutto a fronte della considerevole e continua estensione dell'ambito di applicazione della normativa e dell'evoluzione giurisprudenziale, richiede la presenza di professionalità specifiche e con competenze anche interdisciplinari (profilo giuridico, organizzativo, economico-aziendale, sistema di controllo e gestione dei rischi, giuslavoristico, ecc.). Si tratta di figure non sempre rinvenibili all'interno delle società controllate, specie di quelle di minori dimensioni, ove è maggiormente avvertita l'esigenza della razionalizzazione delle strutture e del contenimento dei costi di gestione.

In tale contesto, pertanto, le società controllate potrebbero ragionevolmente richiedere alle competenti funzioni della capogruppo (in luogo del ricorso a consulenti esterni) un supporto di natura prettamente consulenziale, dai contenuti maggiormente operativi rispetto al ruolo di indirizzo generale sopra richiamato, volto invece ad agevolare le attività di adozione, aggiornamento, implementazione e monitoraggio del proprio Modello 231 (ad es. supporto al management per la valutazione delle attività o processi astrattamente a rischio; orientamento nella strutturazione dei flussi informativi verso l'Organismo di Vigilanza; indicazioni sulle caratteristiche dei possibili presidi da implementare a fronte delle aree di rischio individuate; contributi professionali ai fini dell'aggiornamento dei Modelli per evoluzioni normative con impatto sulle specifiche realtà del gruppo rispetto alle indicazioni generali; attività formative e di

sensibilizzazione sulla materia; supporto operativo all'Organismo di Vigilanza nell'espletamento delle attività di monitoraggio).

Al riguardo, la funzione Internal Audit della capogruppo, contraddistinta da standard di indipendenza e il cui raggio d'azione si estende solitamente anche alle società controllate, può essere chiamata a supportare il management delle controllate (con particolare riguardo a quelle prive di una propria struttura di audit o di revisione interna) nelle iniziative che assumono rilevanza ai fini del Decreto 231. In particolare, l'Internal Audit può promuovere la complessiva coerenza di approccio rispetto agli indirizzi della holding, previa richiesta da parte delle singole società del gruppo e, comunque, nel rispetto dell'autonomia decisionale di ciascuna organizzazione. Qualora nel gruppo siano presenti strutture di Compliance dedicate al presidio del decreto 231 in qualità di controllo di 2° livello, l'attività di supporto può essere svolta dalle suddette funzioni.

Inoltre, è consigliabile che il Modello Organizzativo della holding tenga conto dei processi integrati che coinvolgono l'attività di più società del gruppo, nonché delle attività destinate a confluire in un esito unitario, come avviene per il bilancio consolidato. Può essere opportuno definire concordemente procedure accentrate e protocolli armonizzati (ad esempio in materia di cash pooling, cioè di gestione delle disponibilità finanziarie del gruppo accentrate in un unico tesoriere, al fine di facilitare i rapporti tra le società del gruppo e gli istituti di credito). In ogni caso, è fondamentale che tali procedure siano ispirate ai principi della trasparenza e della correttezza contabile e rispettino i poteri gestori degli organi di vertice delle controllate, nonché la rispettiva autonomia finanziaria e patrimoniale.

Analoga attenzione dovrà essere posta ad eventuali attività/processi affidati in outsourcing ad altre società del gruppo, e in particolare alle caratteristiche dei relativi rapporti contrattuali, alle autorizzazioni relative agli input forniti, ai controlli sugli output ottenuti e alla fatturazione intercompany, nonché alle transazioni infragruppo e ai meccanismi di determinazione del transfer price. A tale riguardo, un adeguato presidio dei processi infragruppo potrebbe includere, ove possibile e significativo, la previsione di forme di certificazione indipendente dei processi di controllo (disegno e funzionamento) delle entità incaricate di svolgere a livello di Gruppo, interamente o in significativa porzione, i più rilevanti processi di supporto (amministrazione, gestione del personale, sistemi informativi, ecc.).

È opportuno anche che le controllate, in seno ai propri Modelli Organizzativi, delineino regole specifiche per la correttezza e la trasparenza nei rapporti con le restanti consociate. In particolare, l'attività di direzione e coordinamento deve svolgersi attraverso comunicazioni rese in forme ufficiali, così da essere successivamente ricostruibili, se necessario.

Inoltre, si potranno definire canali di comunicazione, anche mediante flussi informativi statistici tra società del gruppo, riguardanti lo stato di attuazione del sistema adottato ai sensi del Decreto 231, eventuali violazioni del Modello e sanzioni applicate, aggiornamenti dei modelli effettuati a seguito di nuovi reati-presupposto rilevanti. La capogruppo potrebbe promuovere lo scambio di informazioni tra organi e funzioni aziendali, ovvero l'aggiornamento nel caso di novità normative o modifiche organizzative che interessino l'intero gruppo.

Allo stesso modo, è auspicabile che tra gli Organismi di Vigilanza delle varie società del gruppo si sviluppino rapporti informativi, organizzati sulla base di tempistiche e contenuti tali da garantire la completezza e tempestività delle notizie utili ai fini di attività ispettive da parte degli organi di controllo.

Questi scambi informativi dovranno comunque essere attentamente disciplinati e gestiti, per evitare che l'autonomia di organismi e modelli sia inficiata da rapporti che, di fatto, determinano l'ingerenza decisionale della holding nelle attività di attuazione del decreto nelle singole controllate.

In particolare, tali flussi informativi dovrebbero concentrarsi su: la definizione delle attività programmate e compiute; le iniziative assunte; le misure predisposte in concreto; eventuali criticità riscontrate nell'attività di vigilanza. Essi dovranno avere finalità conoscitiva, mirando a stimolare l'attività di verifica del gruppo, per esempio, su settori di attività rivelatisi a rischio.

A titolo esemplificativo, nel rispetto dell'autonomia e della riservatezza delle informazioni afferenti alle diverse società del gruppo, può essere valutata l'opportunità di prevedere - anche mediante esplicite formulazioni inserite nei singoli Modelli - l'invio all'OdV della holding da parte degli Organismi di Vigilanza delle società del gruppo di:

1. principali verifiche pianificate;
2. relazioni periodiche predisposte dai singoli Organismi di Vigilanza per gli Organi Amministrativi delle rispettive società, relative alle attività svolte;
3. programmazione annuale generale degli incontri degli Organismi di Vigilanza (da intendersi come quadro dei macro-ambiti oggetto di approfondimento nelle riunioni dell'OdV).

Ulteriori canali di contatto e di scambio informativo tra gli Organismi di Vigilanza di un gruppo, da utilizzare sempre con le cautele del caso, possono passare attraverso:

1. l'organizzazione di riunioni congiunte con cadenza, ad esempio, annuale o semestrale, anche per la formulazione di indirizzi comuni riguardo alle attività di vigilanza e alle eventuali modifiche e integrazioni da apportare ai modelli organizzativi;
2. la creazione di un archivio di raccolta e aggiornamento dei modelli organizzativi delle singole società, nonché di ulteriori documenti informativi di interesse (es. analisi delle novità normative; indicazioni giurisprudenziali).

Inoltre, è consigliabile declinare il rapporto tra i vari Organismi di Vigilanza in un'ottica di pariteticità, evitando di prevedere poteri ispettivi in capo a quello della holding. Essi, infatti, potrebbero indebolire l'indipendenza degli OdV istituiti in seno alle società controllate, rendendo più difficile dimostrare il possesso dei requisiti richiesti dall'articolo 6, comma 1, lettera. b). In particolare, è preferibile evitare che gli OdV delle controllate chiedano la condivisione di quello della holding in ordine all'attività di vigilanza da svolgere o alle misure da adottare in seno alla controllata.

Le peculiarità della responsabilità 231 nei gruppi transnazionali

Il gruppo operante in una dimensione transnazionale presenta profili specifici di potenziale pericolosità in termini di criminalità economica: la dispersione geografica delle attività; il decentramento decisionale; il crescente raggio di incidenza, volume e complessità delle operazioni economiche; il possibile più vasto impatto degli episodi criminosi; le accentuate difficoltà nel perseguirli. D'altra parte, le difformità normative dei diversi ordinamenti di riferimento e l'inevitabile confronto con sistemi giurisprudenziali, meccanismi sanzionatori e dinamiche correttive diverse rendono ancor più complesso il lavoro di adeguamento della struttura organizzativa dell'impresa alle prescrizioni poste dal Decreto 231.

Questi fattori devono trovare adeguato riscontro nei modelli adottati dalle società del gruppo transnazionale.

In particolare, il codice di comportamento deve contemplare principi etici che tengano conto della transnazionalità dell'attività svolta. Inoltre, i soggetti apicali e i sottoposti che svolgono attività che li espongono a contatti con Paesi esteri devono ricevere un'adeguata formazione anche in ordine alla normativa vigente in tali Paesi.

Anche i protocolli operativi devono essere concepiti in vista di un migliore coordinamento interno al gruppo, tenendo conto degli specifici profili relativi all'attività transnazionale. Ad esempio, potrebbe essere necessaria una puntuale individuazione dei processi finanziari ed economici realizzati a livello transnazionale.

Più in generale, in considerazione della necessità di adeguarsi a normative simili su ambiti analoghi o contigui potrebbe essere opportuno definire compliance programs che - nel rispetto delle peculiarità delle regolamentazioni locali - consentano di ottemperare a normative differenti, in maniera efficace.

Al fine di fronteggiare contesti complessi e fortemente interrelati, pur nel rispetto dell'autonomia decisionale in capo a ciascuna controllata, la holding potrebbe identificare alcuni principi di controllo minimi, che le controllate potrebbero attuare in virtù di apposite policies.

La stessa attività degli Organismi di Vigilanza dovrà essere integrata per realizzare controlli sinergici ed efficaci nel contrasto ai reati transnazionali.

In conclusione, la normativa in esame - sebbene suscettibile di perfezionamenti - ha il pregio di fornire un efficace segnale alle imprese affinché avviino un percorso di prevenzione in grado di porle al riparo da responsabilità previste dall'ordinamento italiano e da sistemi esteri quale, a titolo d'esempio, quello del noto Bribery Act varato in Inghilterra nel 2010.

3. LE VICENDE MODIFICATIVE DELL'ENTE

Come disposto dagli artt. da 28 a 33 D.lgs. 231/2001, la Responsabilità amministrativa degli enti, resta ferma anche a seguito di vicende modificative (trasformazioni, fusioni, scissioni e cessioni d'azienda) e, nello specifico:

- nel caso di trasformazione, il nuovo ente sarà destinatario delle sanzioni applicabili all'ente originario per fatti commessi anteriormente alla trasformazione stessa (art. 28 del Decreto);

- nel caso di fusione, l'ente risultante (anche per incorporazione) risponderà dei reati dei quali erano responsabili gli enti partecipanti alla fusione (art. 29 del Decreto);
- nel caso di scissione, anche parziale, resterà ferma la responsabilità dell'ente scisso per i reati commessi anteriormente alla scissione. In ogni caso, gli enti beneficiari della scissione, parziale o totale, sono solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'ente scisso per reati anteriori alla scissione, nel limite del valore effettivo del patrimonio trasferito al singolo ente. In ogni caso, le sanzioni interdittive si applicano agli enti a cui è rimasto o è stato trasferito, anche in parte, il ramo di attività nell'ambito del quale è stato commesso il reato (art. 30 del Decreto);
- nel caso di cessione o di conferimento dell'azienda nella cui attività è stato commesso il reato, salvo il beneficio della preventiva escussione dell'ente cedente, il cessionario è solidalmente obbligato con l'ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'azienda ceduta e nei limiti delle sanzioni pecuniarie che risultano dai libri contabili obbligatori, o di cui il cessionario era comunque a conoscenza. (art. 33 del Decreto).

4 LA COSTRUZIONE DEL MODELLO

4.1 L'INDIVIDUAZIONE DELLE AREE A RISCHIO

Al fine di individuare quali attività aziendali siano maggiormente esposte al rischio di commissione di illeciti è stato predisposto, in fase di prima edizione, uno strumento di indagine in forma di questionario. Tramite tale questionario, compilato grazie alla fattiva collaborazione di tutti i soggetti aventi un ruolo di responsabilità all'interno dell'organizzazione aziendale, è stato possibile individuare le attività potenzialmente a rischio (c.d. "attività sensibili"), e quelle c.d. strumentali che, pur non presentando rischi diretti di commissione dei reati, potrebbero potenzialmente supportarne la realizzazione costituendone la modalità di attuazione.

L'elaborazione del materiale così acquisito ha poi consentito la mappatura delle attività a rischio di reato, e l'individuazione delle funzioni aziendali coinvolte. L'analisi ha, inoltre, reso possibile evidenziare quali siano, per ciascuna struttura intervistata, i reati potenzialmente realizzabili nell'esercizio delle singole attività a rischio, e dunque, stante la pena edittale prevista dal Decreto, il rischio inerente collegato a ciascuna attività.

4.2 ANALISI DEL SISTEMA DI CONTROLLO INTERNO

Successivamente alla sopra descritta indagine, si è verificato quali presidi siano stati adottati dall'azienda, con riferimento alle rilevate attività sensibili, al fine di mitigare il rischio di realizzazione di condotte illecite. Nello specifico sono stati esaminati i seguenti elementi:

IL SISTEMA ORGANIZZATIVO

È stata verificata la presenza dei requisiti di formalizzazione e chiarezza, necessari al fine di delineare una corretta separazione dei ruoli, con particolare riferimento all'attribuzione di responsabilità, alla definizione delle linee gerarchiche, ed alla descrizione di compiti e direttive.

Al fine di verificare la sussistenza di detti requisiti sono stati analizzati:

- gli organigrammi delle strutture aziendali interessate dalle attività sensibili;
- i mansionari del personale appartenente a tali strutture;
- le circolari aziendali e gli ordini di servizio emanati dalla Compagnia e diretti alla regolamentazione delle attività aziendali in analisi.

Dall'esame è stato riscontrato quanto segue:

Organigramma

Ciascuna Direzione di Compagnia è dotata di un organigramma caratterizzato da una precisa identificazione dei ruoli e delle linee di riporto.

Gli organigrammi, aggiornati almeno annualmente e distribuiti secondo i normali principi di conoscibilità, sono sotto il diretto controllo del Rappresentante della Sede Secondaria, supportato in tale attività dalla Direzione del Personale.

A quest'ultima è affidato il monitoraggio e l'aggiornamento, almeno annuale, di tali documenti.

Mansionari

Descrivono nello specifico la posizione ricoperta e l'attività svolta da ciascun dipendente o collaboratore della Compagnia, l'eventuale conferimento di procura e/o i limiti di delega e le procedure che ne regolano l'attività. I mansionari sono aggiornati su base annuale, sottoscritti dal lavoratore, verificati e sottoscritti dal Dirigente di riferimento, e raccolti a cura della Direzione del Personale.

Circolari - Ordini di Servizio - Diramati

Le Circolari sono emesse dal Rappresentante della Sede Secondaria e raggruppate dall'Ufficio Legale e Compliance secondo la loro tipologia: e tracciano indirizzi tecnico – organizzativi generali.

Gli Ordini di Servizio, emanati dal Rappresentante della Sede Secondaria o, per le rispettive aree di competenza, dai Direttori, hanno invece lo scopo di regolare l'attività quotidiana dei singoli servizi o uffici tramite, in via esemplificativa e non esaustiva, l'istituzione di procedure operative, il conferimento di poteri decisionali, la creazione di comitati, la determinazione di mobilità interne di personale.

I diramati sono emanati dalla Direzione Commerciale e dalla Direzione Cauzione e regolano le attività delle Agenzie.

IL SISTEMA AUTORIZZATIVO

È stato verificato se l'insieme di deleghe e procure di cui la Compagnia si è dotata:

- sia compiutamente formalizzato e costantemente monitorato ed aggiornato;
- assicurati che i poteri e le autonomie operative siano conferiti in coerenza con le responsabilità organizzative e gestionali assegnate e/o concretamente svolte, e con agli obiettivi aziendali;
- garantisca il principio della separazione dei ruoli in modo che non sia possibile per alcuno gestire in totale autonomia un intero processo aziendale.

È risultato inoltre necessario verificare l'esistenza e l'applicazione di regole, dettate dal Management Aziendale, circa la sottoscrizione di documenti che comportino un esborso in capo alla Compagnia.

Dall'esame è stato riscontrato quanto segue:

La Compagnia compie atti ed assume decisioni in forza di un ben delineato sistema autorizzativo.

Il Consiglio di Amministrazione di Compagnie française d'assurance pour le commerce extérieur conferisce al Legale Rappresentante della Sede Secondaria per l'Italia la Rappresentanza Giudiziale e Legale della società; quest'ultimo delibera l'attribuzione di procure sulla base delle funzioni operative attribuite alla Direzione o al Servizio di cui il procuratore è responsabile, e a fronte dell'effettiva necessità di investire il soggetto del potere di Rappresentare verso terzi la società. Attualmente la Compagnia ha in essere procure con poteri generali, procure attribuite per il conferimento di poteri specifici e procure per la sottoscrizione di polizze. Diversamente, le deleghe sono attribuite tramite Ordini di Servizio e hanno ad oggetto l'assegnazione di autonomie per l'assunzione di decisioni sui rischi della Compagnia. Tali deleghe, puntualmente quantificate ed assegnate a personale dipendente di comprovata professionalità in ragione del livello di inquadramento e del grado di responsabilità rivestito, sono aggiornate almeno semestralmente in virtù dei mutati assetti aziendali. Al fine di garantire un'attribuzione di procure e deleghe in linea con l'organizzazione aziendale, il predetto sistema è oggetto di analisi e rielaborazione almeno annuale.

LE LINEE GUIDA E LE PROCEDURE AZIENDALI

È stata verificata nel sistema delle procedure e linee guida la presenza dei seguenti elementi:

- tracciabilità delle operazioni: per ciascuna attività si richiede che, in maniera verificabile e documentata, possa essere individuato a chi compete l'autorizzazione, chi abbia

materialmente compiuta l'attività, chi abbia provveduto alla sua registrazione, e chi ne abbia effettuato il controllo;

- separazione dei ruoli: assegnazione a soggetti diversi di differenti fasi di cui si compone il processo (autorizzazione, contabilizzazione, esecuzione del controllo);
- documentabilità dei controlli: possibilità di tracciare i controlli effettuati, in modo che ne siano ripercorribili i passaggi.

Nell'analisi delle procedure aziendali si è ritenuto necessario esaminare anche le fasi di istruzione e formazione delle decisioni aziendali di trasferimento di dati e informazioni. In assenza di procedure si è provveduto alla ricostruzione della prassi operativa in essere.

Dall'esame è stato riscontrato quanto segue:

Le linee guida sono emanate dalla sede di Parigi e forniscono istruzioni operative sia nelle aree Tecniche che Amministrative e Patrimoniali. Posseggono i requisiti richiesti.

Le procedure operative aggiornate a cura dei Direttori o dei Responsabili di Servizio, sono raccolte ed archiviate dall'*Internal Audit*. Tale funzione, oltre a monitorare l'aggiornamento, ha cura di protocollare i documenti e di censirli sulla base della Direzione di provenienza, indicando chi siano i *process owner* e quali i servizi interessati.

L'analisi dei predetti documenti, operata per la redazione del Modello, ha costituito un tassello fondamentale nell'utilizzo del sopra menzionato strumento di gap analysis, rendendo così possibile la programmazione di un piano continuo di miglioramento del Sistema di Controllo Interno. Il costante aggiornamento delle procedure aziendali ed il monitoraggio operato dall'OdV sull'efficacia e sull'attualità del Modello consentono di colmare il gap riscontrato in sede di analisi.

IL SISTEMA DI CONTROLLO DI GESTIONE

È stata effettuata l'analisi dell'operatività del controllo di gestione compiuta sulle attività sensibili, con il fine di verificarne l'idoneità a garantire la trasparenza delle attività aziendali a rischio, e ad esercitare un controllo sistematico sul loro svolgimento.

Dall'esame è stato riscontrato quanto segue:

la Compagnia attraverso il sistema di controllo di gestione indirizza la propria attività verso il controllo del raggiungimento degli obiettivi pianificati. Tramite il monitoraggio costante di appositi indicatori, l'azienda è in grado di rilevare lo scostamento tra quanto programmato ed i risultati effettivamente conseguiti, e di verificare se la gestione aziendale si stia svolgendo secondo criteri di economicità. Momento tipico della pianificazione della strategia aziendale è la formulazione, su base annuale, del Budget di Compagnia.

Il processo è avviato dal Rappresentante della Sede Secondaria che richiama ciascuna Direzione al raggiungimento degli obiettivi programmati per area di business, su base societaria,

ed a livello di gruppo. Il Budget, discusso e concordato dal Rappresentante della Sede Secondaria con ciascuna Direzione, è avallato dal Comitato dei Direttori dopo che ne sia stata valutata la coerenza rispetto agli obiettivi strategici ed alle esigenze complessive della Compagnia.

In ultima istanza il Budget è approvato dal Consiglio di Amministrazione di Compagnie française d'assurance pour le commerce extérieur. Al fine di verificare l'effettiva esecuzione in itinere di tale programmazione annuale, la Compagnia si è dotata di un sistema di reportistica mensile, attuato tramite l'elaborazione, da parte del Servizio Controllo di Gestione, di un documento denominato Reporting Book. Lo scopo è quello di monitorare con l'indicata periodicità – l'andamento complessivo della Compagnia tramite un'analisi del turnover, del rapporto sinistri/premi, dell'andamento dei costi e dei risultati economici conseguiti, oltre che di ottenere una visione complessiva del mercato di riferimento e dei principali competitors.

E' di tutta evidenza come la costruzione del descritto apparato, elemento integrante ed essenziale del Sistema di Controlli interni di cui la Compagnia si è dotata, ed il fatto di aver messo a disposizione dell'OdV i dati ed i documenti che da esso promanano, costituiscono uno strumento di fondamentale importanza nell'attività di applicazione, monitoraggio e costante adeguamento del Modello.

IL CODICE DI CONDOTTA COFACE

Coface SA ha redatto un proprio Codice di Condotta COFACE, che costituisce parte integrante del presente Modello e nel quale sono evidenziati valori e regole comportamentali che recepiscono le indicazioni rese dalla Sede Centrale nel Codice di Condotta COFACE di Gruppo, e che sono volti a promuovere e diffondere una condotta moralmente e professionalmente corretta e pienamente conforme alle normative vigenti. Tale Codice definisce, come da sottostante esemplificazione, gli elementi che devono essere tutelati e rispettati dalla Compagnia e dai soggetti che, nello svolgimento delle rispettive attività aziendali, operano per conto di essa:

- legalità;
- imparzialità;
- trasparenza;
- centralità delle risorse umane;
- riservatezza;
- buona fede;
- lealtà, onestà e correttezza;
- professionalità.

Vengono inoltre dettate specifiche norme comportamentali dirette a regolamentare e

descrivere:

- i rapporti che l'azienda intrattiene con i propri dipendenti e con la rete agenziale cui è demandata la vendita dei prodotti;
- quali obblighi sorgano in capo ai dipendenti, agli agenti ed ai collaboratori in virtù del loro rapporto con la Compagnia;
- le relazioni della Compagnia con i propri fornitori, con la Pubblica Amministrazione e con l'Autorità di Vigilanza;
- le relazioni della Compagnia con la clientela, le modalità di tutela del Capitale Sociale, dei creditori e del mercato.

Il Codice traccia, inoltre, i criteri di condotta che la Compagnia si impegna a rispettare nell'ambito della propria gestione aziendale, con particolare riferimento alle registrazioni contabili, al sistema informatico, alla riservatezza dei dati personali, ed al sistema di controllo interno. Per quanto concerne poi i rapporti intercorrenti tra Coface SA e la collettività, il Codice prevede specifiche regole in tema di comunicazioni rivolte a soggetti terzi, di relazioni intessute con le associazioni portatrici di interessi e con le istituzioni, e di gestione dei contributi e delle sponsorizzazioni.

I principi generali di comportamento dettati dal Codice sono espressamente richiamati in ciascuna area sensibile descritta nella Parte Speciale del Modello, in modo che ne risulti chiara la valenza di strumento – alla stessa stregua delle procedure, degli ordini di servizio, delle circolari e del sistema di deleghe – adottato dalla Compagnia a presidio del presente sistema di prevenzione della commissione di illeciti.

Infine, stante l'evidente correlazione tra Modello e Codice, l'OdV ha anche il compito di verificare il rispetto del Codice, ed eventualmente di segnalare l'applicabilità del sistema sanzionatorio.

4.3 STESURA DELLA PARTE SPECIALE DEL MODELLO

La catalogazione delle attività sensibili, e l'analisi del sistema di controllo adottato dalla Compagnia, consentono di redigere la Parte Speciale del Modello.

Come già indicato, essa ha lo scopo di delineare, per ciascun processo aziendale di riferimento, in che modo il pericolo della commissione di illeciti possa concretizzarsi nell'ordinaria attività aziendale, quali siano gli strumenti concepiti dalla Compagnia per mitigare tale rischio, e quali siano, in un'ottica di monitoraggio e miglioramento costante e continuo, i rimedi da adottare per affinare il sistema di prevenzione degli illeciti.

4.4 GAP ANALYSIS

Con l'utilizzo di questo strumento, largamente impiegato dalle aziende al fine di confrontare la performance prodotta con quelli che sono i risultati potenzialmente raggiungibili, l'esistente sistema di controllo è stato rapportato ai principi ed alle disposizioni del dettato legislativo, nonché alle Linee Guida ed ai Suggerimenti ANIA. Ciò ha consentito di focalizzare le aree di miglioramento e di programmare interventi correttivi che indirizzano l'attività di applicazione e costante adeguamento del Modello.

4.5 MANUTENZIONE ED AGGIORNAMENTO DEL MODELLO

Nella Compagnia sono operanti funzioni di controllo del cui supporto l'Organismo di Vigilanza si avvale per l'espletamento delle proprie funzioni.

Di seguito l'indicazione delle attività svolte dalle funzioni di controllo di Coface SA:

- *Risk Management*: attività di controllo di secondo livello svolta sulle attività di business e di supporto, e di quantificazione e valutazione del rischio;
- *Internal Audit*: monitoraggio e raccolta delle procedure, verifica periodica dell'adeguatezza del sistema di controlli interni;
- *Compliance*: identificazione della normativa e prevenzione del rischio di non conformità, valutazione dell'adeguatezza ed efficacia delle misure adottate.

Grazie alla costante collaborazione delle indicate Funzioni, alla mappatura dei rischi effettuata ed alla documentazione di supporto realizzata e raccolta, l'Organismo di Vigilanza è in grado di valutare costantemente la consistenza, la regolare attuazione e la necessità di adeguamento del Modello.

In sintesi, dunque, la cooperazione tra le Funzioni di controllo ed il supporto metodologico da esse fornito all'OdV, rappresentano il criterio scelto dalla Compagnia al fine di garantire una continua, efficace ed efficiente applicazione del Modello, ed un suo costante aggiornamento, anche alla luce degli eventuali mutamenti dell'assetto organizzativo e operativo dell'azienda.

5 COFACE SA E L'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

5.1. PREMessa: DESCRIZIONE DI COFACE SA E DELLE AREE DI ATTIVITÀ

Compagnie française d'assurance pour le commerce extérieur S.A. è una società di diritto francese, con sede legale in Bois Colombes (Francia), Place Costes et Bellonte 1 – CAP 92270.

Essa, ai sensi e per gli effetti degli artt. 2508 e 2508-bis c.c. ha stabilito in Italia la propria Sede Secondaria, nominando quale suo Preposto e Rappresentante Legale il Dott. Ernesto De Martinis, il quale ricopre la funzione di Country Manager.

La Sede Secondaria è sita in Milano (MI), Via Lorenteggio 250 – CAP 20147. Inoltre, la Società è costituita anche da un Unità Locale, sita in Roma (RM), Via Terenzio 35 – CAP 00136.

La prima iscrizione all'elenco IVASS delle imprese di assicurazione comunitarie autorizzate ad operare in Italia in regime di stabilimento risale al 27 luglio 2012. Da allora l'iscrizione è stata rinnovata periodicamente fino all'ultima avvenuta in data 7 maggio 2019.

Coface SA opera nel mercato assicurativo, offrendo ai propri Clienti coperture assicurative sui propri crediti, proteggendoli, così, dal rischio di insolvenza.

I servizi offerti dalla Società consentono alle imprese, che con essa stipulano polizze assicurative, di:

- Prevenire il rischio di insolvenza, proteggendo l'impresa dalle perdite sui crediti;
- Ampliare il proprio parco Clienti;
- Accelerare il processo di incasso e recupero del credito.

Coface SA offre ai propri clienti, a seconda della tipologia di copertura assicurativa attivata, una vera e propria gestione del credito, affiancando l'impresa come partner per l'indirizzo e lo sviluppo delle vendite.

Le polizze Coface SA prevedono l'analisi preliminare dell'affidabilità dei Clienti dell'impresa assicurata, cioè la loro capacità di onorare gli impegni assunti con la vendita a credito e l'assegnazione di un limite di credito, entro il quale interviene la copertura della polizza.

Tali limiti di credito sono aggiornati periodicamente, con un monitoraggio regolare, in linea con le capacità del debitore.

In caso di insolvenza e mancato pagamento da parte del debitore dell'assicurato, Coface SA, per il tramite della propria controllata – Coface Italia S.r.l. - provvede alla gestione del recupero del credito insoluto e, laddove il recupero dovesse essere infruttuoso, procede al pagamento dell'indennizzo in favore del Cliente.

Coface Italia S.r.l., nello specifico, è soggetto autorizzato alle attività di ricerca e raccolta di informazioni commerciali ex art. 134 TULPS e di recupero crediti ex art. 115 TULPS.

La Società, presente in Italia da più di 30 anni, opera su tutto il territorio nazionale, servendosi di una rete di più di 74 Agenti Generali e 39 Agenzie³.

³ Cfr. <https://www.Coface SA.it/A-proposito-di-Coface SA/Coface SA-in-Italia/Coface SA-in-Italia>

Oltre al business principale della Società, rappresentato, appunto, dall'assicurazione del credito, Coface SA offre alle imprese cauzioni e fidejussioni sui propri obblighi contrattuali o di legge, sotto forma di polizze assicurative, consentendo, in questo modo, alle imprese clienti di mantenere le proprie disponibilità finanziarie, non essendo necessario immobilizzare liquidità, nella misura richiesta dalla cauzione.

Nello specifico, Coface SA offre le seguenti tipologie di cauzione⁴:

- **Cauzione per appalti pubblici**, garantendo, così la partecipazione dei propri clienti alle gare pubbliche e la corretta esecuzione dei lavori, servizi e forniture;
- **Cauzioni per concessioni edilizie**;
- **Cauzioni per imposte e tasse**, consistenti in cauzioni per i rimborsi di imposte IVA e IRPEF;
- **Cauzioni per le Dogane**, consistenti in cauzioni prestate per il pagamento differito dei dazi doganali, per temporanee importazioni o per altre operazioni doganali;
- **Cauzioni per autorizzazioni ministeriali e regionali**, rappresentate da cauzioni per lo smaltimento dei rifiuti, per le coltivazioni e la gestione delle cave;
- **Cauzioni per contratti tra privati**, consistenti in cauzioni per subappalti, ordini di forniture, promesse di vendite, permute.

5.2 STRUTTURA ORGANIZZATIVA, DI GESTIONE E DI CONTROLLO DI COFACE SA

La *Branch* italiana di Coface SA è rappresentata dal Preposto della Sede Secondaria Dott. Ernesto De Martinis, al quale è affidata la sua gestione e organizzazione. Inoltre, in qualità di Country Manager egli è da considerarsi il principale referente per i rapporti intercorrenti tra la Branch e la sede principale francese.

La Società, al fine di garantire la massima trasparenza e chiarezza della conduzione dei propri affari, nonché il massimo rispetto delle normative italiane e francesi, ha implementato tre livelli di controllo: (i) Divisione Legale, (ii) Risk Management e Compliance (iii) Internal Audit.

Tali presidi sono stati adottati in conformità alla Legge francese n. 2016 – 1961, in materia di “trasparenza, lotta alla corruzione e modernizzazione della vita economica” (Loi Sapin II).

La struttura operativa, le risorse aziendali, le attività societarie e i processi di Coface SA costituiscono l'oggetto dell'analisi effettuata e il presente Modello 231 ha come finalità quello di prevenire e limitare quei reati presupposto che, ad oggi, si ritengono maggiormente a rischio commissione, fatto salvo, ovviamente la necessità di provvedere ad un suo futuro adeguamento ed ampliamento, laddove la Società dovesse ampliare ulteriormente il proprio organico operativo o estendere/ampliare le proprie attività.

I processi maggiormente sensibili alla commissione dei reati individuati e le responsabilità delineate per ruolo e funzione aziendale verranno descritte dettagliatamente nel prosieguo.

⁴ <https://www.Coface SA.it/L-Offerta-Coface SA/Ottenere-garanzie-cauzionali/Polizze-Cauzioni>

5.3 INDIVIDUAZIONE DELLE ATTIVITÀ A RISCHIO E DEFINIZIONE DEI PROTOCOLLI: METODOLOGIA DI LAVORO

Si è provveduto a predisporre e a sviluppare il presente Modello sulla base della realtà aziendale e della struttura operativa di Coface SA, analizzando tutte le reali attività e strutture organizzative societarie, al fine di valutare i reali “rischi di reato” prospettabili in relazione ad esse, avuto riguardo a tutte le specificità di ogni settore di attività e ad ogni singola ipotesi di reato-presupposto identificata dal Decreto.

Si è “ritagliato” un Modello di Organizzazione, Gestione e Controllo, che tenga conto dei concreti rischi connessi alle attività aziendali.

A tale scopo, la predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie, suddivise in diverse fasi, improntate ai principi fondamentali della tracciabilità e della verificabilità di tutte le operazioni svolte nell’ambito dell’attività societaria, in modo tale da consentire un controllo effettivo sulla stessa, nonché la coerenza con i precetti del Decreto.

5.3.1. PRIMA FASE: RACCOLTA E ANALISI DI TUTTA LA DOCUMENTAZIONE ESSENZIALE

In primo luogo, l’elaborazione del presente Modello ha preso le mosse dalla raccolta e dalla valutazione di tutta la documentazione ufficiale, disponibile presso la Società, e relativa a:

- a) organigramma e ripartizione delle funzioni;
- b) ordini di servizio;
- c) deleghe e procure, altri documenti societari, contabili e di bilancio;
- d) precedenti processi, condanne o comunque procedimenti subiti dalla società, di qualsivoglia natura giuridica;
- e) regolamenti operativi e procedure formalizzate;
- f) contrattualistica rilevante;
- g) i precedenti accadimenti aziendali rilevanti;
- h) ogni altra informazione rilevante.

I suddetti documenti ed informazioni sono stati quindi esaminati, al fine di costituire una piattaforma informativa della struttura e dell’operatività di Coface SA, nonché della ripartizione dei poteri e delle competenze, funzionale allo svolgimento delle attività rientranti nella fase seguente.

5.3.2. SECONDA FASE: IDENTIFICAZIONE DELLE ATTIVITÀ A RISCHIO

Successivamente, si è proceduto all’individuazione di tutte le attività di Coface SA, prendendo le mosse da un meticoloso lavoro di mappatura delle singole operazioni poste in essere dalla stessa, svolto intervistando, i Responsabili di tutte le Funzioni interne e, nel dettaglio:

- Ernesto De Martinis – *Country Manager*.
- Paolo Rusconi – *Legal Manager*.
- Marta Giora – *Chief Financial Officer (CFO)*.
- Lorenze Montrasio – *Chief Compliance Officer (CCO)*
- Silvia Vitali – *Country Human Resources Manager Italy and Greece (HR)*.
- Luciano Festari – *Responsible Information Technology (IT)*

Le interviste ai Referenti aziendali hanno consentito di delineare l'esatto funzionamento della Società, individuando le modalità operative e la ripartizione delle competenze, nonché la sussistenza o l'insussistenza, per ciascuna di esse, di uno specifico rischio di commissione delle ipotesi di reato indicate dal Decreto.

In particolare, le aree a rischio di commissione di reati rilevanti ai sensi del Decreto 231 sono state identificate mediante un'analisi delle varie *policies* e delle procedure, al fine di favorire le migliori conoscenze in relazione all'operatività di ciascun singolo settore di attività societaria.

I risultati degli incontri protrattisi per alcuni mesi, documentati attraverso verbalizzazioni informali, oltre ad illustrare i contenuti e le modalità operative di ciascuna unità organizzativa, esprimono i concreti profili di rischio di commissione delle ipotesi di reato individuate dal Decreto.

Per ciascuna attività, si è poi provveduto ad indicare le specifiche ragioni di sussistenza o insussistenza di ciascun profilo di rischio.

5.3.3. TERZA FASE: INDIVIDUAZIONE E ANALISI DEGLI ATTUALI PRESIDI AL RISCHIO

Per le aree a rischio si è poi richiesto al soggetto responsabile della gestione delle attività di volta in volta identificate di illustrare le procedure operative ovvero i concreti controlli esistenti e idonei a prevenire il rischio individuato.

5.3.4. QUARTA FASE: GAP ANALYSIS

La situazione di rischio e dei relativi presidi emersa all'esito delle fasi che precedono è stata confrontata con le esigenze e i requisiti imposti dal Decreto, al fine di individuare eventuali lacune del sistema esistente.

Si è provveduto, quindi, per ciascuna area di attività a rischio individuata, ad identificare gli interventi/accorgimenti che risultassero idonei a prevenire in concreto le identificate ipotesi di rischio, tenendo altresì conto dell'esistenza di regole operative esplicitamente codificate o, al contrario, non normate, ma ugualmente rispettate nella pratica operativa.

5.3.5. QUINTA FASE: DEFINIZIONE DEI PROTOCOLLI

Per ciascuna funzione in cui un'ipotesi di rischio sia stata ravvisata come sussistente, sono stati definiti uno o più protocolli di decisione e gestione: un insieme di regole originato quindi da una dettagliata analisi di ogni singola attività e del sistema di prevenzione del rischio.

I protocolli sono ispirati alla regola di rendere documentate e verificabili le varie fasi del processo decisionale, onde sia possibile risalire alla motivazione che ha guidato la decisione. Ciascuno dei siffatti protocolli di decisione e gestione dovrà essere recepito, rendendo quindi ufficiali e obbligatorie le regole di condotta nei confronti di tutti coloro che si trovino a compiere l'attività nell'ambito della quale è stato individuato un rischio.

La definizione dei protocolli si completa e si integra con le regole previste dal Codice di Condotta COFACE di Coface SA, il quale rappresenta uno strumento fondamentale per esprimere principi di deontologia aziendale riconosciuti dalla Società come propri e sui quali essa fonda una sana,

trasparente e corretta gestione delle attività poste in essere dai dipendenti e, più in generale, da parte di tutti i soggetti afferenti alla stessa.

Tabella riepilogativa



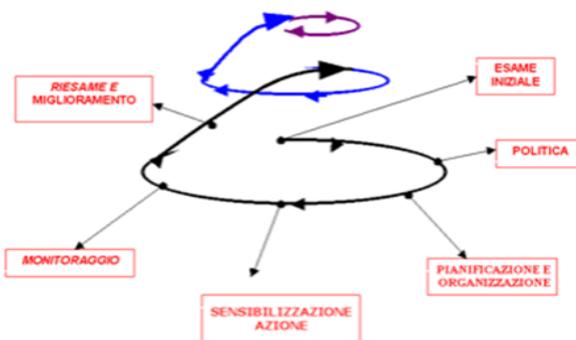
5.4. AGGIORNAMENTO DEL MODELLO

Per espressa previsione dell'art. 6 comma 1 lett. a) del D. Lgs. 231/2001, l'adozione e l'efficace attuazione del Modello costituiscono una responsabilità in capo all'organo dirigente societario.

Vista la professionalità specifica dell'OdV (cfr. *infra*), a quest'ultimo compete il compito di monitorare l'aggiornamento del Modello, su delega dell'Organo Amministrativo/Country Manager, secondo quanto previsto all'interno dello stesso.

L'attività di aggiornamento del Modello - intesa sia come integrazione sia come modifica - è volta a garantire l'adeguatezza e l'idoneità dello stesso, al fine di assicurare la costante funzione preventiva rispetto alla commissione dei reati presupposto ex D. Lgs. 231/2001.

Ad ogni modo, solo l'Organo Amministrativo può deliberare eventuali revisioni del Modello Organizzativo.



6. L'ORGANISMO DI VIGILANZA

6.1. STRUTTURA E COMPOSIZIONE DELL'ORGANISMO DI VIGILANZA

Ai fini dell'esclusione della responsabilità amministrativa dipende da reato, l'art. 6 D.lgs. 231/01, dispone che, non solo la Società debba adottare ed applicare efficacemente il Modello 231, ma prevede che sia necessario l'istituzione di un Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e di controllo e avente il compito di vigilare sulla corretta applicazione del Modello stesso e di curarne l'aggiornamento periodico.

In relazione all'identificazione dell'OdV ed all'esigenza di efficacemente attuare il Modello, si è deciso di nominare un Organismo di Vigilanza secondo i principi qui dappresso descritti.

Il Decreto, in virtù delle modifiche normative apportate dall'art. 1, comma 82 della Legge finanziaria del 2005, stabilisce che l'OdV possa essere sia monosoggettivo che plurisoggettivo.

Coface SA ha optato, nel pieno rispetto della disciplina normativa, per un Organismo di Vigilanza collegiale.

Tale soluzione è stata ritenuta adatta, sulla base delle caratteristiche della propria struttura organizzativa, a garantire l'effettività dei controlli cui l'OdV è istituzionalmente preposto. I componenti dell'OdV garantiscono appieno la professionalità e la competenza nello svolgimento dei compiti affidati all'organismo.

Si è inoltre deciso che la nomina dei membri dell'OdV, nonché l'eventuale revoca, siano di competenza dell'Organo Amministrativo, il quale procede a tali operazioni nel pieno rispetto delle indicazioni di legge, comunque garantendo sempre che l'OdV sia connotato dai seguenti requisiti:

a) Autonomia e indipendenza

I requisiti di autonomia e indipendenza sono fondamentali affinché l'OdV non sia direttamente coinvolto nelle attività operative/gestionali che costituiscono l'oggetto della sua attività di controllo. Tali requisiti si ottengono garantendo all'OdV - inteso come unità di staff a sé stante nella struttura organizzativa - una sostanziale indipendenza gerarchica o comunque una dipendenza minima e prevedendo che, nello svolgimento delle sue funzioni, l'OdV risponda solo al massimo vertice gerarchico, mantenendo un costante contatto con le Funzioni di Controllo Interno e con l'Altra Direzione.

Al fine di rendere effettivi i suddetti requisiti, è stato necessario definire alcune forme di tutela in favore dei componenti dell'OdV, in modo tale da assicurargli un'adeguata protezione da eventuali forme di ritorsione a suo danno (si consideri il caso in cui dagli accertamenti svolti dall'OdV emergano elementi che facciano risalire al vertice aziendale il reato – o il tentativo di commissione del medesimo – ovvero una violazione del presente Modello, di cui si dirà – in special modo – infra al punto c).

A tal fine, l'Organo Amministrativo sarà adeguatamente informato circa le valutazioni sulla performance professionale complessiva, e su ogni intervento retributivo e/o organizzativo relativo all'OdV; il medesimo Organo ne verificherà la congruità con la politica interna aziendale.

b) Professionalità

I componenti dell'OdV devono possedere requisiti tecnico-professionali adeguati alle funzioni che sono chiamati a svolgere; in particolare, deve essere dotato di competenze specialistiche in tema di attività ispettiva e di consulenza (a titolo esemplificativo, gestione dei sistemi di sicurezza e prevenzione degli infortuni, campionamento statistico, tecniche di analisi, conoscenze contabili, metodologie di individuazione delle frodi e del sistema informatico) e competenze giuridiche, con particolare riferimento ai reati previsti dal Decreto. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio richiesto all'Organismo di Vigilanza.

c) Onorabilità

I componenti dell'OdV devono possedere, oltre alle competenze tecniche sopra descritte, ulteriori requisiti soggettivi formali, quali l'onorabilità, la carenza di conflitti d'interessi e di rapporti di parentela con gli organi sociali e con il vertice, nonché l'assenza di imputazioni in procedimenti penali aventi ad oggetto le fattispecie previste dal Decreto, al fine di garantire ulteriormente la suddetta imparzialità nell'operato atteso dall'Organismo.

Non possono essere nominati membri dell'OdV - e se lo sono decadono automaticamente da tale incarico:

- coloro che, ai sensi dell'art. 2382 cod. civ., si trovano nella condizione di inabilitato, interdetto, fallito o condannato ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;
- coloro che siano stati sottoposti a misure di prevenzione, in quanto persone pericolose (L. 27/12/1956 n. 1423) ovvero ai sensi della legge contro la mafia (L. 31/05/1965 n. 575);
- coloro che sono stati condannati a seguito di sentenza, anche non definitiva o emessa ai sensi degli articoli 444 e seguenti del cod. proc. pen., ovvero, anche se con pena condizionalmente sospesa salvi gli effetti della riabilitazione:
 - per uno dei reati societari previsti dal Codice Civile (artt. da 2621 a 2641) o dalla vigente normativa fallimentare (R.D. 16/03/1942 n. 267 e succ. mod.);
 - a pena detentiva, non inferiore ad un anno, per uno dei reati previsti dalle norme che regolano l'attività in ambito assicurativo, bancario e finanziaria ed in materia di mercati e valori mobiliari e di strumenti di pagamento;

- alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, il patrimonio, l'ordine pubblico, l'economia pubblica o per un delitto in materia tributaria;
 - alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;
 - in ogni caso e a prescindere dall'entità della pena, per un delitto contro la pubblica amministrazione o per uno o più illeciti tra quelli tassativamente previsti dal Decreto;
- coloro che hanno rivestito la carica di membro dell'Organismo presso società nei cui confronti siano state applicate le sanzioni previste dal Decreto, salvo che siano trascorsi cinque anni dalla sentenza definitiva ed il componente non sia incorso in condanna penale;
- coloro nei cui confronti siano state applicate le sanzioni accessorie di cui all'art. 187 quater TUF (D.lgs. 24/02/1998 n. 588).

d) Continuità d'azione

L'OdV deve:

- lavorare costantemente sulla vigilanza del Modello con i necessari poteri d'indagine;
- essere una struttura "interna" all'azienda, anche se composta interamente da soggetti indipendenti (siano essi interni – nel senso anzidetto - o esterni) rispetto all'Organo Amministrativo di Coface SA, in modo da garantire la continuità dell'attività di vigilanza;
- curare l'attuazione del Modello e assicurarne il costante aggiornamento;
- non svolgere mansioni prettamente operative che possano condizionare la visione d'insieme delle attività aziendali ad esso richieste e minarne l'obiettività di giudizio.

L'eventuale revoca dei membri dell'OdV, da disporsi esclusivamente per ragioni connesse a gravi inadempimenti in ordine al mandato conferito, dovrà essere deliberata dall'Organo Amministrativo e previamente comunicata agli organi sociali apicali. La revoca dei poteri propri dell'OdV e l'attribuzione dei medesimi poteri ad altri soggetti, potrà avvenire solo per giusta causa, per tale dovendosi intendere anche interventi di ristrutturazione organizzativa di Coface SA, mediante apposita determina dell'Organo Amministrativo.

Il sopravvenire di cause di incompatibilità/ineleggibilità determinerà l'immediata decadenza dei membri dell'OdV. Se nel corso dell'incarico viene a mancare uno dei componenti dell'OdV, l'Organo Amministrativo provvede tempestivamente alla sostituzione dello stesso.

L'OdV provvede direttamente a dotarsi di un Regolamento che disciplini il suo funzionamento in conformità alla legge, nonché alle disposizioni del Codice di Condotta COFACE e del presente Modello.

Inoltre, l'OdV provvederà ad adottare efficaci meccanismi di *whistleblowing protection*, istituendo delle linee fax e/o delle caselle di posta cartacea ed elettronica alle quali ogni dipendente, anche in forma anonima e riservata, potrà trasmettere ogni utile segnalazione circa presunte violazioni del Modello, anche qualora le stesse non integrino gli estremi di un reato.

6.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

I compiti dell'OdV sono espressamente definiti all'articolo 6, comma 1, lett. b) del Decreto:

- vigilare sul funzionamento e sull'osservanza del Modello;
- curarne l'aggiornamento.

In adempimento al primo di siffatti compiti, all'OdV sono affidate le seguenti attività:

- effettuare verifiche sulle attività od operazioni individuate nelle aree a rischio, al fine di valutare l'osservanza e il funzionamento del Modello;
- vigilare sull'adeguatezza e sull'aggiornamento dei protocolli rispetto alle esigenze di prevenzione dei reati;
- vigilare sul sistema di deleghe, al fine di garantire la coerenza tra i poteri conferiti e le attività in concreto espletate;
- promuovere adeguate iniziative volte alla diffusione della conoscenza e della comprensione del Modello organizzativo tra tutti i dipendenti, consulenti e partner;
- confrontarsi con il responsabile Risorse Umane per la definizione di appositi programmi di formazione diretti al personale e del contenuto di comunicazioni periodiche da inoltrarsi ai Dipendenti e agli Organi Sociali, volte a fornire agli stessi la necessaria sensibilizzazione e le basi conoscitive circa la normativa di cui al Decreto;
- predisporre e aggiornare con continuità, in collaborazione con le funzioni interessate, lo spazio nella rete e/o in forma cartacea, contenente tutti i dati relativi al Decreto e al presente Modello;
- valutare le segnalazioni di possibili violazioni e/o inosservanze del Modello, anche non integranti gli estremi di un reato;
- condurre le indagini volte all'accertamento di possibili violazioni delle prescrizioni del Modello;
- coordinarsi con il *management* aziendale per valutare l'adozione di eventuali sanzioni disciplinari, fermo restando la competenza di quest'ultimo all'irrogazione delle sanzioni ed al relativo procedimento disciplinare.

Qualora l'attività richieda competenze specialistiche che eccedono quelle del membro dell'OdV, lo stesso Organo potrà ricorrere a consulenti e professionisti esterni, scegliendoli tra quelli qualificati dall'azienda.

Pur tenendo conto del fatto che la competenza per l'adozione ed efficace attuazione del Modello è espressamente attribuita all'Organo dirigente di Coface SA ai sensi dell'art. 6 comma 1, lett. a), è stata presa la decisione di affidare le procedure di aggiornamento del Modello stesso alla

competenza dell'OdV. Pertanto, nel rispetto del dettato normativo, l'attività di aggiornamento verrà espletata dall'OdV, su delega espressa dell'Organo Amministrativo di Coface SA

Il compito affidato all'OdV di curare l'aggiornamento del Modello si traduce quantomeno nelle seguenti attività:

- programmare controlli ed implementare verifiche su base periodica delle attività di tutte le singole Aree Operative, al fine di garantire la corretta (e costante) individuazione delle attività a rischio e la loro eventuale integrazione;
- attuare le verifiche periodiche e a campione relative all'idoneità ed efficienza dei protocolli previsti in attuazione delle procedure adottate dall'azienda, della documentazione di supporto alle operazioni aziendali, anche di carattere contabile, riscontrando e segnalando all'organo dirigente ogni eventuale anomalia;
- verificare che ogni parte che concorre a realizzare il Modello sia e resti rispondente e adeguata alle esigenze del Modello, come individuate dalla legge;
- verificare e aggiornare il Modello in ogni sua parte a seguito di modifiche aziendali, legislative e di ogni altra natura che abbiano incidenza su quanto previsto dallo stesso;
- valutare, unitamente alle funzioni competenti, le iniziative anche operative da assumere nell'ottica di un efficace aggiornamento del Modello e predisporre il piano di miglioramento;
- curare, su delega espressa dell'Organo Amministrativo, gli eventuali aggiornamenti ed adeguamenti del Modello, da realizzarsi attraverso le modifiche e/o le integrazioni rese necessarie da significative violazioni delle prescrizioni, da mutamenti nell'organizzazione o nell'attività, da interventi legislativi che ne richiedano l'adeguamento o dall'effettiva commissione di reati;
- segnalare all'organo dirigente le violazioni del Modello in grado di determinare la responsabilità in capo all'ente, registrare e conservare accuratamente le medesime;
- verificare l'effettività e la funzionalità delle modifiche del Modello di volta in volta adottate dagli organi competenti;
- qualora si renda necessario, in conseguenza alla modificazione del Modello, un intervento modificativo sulle *policies* o sulle procedure contenute nei manuali operativi, l'OdV potrà disporre autonomamente tale modifica;
- redigere un verbale ad esito di ciascuna riunione;
- conservare accuratamente i verbali, le decisioni, i suggerimenti, le proposte ed ogni documentazione dell'attività svolta, delle segnalazioni e della documentazione rilevante.

Per l'espletamento di siffatti compiti, l'OdV, nell'esercizio dei propri poteri, e in perfetta autonomia, provvederà direttamente alle seguenti incombenze:

- predisporre il piano annuale delle verifiche su adeguatezza e funzionamento del Modello;
- predisporre misure idonee al fine di mantenere aggiornata la mappatura delle aree a rischio e la tracciabilità dei flussi informativi e decisionali, secondo le modalità e i principi seguiti nell'adozione del Modello;

- raccogliere, elaborare e conservare le informazioni rilevanti per il rispetto del Modello, curando anche il loro aggiornamento e l'effettiva trasmissione delle informazioni richieste.

Per adempiere pienamente e in autonomia ai propri compiti, all'OdV sarà attribuito un budget adeguato - stabilito nel regolamento interno dell'Organismo medesimo - che sarà approvato nella prima convocazione. Il suddetto budget viene predisposto annualmente dall'OdV ed è approvato dall'Organo Amministrativo di Coface SA, il quale non potrà sindacare l'ammontare, bensì semplicemente chiederne giustificazione in caso di evidenti incongruità. In casi eccezionali, tale budget annuo potrà essere aumentato su richiesta dell'OdV, ove necessario per adempiere ai propri compiti istituzionali.

L'OdV non dispone di poteri operativi o decisionali, neppure di tipo impeditivo, in relazione all'attività imprenditoriale di Coface SA. In ogni caso, l'Organo Amministrativo deve essere informato di ciascuna deliberazione dell'OdV alla prima riunione utile.

Le suddette deliberazioni hanno mero carattere consultivo e/o propositivo, e non possono in alcun modo vincolare l'Organo Amministrativo. Per adempiere ai propri compiti, l'OdV si avvarrà della collaborazione di ogni funzione e di ogni risorsa della Società, al fine di ottenere le informazioni o i dati rilevanti, ritenuti necessari per lo svolgimento dei propri compiti istituzionali, senza necessità di alcuna autorizzazione preventiva.

In ogni caso potrà ricorrere anche a consulenti esterni, ove la loro collaborazione si renda necessaria.

Quanto all'ambito di applicazione dei poteri di controllo dell'OdV, il Decreto non pare poter modificare la normativa societaria già vigente, nel senso cioè di poter comportare una significativa e non giustificabile restrizione dell'autonomia statutaria e organizzativa degli enti, con la conseguenza che, per quanto concerne i soggetti depositari delle deleghe operative espresse in termini di maggiore autonomia e poteri delegati, ossia i soggetti nei confronti dei quali la Società ha già ritenuto di conferire la propria massima fiducia, non potranno che continuare a valere le sole forme di controllo già espressamente previste dall'ordinamento vigente e, con esse, i rimedi per le violazioni di legge di cui tali soggetti si rendessero responsabili.

All'OdV resta in ogni caso riconosciuto il potere di interloquire con i soggetti legittimati per legge all'attività di controllo, e la facoltà di poter sollecitare verifiche relative alla sussistenza degli elementi richiesti per legge, ai fini di poter proporre azioni di responsabilità o di revoca per giusta causa.

Gli incontri con gli organi societari cui l'Organismo di Vigilanza riferisce devono essere documentati. Copia della documentazione deve essere custodita a cura dell'OdV stesso.

L'OdV, nonché tutti i soggetti dei quali quest'ultimo si avvale a qualsiasi titolo, sono vincolati all'obbligo di riservatezza in relazione a tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni.

6.3. REPORTING DELL'ORGANISMO DI VIGILANZA

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'OdV non riporta in linea gerarchica a nessuna funzione all'interno della Società.

Annualmente l'OdV elabora una relazione scritta per l'Organo Amministrativo/Country Manager, contenente informazioni sull'attività svolta – *report* dei controlli effettuati e relativi esiti, eventuale aggiornamento della mappatura delle attività sensibili, etc. – nonché un piano delle attività previste per l'anno successivo.

Nel caso in cui l'OdV riscontri anomalie o criticità riferibili a qualcuno dei soggetti referenti, la segnalazione dovrà essere indirizzata a uno degli altri soggetti di cui sopra.

L'attività di *reporting* ha ad oggetto:

- l'attività svolta dall'OdV;
- le revisioni apportate al Modello o le proposte di modifica del medesimo;
- le eventuali anomalie riscontrate, sia in termini di comportamenti in Coface SA, sia in termini di efficacia del Modello.

Gli incontri tra l'OdV e i soggetti referenti devono essere verbalizzati; le copie dei verbali devono essere custodite dall'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni e i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

6.4. FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

6.4.1. Flussi informativi verso gli Organi societari ed i Vertici aziendali

L'OdV è artefice delle seguenti informative:

- riferisce delle infrazioni al Codice di Condotta COFACE, al Modello, alle procedure di attuazione dello stesso:
 - al Rappresentante della Sede Secondaria e/o al C.d.A qualora l'infrazione sia commessa da figura apicale;
 - al Rappresentante della Sede Secondaria, qualora l'infrazione sia commessa da un qualsiasi altro soggetto.
- relaziona su base semestrale il Rappresentante della Sede Secondaria circa:
 - l'attività svolta dall'OdV
 - le eventuali criticità emerse sia in termini di comportamenti o eventi interni, sia in termini di efficacia ed efficienza del Modello e del Codice di Condotta COFACE;
 - le modifiche e/o integrazioni al Modello;
 - la pianificazione delle attività e degli interventi correttivi e migliorativi al Modello e/o al Codice di Condotta COFACE già approvati, con relativo stato di avanzamento lavori;
 - le violazioni al Modello Organizzativo ed al Codice di Condotta COFACE rilevate nel periodo di riferimento, e le relative sanzioni disciplinari adottate.

Il Rappresentante della Sede Secondaria e l'Alta Direzione hanno la facoltà di convocare in qualsiasi momento l'OdV il quale, a sua volta, ha la facoltà di richiedere la convocazione dei predetti soggetti per motivi urgenti.

6.4.2. Flussi informativi verso l'Organismo di Vigilanza

È fatto obbligo a tutti i dipendenti ed a coloro che a vario titolo collaborano con Coface SA di comunicare all'OdV qualsiasi condotta che, sulla scorta di quanto previsto dal Decreto, possa recare pregiudizio alla Compagnia.

Tali segnalazioni sono effettuate, al verificarsi di comportamenti sospetti o illeciti ovvero, a seguito di esplicita richiesta da parte dell'Organismo, su base periodica. Le segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei reati o comunque circa la realizzazione di comportamenti non in linea con le regole di comportamento di cui al Modello ed al Codice di Condotta COFACE devono essere effettuate per iscritto, ed inviate o via e-mail all'indirizzo organismodivigilanza@coface.com o via posta a **Organismo di Vigilanza di Coface S.A. Sede Secondaria e Rappresentanza Generale per l'Italia, all'attenzione del Responsabile Compliance, Via Lorenteggio 240, 20147, Milano.**

L'accesso e la gestione della menzionata casella di posta elettronica, della posta cartacea e dei relativi archivi, sono consentiti ai soli componenti dell'OdV a tal proposito si evidenzia che le segnalazioni, così come tutta la documentazione e gli atti prodotti o acquisiti dall'OdV nello svolgimento della sua attività, sono trattati ed archiviati, in forma elettronica così come cartacea, nel rispetto del principio di riservatezza ed in ottemperanza dei vigenti obblighi di conservazione decennale. Le decisioni inerenti la consultazione di tali archivi sono demandate all'OdV, che ha cura di conservare traccia di tutti gli accessi e delle eventuali movimentazioni di atti o documenti. Ricevuta la segnalazione l'OdV si riunisce per analizzarne congiuntamente il contenuto e valutarne la fondatezza, compiere gli opportuni accertamenti e, se del caso, dare avvio al procedimento sanzionatorio.

Oltre alle predette informative, devono essere obbligatoriamente ed immediatamente trasmesse all'OdV le notizie afferenti: i singoli rischi nelle specifiche aree analiticamente indicati nella Parte Speciale del Modello.

6.4.3. Whistleblowing protection (protezione delle segnalazioni)

Il sistema di protezione delle segnalazioni relative alla violazione di disposizioni di legge, del Codice di Condotta COFACE e del Modello di Organizzazione, Gestione e Controllo è considerato strumento fondamentale per l'efficace applicazione del sistema di prevenzione dei rischi di reato.

Pertanto, un dipendente che segnala una violazione del Modello, anche se non costituente reato, non deve trovarsi in alcun modo in posizione di svantaggio per questa azione, indipendentemente dal fatto che la sua segnalazione sia risultata in seguito fondata o meno.

Un dipendente che ritenga di essere stato discriminato nella sua attività o di aver subito ritorsioni a causa della Segnalazione, secondo quanto previsto nella Procedura di Whistleblowing, adottata dalla Società, dovrà immediatamente darne notizia alle Autorità competenti.

Coface SA si impegna ad offrire un ambiente di lavoro privo di discriminazioni e molestie e si aspetta che tutti i dipendenti facciano il possibile per mantenere questo tipo di ambiente di lavoro. Coface SA: non potrà tollerare molestie a un dipendente da parte di nessuno (si vedano le prescrizioni dettate al riguardo dal Codice di Condotta COFACE).

Saranno intraprese azioni disciplinari nei confronti di chiunque metta in atto azioni discriminatorie, o rechi molestie a qualsiasi dipendente che segnali una violazione del Modello.

Un dipendente che segnali una violazione del Modello o trasmetta un'accusa, sia essa falsa o presentata con mezzi diversi da quelli riconosciuti dal sistema di protezione non avrà diritto alle tutele offerte da quest'ultimo. Allo stesso modo non saranno considerati meritevoli di protezione coloro i quali effettuano una Segnalazione, per ragioni puramente personali e con l'unico scopo di arrecare un danno e/o pregiudizio nei confronti del segnalato.

Verranno avviate procedure disciplinari nei confronti di chiunque sollevi intenzionalmente accuse false o irregolari.

Coface SA incoraggia tutti i Destinatari che desiderino sollevare una questione inerente ad una violazione del Modello, a discuterne con il *manager* responsabile prima di seguire le normali procedure di *whistleblowing*, salvo evidenti controindicazioni.

I consulenti esterni e qualunque soggetto terzo, che presta la propria attività lavorativa in favore della Società, effettuano la segnalazione direttamente all'OdV, secondo quanto previsto e disposto nella Procedura di Whistleblowing.

Tale Procedura, al fine di consentirne, la diffusione e conoscenza a tutti i Destinatari, dovrà essere pubblicata sul sito Internet aziendale.

Per consentire un accertamento corretto e un'indagine completa di una segnalazione relativa a un comportamento sospetto, quando segnalano la presunta violazione, i Destinatari devono fornire le informazioni riportate qui di seguito, che confluiscono in apposito documento redatto dall'OdV:

- una descrizione della questione con tutti i particolari di rilievo (ad esempio l'accaduto, il tipo di comportamento, la data e il luogo dell'accaduto e le parti coinvolte);
- un'indicazione del motivo per il quale la questione è ritenuta preoccupante;
- un'indicazione che confermi se il fatto è avvenuto, sta avvenendo o è probabile che avvenga;
- un'indicazione del modo in cui il dipendente è venuto a conoscenza del fatto/della situazione;
- l'esistenza di testimoni;
- ulteriori informazioni ritenute rilevanti da parte del dipendente;
- se il dipendente ha già sollevato il problema con qualcun altro e, in caso affermativo, a chi;

- la specifica funzione nell'ambito della quale si è verificato il comportamento sospetto.

Ove possibile e non controindicato, il dipendente che effettua la segnalazione deve anche fornire il suo nome e le informazioni per eventuali contatti. La procedura di segnalazione non anonima deve essere preferita, in virtù della maggior facilità di accertamento della violazione. In ogni caso:

- tutto il personale a qualunque titolo coinvolto nel sistema di *whistleblowing* è tenuto a mantenere standard elevati di professionalità e riservatezza;
- qualsiasi documento creato in relazione a una segnalazione di *whistleblowing* deve essere tenuto in modo rigorosamente riservato;
- nel corso di qualsiasi comunicazione e/o riunione, è necessario prestare attenzione ed evitare possibili dichiarazioni dannose per proteggere l'identità delle persone coinvolte e assicurarsi che le indagini non rechino danni;
- tutte le indagini devono essere eseguite in modo tale da evitare l'eccessiva attenzione e/o la speculazione da parte di coloro che non devono essere coinvolti;
- le comunicazioni devono essere rivolte solo alle persone che devono essere informate;
- ogni dipendente interrogato in relazione ad un'indagine deve essere a conoscenza del fatto che la problematica verrà trattata in modo riservato e che deve evitare di parlarne con terzi.

Qualsiasi questione relativa a presunte violazioni di quanto stabilito dal Decreto, dalle altre fonti di legge, dal Codice di Condotta COFACE e dal Modello deve essere indirizzata direttamente all'OdV. Tale segnalazione potrà essere esposta in modo anonimo, benché resti preferibile che sia sottoscritta dal *whistleblower* per agevolare la successiva attività di indagine.

I *whistleblowers* anonimi sono comunque invitati a fornire quantomeno informazioni sufficienti relative a un fatto o a una situazione per consentire un'adeguata indagine.

Le segnalazioni relative a presunte violazioni relative all'applicabilità della presente procedura saranno esaminate in modo approfondito, equo e tempestivo. Le indagini devono iniziare al più presto e devono essere svolte in modo diligente. Tutte le persone coinvolte in un'indagine devono prestare attenzione e agire in modo imparziale in tutte le fasi della procedura. Devono essere raccolte prove oggettive relative all'evento o alla situazione segnalato, non le opinioni o le speculazioni.

L'OdV deve conservare tutti i documenti esistenti al momento in cui è stata segnalata la violazione. Se necessario, i documenti devono essere prelevati dalle aree e dagli archivi in cui sono conservati.

Qualora la segnalazione pervenga in forma scritta anonima, l'OdV valuta l'opportunità di procedere ad indagini, sempre che la segnalazione contenga riferimenti sufficientemente specifici per effettuare gli accertamenti del caso.

Nell'esercizio del proprio potere ispettivo, l'OdV deve poter accedere liberamente, senza la necessità di una preventiva autorizzazione, a tutte le fonti di informazione dell'ente, nonché prendere visione di documenti e consultare i dati societari.

Tutte le informazioni, i documenti e le segnalazioni raccolte nell'espletamento dei compiti istituzionali da parte dell'OdV devono essere archiviate e custodite a cura dell'Organismo in un apposito *data base* (informatico o cartaceo) per un periodo di 5 anni.

L'OdV, inoltre, ha cura di mantenere riservati i documenti e le informazioni acquisiti, anche nel rispetto della normativa sulla *privacy*.

Coface SA ha adottato una specifica Procedura *Whistleblowing*, allegata al presente Modello sub [Allegato 7](#).

Va segnalato, inoltre, che nel rispetto della normativa francese – Loi Sapin II -, la Società ha predisposto anche una "*Procedura Ombudsman*" ([Allegato 7-bis](#)), che può essere utilizzata da tutti i Dipendenti di Coface SA per segnalare:

- Reati in generale, commessi nell'esercizio dell'attività lavorativa (non solo reati presupposto ex D.lgs. 231/2001, ma qualsiasi tipologia di illecito penale);
- Violazione di leggi o regolamenti;
- Minacce ad interessi pubblici generali (Es. pericolo o potenziale pericolo per la salute ed incolumità pubblica);
- Violazioni del Codice di Condotta di Coface SA.

Tali segnalazioni potranno essere effettuate attraverso qualsiasi mezzo ed in qualsiasi forma (anche telefonicamente o a mezzo e-mail) ed il destinatario sarà l'Ombudsman.

7. IL SISTEMA SANZIONATORIO

7.1. STRUTTURA E FUNZIONE DEL SISTEMA SANZIONATORIO

Il sistema disciplinare di Coface SA è stato redatto ed elaborato in attuazione del dettato normativo di cui al D. Lgs. n. 231/2001. Infatti, gli artt. 6 e 7 del citato decreto legislativo prevedono che gli enti siano esonerati dalle responsabilità ivi previste, qualora abbiano adottato un Modello Organizzativo idoneo a prevenire i reati c.d. presupposto descritti nel Decreto ovvero un sistema di sanzioni "disciplinari" da applicarsi in caso di inosservanza delle disposizioni dettate dal D. Lgs. n. 231/2001 o dal suddetto Modello.

Coface SA ha predisposto il presente documento tenendo in considerazione che la commissione o il concorso nella commissione dei reati di cui al Decreto è già sanzionata dal Codice Penale, dal quale il presente sistema disciplinare deve essere considerato autonomo e distinto. Pertanto, le regole e le sanzioni indicate nel presente testo integrano e non sostituiscono le norme di legge e le clausole della pattuizione collettiva in tema di sanzioni disciplinari. Le stesse potranno trovare attuazione a prescindere dalla rilevanza penale della

condotta inadempiente, fatte salve le previsioni normative sul rapporto tra procedimento disciplinare e procedimento penale.

Il sistema disciplinare prende in considerazione le oggettive differenze normative esistenti tra dirigenti, tutte le altre categorie di collaboratori, consulenti esterni e terzi che agiscono in nome e per conto di Coface SA

Va precisato che il suddetto sistema è stato predisposto nel rispetto degli artt. 2118 e 2119 c.c., della Legge n. 300/1970 (c.d. "Statuto dei lavoratori") e del vigente Contratto Collettivo Nazionale di Lavoro adottato in ambito aziendale. In particolare, la comminazione delle sanzioni previste dal sistema disciplinare tiene conto delle disposizioni applicabili per legge in relazione al Contratto Collettivo Nazionale di Lavoro adottato.

Il sistema disciplinare configurato da Coface SA, riferito alla violazione di regole di condotta previste nelle procedure organizzative aziendali, nel Codice di Condotta COFACE e nel presente Modello, adottate per prevenire la commissione dei reati di cui al Decreto, individua e definisce:

- le condotte inadempienti;
- le sanzioni applicabili alle diverse categorie di lavoratori della Società;
- i criteri di commisurazione delle stesse.

Il sistema disciplinare previsto nel presente Modello, dunque, è:

- correlato e riferito alla violazione degli obblighi imposti dalla legge, dal D. Lgs. 231/2001, dal Modello, dal Codice di Condotta COFACE e dalle procedure interne formalizzate dalla Società;
- complementare e non alternativo a quello stabilito dal CCNL applicato dall'Azienda ai lavoratori e dal codice disciplinare interno alla Società;
- portato a conoscenza di tutti i collaboratori e consulenti esterni di Coface SA da parte dell'Organo Amministrativo/Country Manager, nonché dei vari organi di controllo e di gestione, quali il Collegio Sindacale (ove nominato) e l'Organismo di Vigilanza stesso;
- conforme al principio del contraddittorio, che viene garantito tramite la previa pubblicità del Modello e l'applicazione della procedura prevista dall'art. 7 dello Statuto dei Lavoratori (in forza del quale l'eventuale irrogazione della sanzione disciplinare è preceduta dalla contestazione degli addebiti e dalla successiva assegnazione del termine di difesa);
- graduato in dipendenza e conseguenza delle violazioni commesse: le sanzioni disciplinari sono state elaborate e verranno applicate secondo la gravità dell'infrazione, tenendo conto di tutte le circostanze, oggettive e soggettive aggravanti e non, che hanno caratterizzato la condotta contestata, nonché dell'intensità della lesione del bene aziendale tutelato.

Inoltre, il sistema disciplinare dovrà attenersi ai principi di tempestività e tipicità e, pertanto, la contestazione e, se del caso, la relativa sanzione dovranno intervenire entro un termine

ragionevole; inoltre, le condotte contestate dovranno essere espressamente previste come sanzionabili dal Decreto o dal Modello organizzativo di Coface SA

Saranno ritenute sanzionabili anche le condotte finalizzate o idonee a violare, mettere a rischio o comunque eludere le procedure, i divieti e le prescrizioni del presente Modello e del Decreto, ovvero tese alla commissione di un reato previsto dal Decreto, ancorché il reato o la violazione delle prescrizioni del Modello e del decreto non si siano concretizzati.

Le sanzioni previste dal presente Sistema Sanzionatorio saranno, dunque, applicate ad ogni violazione del Modello, indipendentemente dall'instaurazione di un procedimento penali o dall'esito dello stesso.

Sono soggetti all'applicazione del sistema disciplinare l'Organo Amministrativo, il Preposto della Sede Secondaria, i Procuratori Speciali, i dirigenti, i dipendenti, i consulenti esterni, i collaboratori e i terzi in genere che abbiano rapporti contrattuali con la Società.

Il procedimento per l'irrogazione delle sanzioni di cui al presente sistema disciplinare tiene conto delle particolarità derivanti dallo *status* giuridico del soggetto nei cui confronti si procede. In ogni caso, l'OdV deve essere coinvolto nel procedimento disciplinare.

Laddove l'OdV dovesse essere destinatario di una segnalazione relativa ad un violazione del Modello, o ne dovesse venire a conoscenza durante la propria attività di vigilanza, sarà tenuto a svolgere tempestivamente tutti gli accertamenti del caso e, nel caso in cui dovesse ritenere sussistente una condotta fraudolenta, dovrà immediatamente darne notizia all'Organo Amministrativo/Country Manager, affinché proceda con le contestazioni nei confronti dell'autore e dia avvio all'iter disciplinare.

Il procedimento disciplinare è attribuito, in tutte le sue fasi, dalla contestazione degli addebiti, alla formulazione delle difese, alla irrogazione delle sanzioni, alla competenza dell'Organo Amministrativo e del Preposto della Sede Secondaria, nonché del Responsabile Risorse Umane, il quale, dovrà essere reso edotto nel procedimento a carico dei dipendenti e delle eventuali sanzioni irrogate.

7.1.1 Violazione del Modello: le condotte rilevanti

Ai fini del presente sistema disciplinare, si considerano violazione del Modello tutte le condotte, commissive od omissive (anche colpose), idonee a pregiudicare l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati c.d. presupposto.

Sono sanzionabili, inoltre, i tentativi di elusione del Modello 231.

La finalità del presente sistema disciplinare è quella di reprimere qualsiasi significativa violazione delle disposizioni contenute nel Modello e nel Codice di Condotta COFACE adottati dalla Società.

In particolare, sono sanzionabili:

- le violazioni delle procedure previste nel Modello adottato da Coface SA ovvero l'attuazione di comportamenti non conformi a quanto espressamente prescritto dal Modello (sia nel caso che espongano sia che non espongano la Società ad una situazione oggettiva di rischio di commissione di uno dei reati previsti);
- le condotte che espongano la società al rischio di commissione di uno dei reati presupposto ex D.lgs. 231/2001;
- la violazione dei principi e delle norme comportamentali contenute nel Codice di Condotta COFACE e nel Modello;
- la violazione delle procedure e regole di comportamento contenute del Regolamento Aziendale Generale;
- la violazione degli obblighi informativi previsti nei confronti dell'Organismo di Vigilanza;
- l'ingiustificato impedimento di accesso alle informazioni e alla documentazione nei confronti dei soggetti preposti ai controlli;
- l'assenza o non corretta vigilanza sulle condotte del personale che opera nel proprio ambito di responsabilità;
- l'omissione o violazione di qualsiasi prescrizione del Modello finalizzata a garantire la sicurezza e la salute nei luoghi di lavoro, ovvero a prevenire inquinamento o danno ambientale.

È sanzionato, inoltre, chiunque compia atti ritorsivi e discriminatori nei confronti di chi segnali violazioni del Modello 231, del Codice di Condotta COFACE e delle procedure interne.

Si ricorda, inoltre, che come disposto dal D.lgs. 24/2023, la tutela prevista in favore del Segnalante è estesa:

- ai facilitatori**, da intendersi quali persone fisiche che assistono il Segnalante nel processo di Segnalazione e che operano nel suo medesimo contesto lavorativo;
- alle persone del medesimo contesto lavorativo** del Segnalante, ad egli legate da uno stabile legame affettivo o di parentela entro il IV grado;
- ai colleghi di lavoro** del Segnalante che lavorano del medesimo contesto lavorativo e che hanno che egli un rapporto abituale e corrente;

- c. agli enti di proprietà del Segnalante o per i quali egli lavora, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

7.1.2. Principi generali di commisurazione delle sanzioni.

Le sanzioni irrogate a seguito dell'accertamento di una violazione del presente Modello e/o del Codice di Condotta COFACE dovranno essere proporzionate rispetto alla violazione commesse.

A tal fine, saranno valutati i seguenti elementi:

- gravità della violazione;
- tipologia di autore della violazione;
- gravità del pericolo e/o del danno cagionato alla Società;
- eventuale recidiva nella violazione.

7.1.3. Sanzioni applicabili ai Dipendenti

La violazione, da parte dei dipendenti soggetti al CCNL, delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei confronti di detti lavoratori - in conformità alle procedure di cui all'art. 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio in linea con il CCNL previsto, ossia:

- 1) biasimo inflitto verbalmente per le mancanze lievi;
- 2) biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui al precedente punto 1;
- 3) multa in misura non eccedente l'importo di 4 ore della normale retribuzione di cui all'art. 185;
- 4) sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;
- 5) licenziamento con preavviso;
- 6) licenziamento disciplinare senza preavviso.

L'applicazione della sanzione consistente nel licenziamento disciplinare deve essere coordinata con le disposizioni contenute nel D. Lgs. 23/2015.

Nei casi richiesti dalla natura della colpa o per necessità investigative, Coface SA – in attesa di decidere sul provvedimento disciplinare finale – ha la facoltà di sospendere temporaneamente il lavoratore dal servizio per il tempo strettamente necessario. Restano ferme – e si intendono qui richiamate – tutte le previsioni del CCNL applicate a seconda del rapporto di lavoro intercorrente, tra cui, in particolare:

- l'obbligo – in relazione all'applicazione di qualunque provvedimento disciplinare – della previa contestazione dell'addebito al dipendente e dell'assegnazione a quest'ultimo di un termine per la difesa. Tale termine non potrà essere inferiore a 5 giorni lavorativi dal ricevimento della contestazione;
- l'obbligo di consentire al Lavoratore di presentare, anche verbalmente, le proprie giustificazioni, con l'eventuale assistenza di un rappresentante dell'organizzazione sindacale cui aderisce o conferisce mandato;
- l'obbligo, entro 10 giorni dalla scadenza del termine assegnato al Lavoratore per la presentazione delle sue giustificazioni, di comunicare, al dipendente l'adozione del provvedimento disciplinare.

a) Biasimi verbali, biasimi scritti, multe e sospensioni

Incorre nei provvedimenti di biasimo, multa e sospensione il lavoratore che commette:

- violazione, che configuri lieve irregolarità, di una o più regole procedurali o comportamentali previste nel Modello o nel Codice di Condotta COFACE;
- violazioni che determinino un danno patrimoniale non grave alla Società (compresa l'integrità dei beni aziendali);
- qualsiasi mancanza che arrechi pregiudizio alla disciplina, alla morale, all'igiene relativamente agli obblighi previsti nel Modello e nel Codice di Condotta COFACE.

Le condotte sopra riportate costituiscono un'elencazione esemplificativa, e non esaustiva, delle condotte rilevanti ai dichiarati fini.

La multa è comminata quando vengono riscontrate mancanze di minor rilievo, la sospensione per quelle di maggior gravità o recidiva.

Per il lavoratore la sospensione si può applicare a quelle mancanze le quali, anche in considerazione delle circostanze speciali che le hanno accompagnate, non siano così gravi da rendere applicabile una maggiore punizione ma abbiano tuttavia tale rilievo da non trovare adeguata sanzione con misure meno afflittive.

b) Licenziamento

La sanzione del licenziamento, con immediata rescissione del rapporto di lavoro può essere inflitta, con la perdita dell'indennità di preavviso, ogni qualvolta il lavoratore commetta gravi infrazioni alla disciplina o alla diligenza nel lavoro o provochi alla Società grave nocumento morale o materiale che possa determinare la concreta applicazione a carico di Coface SA della responsabilità amministrativa delle persone giuridiche, o qualora il lavoratore compia in connessione con lo svolgimento del rapporto di lavoro azioni che costituiscano reato.

A titolo di esempio la sanzione è applicabile nei seguenti casi:

- grave insubordinazione o mancata osservanza degli ordini dei superiori;
- dolosa violazione o elusione di procedure con rilevanza esterna, (a titolo esemplificativo tale condotta può essere realizzata attraverso un comportamento diretto a realizzare inequivocabilmente uno dei reati di cui al D.Lgs. n. 231/2001);
- dolosa violazione o elusione del sistema di controllo, (a titolo esemplificativo tale condotta può essere realizzata mediante la distruzione od alterazione della documentazione relativa alla procedura, oppure impedendo l'accesso a documenti ed informazioni da parte degli organi preposti, compreso l'Organismo di Vigilanza).

Le condotte sopra riportate costituiscono un'elencazione esemplificativa, e non esaustiva, delle condotte rilevanti al dichiarato fine.

7.1.4. Sanzioni applicabili ai Dirigenti

In caso di mancato rispetto da parte dei Dirigenti, delle prescrizioni indicate nel Modello, la Società provvede ad applicare nei loro confronti le misure disciplinari più idonee, in conformità alle disposizioni di legge ed a quanto eventualmente stabilito dal CCNL per i Dirigenti.

Nei casi richiesti dalla natura della colpa o per necessità investigative, Coface SA – in attesa di decidere sul provvedimento disciplinare finale – ha la facoltà di sospendere temporaneamente il Dirigente dal servizio per il tempo strettamente necessario. Il rispetto di quanto previsto dal presente Modello costituisce adempimento fondamentale del contratto dirigenziale, pertanto, ogni violazione al presente Modello posta in essere da un Dirigente di Coface SA sarà considerata, ad ogni fine, come inadempimento grave.

Nello specifico, le sanzioni applicabili sono:

- **lettera di richiamo**: misura applicata nel caso siano ravvisati comportamenti, nell'espletamento di attività in aree a rischio, che costituiscano violazioni di grave entità rispetto alle disposizioni del Modello 231;
- **risoluzione del rapporto**: misura applicata qualora siano ravvisati comportamenti, nell'espletamento di attività in aree a rischio, che costituiscano violazioni di grave entità rispetto alle disposizioni del Modello 231.

Gli episodi di condotta illecita, qualora venga mantenuto il rapporto, devono, comunque, essere riportati nelle rispettive schede valutative.

Tale annotazione ha una duplice funzione: consente di archiviare e documentare eventuali recidive e, allo stesso tempo, tale annotazione potrà essere valutata ai fini del conferimento di ulteriori incarichi e deleghe, nonché in sede di elargizione di gratifiche, premi, benefit, aumento dei compensi.

7.1.5. Misure nei confronti degli Agenti⁵

L'accordo nazionale tra Agenti ed Imprese Assicuratrici non censisce provvedimenti sanzionatori. Solo l'Accordo Nazionale Agenti (A.N.A.) prevede in ipotesi (artt. 12, 1° comma, lett. e, e 18) tra le cause di cessazione del rapporto di agenzia il recesso per giusta causa, senza tuttavia il richiamo ad alcuna casistica specifica o a particolari regole procedurali.

La Compagnia ha, tuttavia, inteso regolamentare contrattualmente l'obbligo dell'Agente di prendere visione e conoscenza del Modello Organizzativo e del Codice di Condotta COFACE, e di osservarne diligentemente le norme. L'eventuale violazione delle disposizioni in essi contenute costituisce inosservanza degli obblighi derivanti dal rapporto di Agenzia, ed è sanzionata secondo quanto previsto nelle specifiche clausole inserite nel contratto di mandato.

Nei confronti dell'Agente che si renda responsabile delle predette violazioni, la Compagnia può, a seconda della gravità del comportamento, del livello di autonomia negoziale ed operativa dell'Agente, del fatto che si tratti di un'infrazione dolosa o colposa, nonché dell'eventuale esistenza di precedenti:

- emanare censura scritta, con richiamo al rispetto delle disposizioni violate;
- esercitare, nel caso in cui la violazione sia di entità tale da minare il rapporto di fiducia, il diritto di recesso dal mandato per giusta causa.

Resta salva l'eventuale richiesta di risarcimento qualora dall'illecito comportamento derivino o possano derivare danni alla Compagnia, come nel caso di applicazione nei confronti di quest'ultima delle sanzioni previste dal Decreto.

7.1.6. Sanzioni a carico dei Consulenti, agenti, collaboratori e soggetti terzi.

Come già più volte evidenziato nelle pagine precedenti, sono da considerarsi, a tutti gli effetti, Destinatari del presente Modello di Organizzazione, Gestione e Controllo anche i soggetti terzi che prestano la loro attività in favore della Società (Es. Consulenti, agenti, collaboratori).

Per tale ragione, è indispensabile che nei contratti stipulati tra Coface SA e questi soggetti, siano inserite specifiche clausole risolutive espresse che prevedano – appunto – lo scioglimento del contratto qualora le controparti contrattuali tengano comportamenti contrari con i principi contenuti nel presente Modello, cui Coface SA si attiene nello svolgimento dell'attività sociale, e integranti un pericolo di commissione dei reati indicati dal Decreto, salvo e impregiudicato comunque il diritto di Coface SA di chiedere il risarcimento del danno, qualora la condotta della

⁵ Per "Agente" si intende colei/colui che, a fronte di delega o sub-delega, gestisce l'attività di promozione e commercializzazione relativa ai prodotti di Compagnie française d'Assurance pour le commerce extérieur – Rappresentanza Generale per l'Italia.

controparte sia tale da determinare un danno a carico della Società, come nel caso di applicazione delle misure previste dal Decreto nei confronti della stessa da parte del giudice.

Pur rimandando al prosieguo per gli specifici protocolli preventivi, è opportuno ricordare che i clienti ed i fornitori, nonché i consulenti di Coface SA debbono essere previamente sottoposti a verifica, finalizzata a garantire che gli stessi agiscano nel rispetto della normativa applicabile. A tali fini, una copia del Modello (o delle parti di esso rilevanti per l'adempimento del contratto) deve essere resa disponibile alle controparti contrattuali.

6.1.6. Sanzioni nei confronti degli Amministratori e del Preposto della Sede Secondaria

In caso di violazione del presente Modello da parte dell'Organo Amministrativo e/o del Preposto della Sede Secondaria, l'OdV informa l'organo di controllo contabile, laddove nominato, il quale prende gli opportuni provvedimenti tra cui, in maniera esemplificativa, ma non esaustiva, la convocazione dell'assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

Laddove non sia presente alcuno organo di controllo contabile, l'OdV darà tempestiva comunicazione della violazione accertata allo stesso Organo Amministrativo, il quale provvede a convocare immediatamente l'assemblea dei soci per le determinazioni del caso.

6.1.7. Misure applicabili nei confronti dei membri dell'Organismo di Vigilanza

Qualora la violazione riscontrata sia imputabile ad un membro dell'Organismo di Vigilanza, gli altri componenti, ovvero chiunque venga a conoscenza di sue violazioni, segnala immediatamente l'accaduto al Preposto della Sede Secondaria o all'Organo Amministrativo, i quali adotteranno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico e la conseguente nomina di un sostituto, ovvero la revoca dell'interno Organismo e la conseguente nomina di un nuovo OdV.

Sono considerate infrazioni sanzionabili, ai sensi del presente sistema disciplinare, le ipotesi di grave negligenza o di imperizia da parte dei membri dell'OdV, che abbiano dato luogo ad omesso controllo sull'attuazione, sul rispetto e sull'aggiornamento del Modello.

7.2. PROCEDURA PER L'ACCERTAMENTO DELLA VIOLAZIONE, CONTESTAZIONE DISCIPLINARE E IRROGAZIONE DELLE SANZIONI

Il procedimento di accertamento delle violazioni, di contestazione disciplinare e di irrogazione delle sanzioni è strutturato secondo le seguenti fasi:

- rilevazione ovvero segnalazione di violazione effettiva o presunta delle procedure e/o prescrizioni di cui al Modello e/o delle regole o dei principi del Codice di Condotta COFACE;
- fase preistruttoria, diretta a verificare la fondatezza della Segnalazione;

- fase istruttoria, diretta ad accertare la fondatezza della violazione sulla base delle risultanze dell'attività d'istruzione;
- fase di contestazione ed eventuale irrogazione della sanzione.

Ogni violazione del Modello e/o del Codice di Condotta COFACE, da chiunque commessa, dovrà essere immediatamente segnalata per iscritto all'OdV, il quale dovrà valutare la necessità di modifiche o adeguamenti del Modello, al fine di evitare la consumazione di reati della stessa specie o indole.

Nel caso in cui le violazioni del Modello e del Codice di Condotta COFACE dovessero essere rilevate ed accertate direttamente ad opera dell'Organo Amministrativo o del Preposto alla Sede Secondaria, questo sarà tenuto a darne tempestiva comunicazione all'OdV, al fine di consentire a quest'ultimo di valutare eventuali modifiche o integrazioni da apportare alle procedure e protocolli.

Come già anticipato, qualora dovesse pervenire all'OdV segnalazione di violazioni del Modello, egli dovrà porre in essere gli accertamenti che riterrà più appropriati e, svolte le opportune analisi e valutazioni, dovrà informare l'Organo Amministrativo e il Preposto alla Sede Secondaria, affinché si proceda, alternativamente, all'archiviazione della segnalazione, ovvero alla contestazione della stessa e alla eventuale applicazione della relativa prescritta sanzione.

7.2.1 Dovere di segnalazione degli illeciti e procedura disciplinare

Tutti i soggetti indicati nei precedenti paragrafi, ed in generale tutti gli *stakeholder* di Coface SA devono segnalare all'OdV qualora ne vengano in qualsiasi modo a conoscenza, ogni violazione consumata o tentata, o ogni sospetto di violazione, dei principi enunciati dal presente Modello, delle disposizioni contenute nel Codice di Condotta COFACE ed in generale delle regole e *policy* aziendali.

L'OdV analizza la segnalazione, ascoltando eventualmente l'autore della stessa ed i soggetti coinvolti nel fatto. Durante lo svolgimento dell'intero procedimento disciplinare, l'OdV si conforma a quanto previsto dalla normativa vigente e dal C.C.N.L. di categoria.

L'OdV agisce in modo da scongiurare qualsiasi tipo di ritorsione, intendendosi quest'ultima come qualsiasi atto che possa dar adito anche al solo sospetto di discriminazione o penalizzazione operata nei confronti dei denunciati. A tal proposito è altresì assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Compagnia.

L'OdV compie gli opportuni accertamenti in merito alle condotte oggetto di segnalazione, o a quelle rilevate come illecite a fronte della periodica attività di monitoraggio esercitata. Qualora

tali indagini evidenziassero la commissione o il tentativo di commissione di un'infrazione, l'OdV ne dà pronta comunicazione al Rappresentante della Sede Secondaria, cui compete l'eventuale informativa al Consiglio di Amministrazione.

Il Rappresentante provvede con celerità ad analizzare la violazione di cui si tratta ed a definire la più adeguata conseguenza sanzionatoria. Stabilita in tal modo la sanzione da comminare, la Direzione del Personale ne cura l'immediata applicazione, e viene supportata dall'OdV nella verifica della sua esecuzione.

8. INFORMAZIONE E FORMAZIONE DEL PERSONALE

8.1 Premessa

Elemento fondante di un corretto funzionamento del Modello di Organizzazione, Gestione e Controllo, è la sua divulgazione tra i Destinatari e la conseguente attività di formazione ad essi rivolta, avente ad oggetto i contenuti del documento ed i principi introdotti dal Decreto.

L'obiettivo che la Compagnia si prefissa è di svolgere tali attività nei confronti della totalità dei destinatari, a prescindere dal momento in cui abbia avuto inizio il loro rapporto con la Compagnia. A tale scopo, in fase di prima edizione, il documento – unitamente al Codice di Condotta COFACE – è stato distribuito a tutti i dipendenti ed alla Rete Agenziale.

Diversamente, per tutti i rapporti di lavoro instaurati e per tutti i contratti di agenzia conclusi successivamente a tale momento, il Modello ed il Codice di Condotta COFACE sono consegnati in fase di sottoscrizione del rapporto. In tale sede il destinatario si impegna a prendere visione e conoscenza dei citati documenti e si obbliga ad osservarne diligentemente il contenuto.

I momenti formativi sono periodicamente organizzati dalla Compagnia, per tramite della Direzione delle Risorse Umane. La partecipazione ai programmi di formazione è obbligatoria e l'OdV, con il supporto della Direzione organizzante, ne verifica i contenuti e l'effettiva frequenza da parte dei destinatari.

Al fine di garantire la maggior diffusione possibile del Modello e del Codice di Condotta COFACE, nonché dei principi cui l'attività aziendale si ispira, copia degli stessi è stata pubblicata nella Intranet Aziendale e sul sito istituzionale della Compagnia: www.Coface SA.it.

8.2 Formazione e comunicazione ai destinatari

L'indicata attività di formazione è pianificata, con il supporto del Servizio del Personale, e sentite le Direzioni di Compagnia, sulla base delle differenti qualifiche, funzioni e ruoli ricoperti dai destinatari, nonché del livello di rischio delle aree in cui essi operano. Qualora lo ritenga utile o necessario l'Azienda, nella determinazione dei contenuti e nel materiale svolgimento dei

momenti formativi, può farsi supportare dall'attività di consulenti esterni. Per quanto attiene la Rete Agenziale, posto che essa è costituita da persone giuridiche autonome e distinte rispetto alla Compagnia, quest'ultima con un'apposita integrazione del mandato agenziale – ha inteso chiarire la valenza contrattuale del Modello e del Codice di Condotta COFACE specificando che una loro violazione costituisce inosservanza degli obblighi derivanti dal rapporto di Agenzia.

Lo stesso criterio è stato adottato per la scelta dei fornitori cui esternalizzare processi aziendali: la loro disponibilità a sottoscrivere il Modello ed il Codice di Condotta COFACE della Compagnia costituisce elemento fondante la loro valutazione complessiva.

Il contenuto del Modello e del Codice di Condotta COFACE è altresì comunicato alla società di revisione, ai consulenti ed alle altre entità italiane del Gruppo Coface SA, in modo che tali soggetti vengano resi edotti delle conseguenze derivanti dalla violazione dei principi e delle disposizioni in essi contenute. L'OdV esercita la necessaria verifica sulla completezza del piano di formazione sia a livello di contenuti che di destinatari.

8.3 Comunicazione al pubblico

In aggiunta alla menzionata pubblicazione del Modello e del Codice di Condotta COFACE sul sito internet della Compagnia, l'OdV verifica che siano predisposti ed adottati ulteriori strumenti idonei a consentire alle terze parti, di conoscere i documenti adottati dalla Compagnia in esecuzione di quanto contenuto nel Decreto.

In tal modo Coface SA intende mettere a parte gli stakeholder dei principi etici e comportamentali su cui si fonda la propria attività imprenditoriale.

PARTE SPECIALE

1. PREMESSE

La Parte Speciale del Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/2001 ha come finalità quella di individuare ed analizzare i reati-presupposto che, a seguito delle attività di *Risk Assessment*, si ritengono a rischio consumazione, rispetto alle attività aziendali, nonché identificare dei Protocolli e delle Procedure, alle quali il personale della Società e i Destinatari del Modello in generale, dovranno attenersi, al fine di prevenire e limitare la consumazione di tali illeciti penali.

Al fine di pervenire alla corretta mappatura dei profili di rischio riconducibili alla realtà societaria di Coface SA, si è provveduto ad analizzare, *in primis*, il *business* della Società, per poi esaminare le singole aree di attività, intervistando i Responsabili delle funzioni, la “*governance*” societaria e la sua struttura organizzativa, verificando la distribuzione di poteri e funzioni tra il personale della Società.

Per ciascun processo aziendale sono state individuate le categorie di reato-presupposto ex D.lgs. 231/2001 ritenute a rischio consumazione.

Nello specifico, si ritengono, in astratto, a rischio commissione le seguenti famiglie di reati:

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell’Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24 D.lgs. 231/2001);
2. Delitti informatici e trattamento illecito di dati (Art. 24-bis D.lgs. 231/2001);
3. Delitti di criminalità organizzata (Art. 24-ter D.lgs. 231/2001);
4. Peculato, concussione, induzione a dare o promettere utilità, corruzione e abuso d’ufficio (Art. 25 D.lgs. 231/2001);
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis D.lgs. 231/2001);
6. Delitti contro l’industria e il commercio (Art. 25-bis 1 D.lgs. 231/2001);
7. Reati societari (Art. 25-ter D.lgs. 231/2001);
8. Reati di abuso di mercato (Art. 25-sexies D.lgs. 231/2001);
9. Reati di omicidio e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro (Art. 25-septies D.lgs. 231/2001);

10. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-*octies* D.lgs. 231/2001);
11. Delitti in materia di violazione del diritto d'autore (Art. 25-*novies* D.lgs. 231/2001);
12. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-*decies* D.lgs. 231/2001);
13. Reati ambientali (Art. 25-*undecies* D.lgs. 231/2001);
14. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-*duodecies* D.lgs. 231/2001);
15. Reati tributari (Art. 25-*quinquiesdecies* D.lgs. 231/2001).

In ragione della natura delle attività e delle caratteristiche della Società, non sembra che, allo stato, possano sussistere concreti ed attuali profili di rischio rispetto alle macro-categorie di reato di seguito indicate.

Tali illeciti sono, in ogni caso, complessivamente presidiati dalle disposizioni di cui al Codice di Condotta COFACE e di Comportamento, nonché dalle procedure e protocolli al Modello di Organizzazione, Gestione e Controllo:

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* D.lgs. 231/2001);
- Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater* 1 D.lgs. 231/2001);
- Delitti contro la personalità individuale (art. 25-*quinqüies* D.lgs. 231/2001);
- Delitti in materia di strumenti diversi dai contanti (Art. 25-*octies* 1. D.lgs. 231/2001);
- Razzismo e xenofobia (art. 25-*terdecies* D.lgs. 231/2001);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies* D.lgs. 231/2001);
- Contrabbando (Art. 25-*sexiesdecies* D.lgs. 231/2001);
- Delitti contro il patrimonio culturale (art. 25-*septiesdecies* D.lgs. 231/2001);
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-*duodevicies* D.lgs. 231/2001).
- Reati commessi in modalità transnazionale (art. 10 L. 146/2006);
- Reati per enti che operano nell'ambito della filiera degli oli vergini di oliva (art. 12 L. n. 9/2013).

Si espongono di seguito le linee guida generali che regolano:

- i presidi messi in atto al fine di ostacolare il compimento di condotte illecite;
- i comportamenti prescritti a carico dei "Destinatari";
- l'attività dell'OdV

Rimandando ai capitoli dedicati ai singoli reati eventuali integrazioni specifiche.

1.1. I presidi messi in atto allo scopo di ostacolare il compimento di condotte illecite

CODICE DI CONDOTTA COFACE

Il Codice di Condotta COFACE, adottato da Coface SA, individua i principi e valori fondamentali, nonché criteri di condotta da seguire nell'espletamento delle attività aziendali allo scopo di mitigare il rischio di realizzazione di condotte illecite.

SISTEMA DI CONTROLLO INTERNO

Il Sistema di Controllo Interno dell'Azienda è importante al fine di verificare quali presidi siano stati adottati allo scopo di ostacolare il compimento di condotte illecite. In particolare, sono presi in esame i componenti del SCI (sistema organizzativo, autorizzativo, procedure, sistema di controllo di gestione) esistenti nella Compagnia.

Nella Parte Speciale del Modello per ciascun reato (o gruppi di reati) è esaminato se il SCI esistente sia efficiente ed efficace allo scopo di prevenire ciascun specifico reato all'esame. Dall'esame effettuato è risultato:

- per quanto riguarda il Sistema Organizzativo l'esistenza di aggiornato organigramma e di mansionari che assicurano una chiara definizione di ruoli e responsabilità; l'esistenza di Circolari Ordini di Servizio che garantiscono un corretto sistema di diffusione dei principi organizzativi aziendali;
- per quanto riguarda il Sistema Autorizzativo l'esistenza di un equilibrato apparato delegatorio che assicura una chiara definizione di poteri e responsabilità verso l'interno e verso l'esterno;
- per quanto riguarda il Sistema dei Controlli l'esistenza di funzioni che svolgono controlli di II° e III° livello normati da linee guida della Sede nell'abito di predefiniti programmi, nonché l'esistenza di apposito ufficio dedicato al controllo di gestione che garantisce il controllo dell'operatività quotidiana e il raffronto con le previsioni;
- per quanto riguarda il Sistema delle Procedure l'esistenza di:
 - linee guida (procedure di gruppo) emanate dalla Sede che garantiscono chiare e collaudate istruzioni operative sia nelle aree tecniche che amministrative che gestionali;
 - un piano di aggiornamento delle procedure locali che garantisce di colmare il gap riscontrato in sede di analisi determinato dalle recenti trasformazioni aziendali;
 - procedure indirizzate ad ostacolare la creazione di fondi neri (che disciplinano l'intero processo di redazione e gestione dei contratti di acquisto e fornitura);

- procedure rivolte all'analisi e alla conoscenza delle controparti (partner commerciali, fornitori, intermediari) e alla raccolta dei dati della clientela in fase negoziale (Modello di proposta compilabile);
- procedure indirizzate al controllo dei flussi finanziari aziendali (versamenti destinati a terzi, operazioni infragruppo, procedure di verifica della regolarità delle erogazioni);
- linee guida per la redazione e la gestione dei contratti di acquisto e fornitura;
- linee guida in materia di scelta dell'affidamento in outsourcing di attività aziendali;

Grazie alla predisposizione dell'apposita procedura sopra menzionate la Compagnia ha potuto disciplinare le fasi che caratterizzano l'esternalizzazione di attività che dettano i criteri di selezione dell'outsourcer, le modalità di monitoraggio della prestazione erogata, e la conseguente verifica della fatturazione.

Così operando, la Compagnia ha la possibilità di disporre di un costante ed efficiente monitoraggio dei propri fornitori, riducendo così al minimo la possibilità che quest'ultimi possano essere destinatari di fondi distratti per fini illeciti.

La Società ha inoltre introdotto opportune clausole contrattuali finalizzate all'osservanza da parte dei fornitori delle norme di legge a prevenzione dei reati previsti dal Decreto.

In particolare, la Società verifica, che i partner commerciali rispettino gli obblighi di legge in tema di: tutela del lavoro minorile, condizioni igienico sanitarie e di sicurezza, diritti sindacali.

1.2. I comportamenti a carico dei destinatari

La predisposizione della mappa dei rischi alla luce dei principi di controllo sopra indicati ha evidenziato che la Compagnia possiede i sufficienti elementi organizzativi per contenere e controllare i rischi.

Le raccomandazioni espone nella sezione "Gap Analysis" si ispirano all'esigenza di osservare i rischi cui la Società (anche teoricamente) è esposta e di effettuare l'opportuna attività di manutenzione del SCI che tutte le aziende debbono programmare per sempre migliorare e adeguare il livello di controllo alla mutevole realtà aziendale.

I principi di comportamento di seguito indicati sono rivolti ai "Destinatari" allo scopo di ostacolare il compimento di condotte illecite.

Sono Destinatari gli Amministratori Operativi, il Rappresentante della Sede Secondaria, i Dirigenti, i Dipendenti e i terzi con cui Coface SA intrattiene rapporti di natura contrattuale quali ad esempio i consulenti, agenti, rappresentanti che svolgono a qualsiasi titolo le attività a rischio reato.

Le norme di comportamento cui i “Destinatari” debbono attenersi si distinguono in:

- Norme e principi di comportamento generali (da osservare in qualunque area);
- Norme e principi di comportamento specifici (da osservare nell’espletamento dell’attività di particolari aree).

Si indicano di seguito i principi di comportamento generali cui i destinatari debbono uniformarsi (nei capitoli dedicati alle singole aree a rischio saranno indicati i principi di comportamento da tenere nella gestione peculiare dell’area):

- ogni decisione e ogni contatto finalizzato ad effettuare attività a rischio reato risulta da un documento (quale, ad esempio, il mansionario) o da una direttiva scritta, adottati mediante autorizzazione di soggetto legittimamente e correttamente investito dei relativi poteri autorizzativi;
- ciascun Destinatario coinvolto nell’esercizio di un’Attività a rischio reato deve predisporre evidenze scritte che comprovino l’attività svolta e da svolgere;
- non vi deve mai essere identità soggettiva tra coloro che decidono e pongono concretamente in essere un’attività a rischio reato e coloro che risultano investiti del potere di destinarvi le necessarie risorse economiche e finanziarie, risultando le funzioni aziendali preposte a tali attività formalmente e fattivamente separate;
- l’utilizzo di risorse economiche e finanziarie è sempre puntualmente contabilizzato, in modo da averne debita evidenza scritta.

Fermo quanto precede, è, in ogni caso, fatto espresso obbligo ai Destinatari di rispettare le procedure che disciplinano specificamente i comportamenti che i medesimi devono tenere per evitare la commissione delle fattispecie criminose previste dal D.Lgs.231/2001.

In generale, è assolutamente vietato ai Destinatari:

- porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente, integrino, direttamente o indirettamente, anche solo in astratto o in via potenziale, i reati previsti dal D.Lgs. n. 231/01 specificati nelle parti speciali del presente modello;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé ipotesi di reato, possano esserne il presupposto (ad esempio, mancato controllo) o possano potenzialmente diventare fattispecie di reato;
- porre in essere comportamenti non conformi alle procedure aziendali o, comunque, non in linea con i principi e le disposizioni contenute nel Modello e nel Codice di Comportamento.

1.3. L’attività dell’Organismo di Vigilanza

Flussi informativi verso l’Organismo di Vigilanza

L'OdV per svolgere l'attività di vigilanza sul funzionamento e l'osservanza del modello deve periodicamente ricevere segnalazioni e informazioni da parte dell'azienda.

Tali segnalazioni si distinguono in:

- segnalazioni di carattere generale (relative a tutte le aree);
- segnalazioni specifiche (che riguardano particolari aree).

Si indicano di seguito le segnalazioni di carattere generale da inoltrare all'OdV (nei capitoli dedicati alle singole aree a rischio saranno indicate le informazioni peculiari dell'area da trasmettere):

- le operazioni straordinarie della società;
- i provvedimenti assunti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, nei confronti di membri degli organi sociali, dipendenti, collaboratori, agenti, consulenti di Coface SA dipendenti delle altre entità italiane del Gruppo, che abbiano ad oggetto attività svolte per conto o nell'interesse di Coface SA;
- l'esecuzione di attività aziendali che possono esporre la Compagnia al rischio di una violazione – dolosa o colposa – del Decreto;
- le eventuali ispezioni subite (ASL, Agenzia Entrate, Guardi di Finanza, Vigili del Fuoco, ACPR, IVASS, INPS, INAIL, Garante Privacy, Vigili Urbani, Carabinieri...);
- i procedimenti disciplinari aperti dalla Compagnia, il loro esito e le eventuali sanzioni applicate;
- la politica remunerativa in essere e le assunzioni effettuate nell'anno;
- l'esito dei controlli effettuati sulle varie funzioni aziendali, sulla rete agenziale, sui consulenti, sulle altre entità italiane del Gruppo Coface SA o sulle società di outsourcing, nel caso in cui si delineino elementi di criticità in ordine al rispetto del Decreto.

Coloro che svolgono una funzione di controllo e supervisione devono:

- riferire immediatamente all'OdV eventuali situazioni di irregolarità riscontrate;
- riferire con periodicità da concordare all' OdV l'avvenuta predisposizione e/o implementazione di procedure e, in generale la messa in opera delle misure di miglioramento del sistema di controllo interno consigliate a seguito della predisposizione della Mappa dei Rischi.

Flussi informativi dall'Organismo di Vigilanza al Vertice

Nella parte Generale del Modello sono stati indicati i fondamentali flussi informativi dovuti dall'OdV ai Vertici aziendali:

- infrazioni al Codice di Condotta COFACE, al Modello e alle Procedure (da effettuare al

verificarsi dell'evento);

- relazione sull'attività svolta (da effettuare con periodicità concordata).

Si espongono di seguito nozioni sull'attività che l'OdV svolge

Attività dell'Organismo di Vigilanza

Per poter svolgere correttamente la sua attività l'OdV con continuità deve effettuare:

- Attività di controllo e monitoraggio sull'osservanza del Modello in generale;
- Attività di controllo e monitoraggio in specifiche aree.

Si indica di seguito schematicamente l'attività di controllo generale in capo all'OdV (nei capitoli dedicati alle singole aree a rischio saranno evidenziate specifiche attività che l'OdV deve espletare):

- esaminare eventuali segnalazioni pervenute e disporre gli accertamenti ritenuti necessari e le eventuali comunicazioni al Rappresentante della Sede Secondaria o dal Consiglio di Amministrazione;
- verificare periodicamente il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al responsabile di funzione od ai sub responsabili;
- verificare periodicamente, l'osservanza da parte dei Destinatari dei contenuti del Modello e del Codice di Condotta COFACE e l'attuazione dei previsti meccanismi sanzionatori qualora si accertino violazioni delle prescrizioni;
- verificare periodicamente la validità e l'applicazione delle procedure emesse finalizzate a garantire l'osservanza da parte dei Collaboratori delle disposizioni del D.Lgs. n. 231/01;
- effettuare controlli volti a verificare la regolare gestione del processo di liquidazione dei sinistri (completezza della documentazione, esistenza dei presupposti per la liquidazione, correttezza degli importi erogati e loro esatta destinazione);
- indicare, nel rispetto di quanto previsto nella Parte Generale del Modello, al Rappresentante della Sede Secondaria o al Consiglio di Amministrazione, laddove riscontri nella pratica delle carenze, le eventuali necessarie integrazioni ai sistemi di gestione finanziaria già presenti, con l'evidenza degli accorgimenti opportuni a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

I REATI PRESUPPOSTO RILEVANTI PER COFACE SA

A) REATI IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (Artt. 24 e 25 D.lgs. 231/2001)

Con riferimento ai “Reati in danno allo Stato o di altro Ente Pubblico”, considerando, che Coface SA, in virtù della attività sociale prestata, opera sotto la diretta vigilanza dell’IVASS, con iscrizione all’elenco delle imprese assicuratrici estere in regime di stabilimento e che il 90% delle cauzioni concesse ai propri Clienti hanno come beneficiario Amministrazioni Pubbliche, è evidente come il rischio di consumazione di tali delitti appaia alto.

Inoltre, nonostante ad oggi, Coface SA non abbia mai richiesto o ottenuto sovvenzioni/fondi/mutui agevolati, da parte dello Stato italiano o di Enti Europei, non può escludersi, aprioristicamente, che ciò non avvenga in futuro.

Di seguito saranno, sinteticamente, descritte le singole fattispecie di reato ex artt. 24 e 25 D.lgs. 231/2001 e individuate alcune possibili modalità attuative.

* * *

1.1. Malversazione a danno dello Stato o della Unione Europea (art. 316 bis Cod. Pen.) Fattispecie

Tale reato si configura laddove, chi, estraneo alla Pubblica Amministrazione, dopo aver legittimamente ricevuto contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, da parte dello Stato italiano o da altro ente pubblico o dalle Comunità europee, non utilizzi le somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell’aver distratto, anche parzialmente, la somma ottenuta; nessun rilievo assume il fatto che l’attività programmata si sia comunque svolta).

Ovviamente si fa riferimento ad erogazioni con vincolo di destinazione, dato che la condotta censurata e aver utilizzato le somme, per scopi o finalità diverse da quelle previste.

Il reato *de quo* si configura anche nel caso in cui le somme ottenute siano destinate a finalità pubbliche diverse da quelle destinataria dell’erogazione.

Finalità della norma è, dunque, garantire il corretto uso delle finanze pubbliche.

È importante sottolineare come il reato ex art. 316-bis Cod. Pen. si differenzia dal reato di “Truffa aggravata per il conseguimento di erogazioni pubbliche” ex art. 640-bis Cod. Pen., in quanto quest’ultimo si configura a seguito di artifici e raggiri tesi all’ottenimento dell’erogazione pubblica, mentre il primo sussiste allorché somme legittimamente ottenute siano distratte dalla loro finalità destinata.

1.2. Indebita percezione di erogazioni in danno dello Stato o della UE (art. 316 ter Cod. Pen.)

Il reato in oggetto si configura nei casi in cui - mediante l’utilizzo o la presentazione di dichiarazioni o di documenti falsi o l’omissione di informazioni dovute - si ottengano, per sé o

per altri, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato o da altri enti pubblici o dalle Comunità europee. È irrilevante l'uso che venga fatto delle erogazioni, poiché il reato si consuma nel momento in cui vengono ottenuti indebitamente i finanziamenti.

Questa ipotesi di reato è sussidiaria rispetto alla più grave fattispecie di "Truffa ai danni dello Stato" ex art. 640 comma II n. 1 Cod. Pen., in quanto, a differenza del reato più grave, il delitto ex art. 316 ter Cod. Pen., non richiede che vengano posti in essere artifici o raggiri, difettando quindi gli elementi tipici della Truffa.

1.3. Truffa aggravata in danno dello Stato o di altro ente pubblico o delle Comunità Europee (art. 640, comma 2, n. 1 Cod. Pen.)

Tale delitto sussiste laddove, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto cagionando un danno allo Stato, ad altro ente pubblico o all'Unione Europea.

A differenza del reato precedentemente analizzato, ritroviamo gli elementi propri del reato di "Truffa", quali gli artifici e i raggiri, l'altrui errore e l'ingiusto profitto con altrui danno.

Per "artificio" va intesa un'alterazione della realtà esteriore che si realizza simulando l'inesistente o dissimulando l'esistente.

Per "raggiro", invece, si intende una menzogna che influisce direttamente sulla psiche del soggetto passivo, prospettando una realtà diversa da quella che realmente è.

1.4. Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis Cod. Pen.)

Il reato si configura nel caso in cui la truffa sia posta in essere per conseguire contributi, sovvenzioni, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Se a primo sguardo i reati ex artt. 640 comma 2 n.1 e 640- bis, possano sembrare identici, sanzionando la stessa condotta, in realtà il secondo contiene un elemento di specialità rispetto al primo, ed invero, gli artifici e/o i raggiri sono finalizzati ad ottenere un'erogazione pubblica, non essendo "sufficiente", dunque, un generico danno nei confronti della Stato, ente pubblico o Comunità europea.

1.5. Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter Cod. Pen.)

Il reato ex art. 640 ter punisce chiunque, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto.

Tale delitto rileva ai fini della responsabilità amministrativa dell'ente esclusivamente laddove il danno sia realizzato in danno allo Stato, ad altro ente pubblico o all'Unione Europea.

Il delitto di “Frode informatica” si differenzia del reato di “Truffa” in quanto non sussiste l’evento intermedio dell’induzione in errore e le condotte di “artifici e raggiri” sono sostituite da due comportamenti alternativi, come l’alterazione del funzionamento di un sistema informatico o telematico e un qualsiasi intervento senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico.

Va precisato come per “alterazione del funzionamento di un sistema informatico o telematico” si intenda la commissione di tutte quelle condotte idonee a provocare un irregolare funzionamento del processo di elaborazione o trasmissione dei dati.

1.6 Frode nelle pubbliche forniture (art. 356 Cod. Pen.)

Tale delitto si configura nel caso in cui chiunque ponga in essere una frode nell’esecuzione dei contratti di fornitura o nell’adempimento degli altri obblighi contrattuali conclusi con lo Stato, o con un altro ente pubblico, ovvero con un’impresa esercente servizi pubblici o di pubblica necessità.

Tale delitto si configura in riferimento a qualsiasi tipo di contratto di fornitura, compresi i contratti di compravendita, somministrazione e appalto.

È importante chiarire il concetto di frode, che non va inteso quale sinonimo di “artifici o raggiri,” ma quale violazione degli obblighi di buona fede dell’esecuzione del contratto.

Tale reato sussiste allorché il reo vuole far apparire, contrariamente al vero, il corretto adempimento del contratto.

1.7. Concussione (art. 317 Cod. Pen.)

Il reato si configura nel caso in cui un Pubblico Ufficiale o un Incaricato di Pubblico Servizio, abusando della propria qualità o dei propri poteri, costringa taluno a dare o a promettere indebitamente a sé o a un terzo denaro o altre utilità.

Il delitto *de quo* è un reato proprio e, pertanto, la Società ne risponderà esclusivamente laddove un soggetto apicale o subordinato agisca in concorso con il pubblico ufficiale o con l’incaricato di un pubblico servizio.

È importante soffermarci sulla condotta criminosa oggetto del presente delitto e, in particolare, sul significato da attribuire all’espressione “costrizione”. Essa non va intesa quale violenza fisica, ma quale violenza morale esercitata dal pubblico ufficiale o dall’incaricato di pubblico servizio, per annullare il processo volitivo di altro soggetto.

1.8. Corruzione per l’esercizio della funzione (Art. 318 Cod. Pen.)

Commette il reato di cui alla fattispecie in esame, il Pubblico Ufficiale, che, in relazione all’esercizio delle sue funzioni o dei suoi poteri, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa.

Le ipotesi di corruzione, previste ai sensi del Decreto, devono essere valutate sotto un duplice profilo:

- corruzione attiva, allorché un dipendente della Società corrompa un Pubblico Ufficiale od Incaricato di Pubblico Servizio per l'ottenimento di qualche vantaggio a favore della Società medesima (es: affinché non siano rilevate eventuali irregolarità emerse nel corso di un'ispezione);
- corruzione passiva, allorché un dipendente della Società, in qualità di Pubblico Ufficiale o Incaricato di Pubblico Servizio, riceva denaro o la promessa di denaro od altra utilità per compiere atti contrari ai doveri del proprio ufficio. Quest'ultima ipotesi è circoscritta alle sole ipotesi, in cui la società o ente sia controllata pubblica o, in virtù dell'attività svolta vada ad acquisire i connotati dell'esercente di una pubblica funzione.

Si configura il delitto di Corruzione allorché le parti, essendo in posizione paritaria fra di loro, pongono in essere un vero e proprio accordo, diversamente da quanto accade nell'ipotesi di concussione che, al contrario, presuppone lo sfruttamento da parte del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio della propria posizione di superiorità che si contrappone alla posizione di soggezione del privato.

Tali condotte potrebbero concretizzarsi, ad esempio, tramite l'assunzione di personale segnalato dal Pubblico Ufficiale o dall'Incaricato di Pubblico Servizio, mediante il riconoscimento al Pubblico Ufficiale od all'Incaricato di Pubblico Servizio o a terzi a questi ricollegabili di compensi non in linea con la prestazione/fornitura erogata, mediante l'emissione di fatture a fronte di prestazioni/operazioni inesistenti, attraverso la corresponsione di rimborsi spese fittizi, presentati anche attraverso consulenti, oppure mediante la fittizia assegnazione di beni a titolo di omaggio o liberalità.

1.9. Corruzione per un atto contrario ai doveri d'ufficio (Art. 319 Cod. Pen.)

Commette il reato di cui alla fattispecie in esame, il Pubblico Ufficiale che, per omettere o ritardare o per aver ommesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

1.10. Corruzione in atti giudiziari (Art. 319 ter Cod. Pen.)

Il reato de *quo* si configura allorché i fatti di corruzione, indicati negli artt. 318 e 319 Cod. Pen., siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. La pena è aumentata se dal fatto deriva l'ingiusta condanna di taluno.

L'espressione "atti giudiziari" deve essere intesa secondo un'ampia interpretazione rientrando in tale categoria tutti quegli atti che, direttamente o indirettamente, siano idonei ad influire sull'esito di un dato processo.

La Giurisprudenza, sul punto, ad esempio, ha specificato che sia da intendersi quale atto giudiziario anche il parere espresso dal medico penitenziario sulle condizioni di salute di un imputato detenuto.

Ciò che differenzia tale delitto dai reati di corruzione ex artt. 318 e 319 Cod. Pen. è che il *pactum sceleris* sia finalizzato a favorire una parte processuale.

Importante sottolineare per “parte in un processo penale” va inteso anche l’indagato.

1.11. Induzione indebita a dare o promettere utilità (Art. 319 *quater* Cod. Pen.)

Tale articolo è stato introdotto dalla Legge 190/2012 e punisce il pubblico ufficiale o l’incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità, salvo che il fatto costituisca più grave reato.

Tale reato si differenzia dal delitto di “Concussione” ex art. 317 Cod. Pen., in quanto la condotta posta in essere dal pubblico ufficiale o dall’incaricato del pubblico servizio si concretizza in una mera induzione e non in una costrizione, come previsto per la concussione.

L’induzione sussiste laddove il privato venga “convinto”, dall’autore del reato, alla prestazione senza subire alcuna compressione nel suo processo volitivo.

Diversamente da quanto previsto per il reato di “Concussione”, risponde di “Induzione indebita” non solo il pubblico ufficiale o l’incaricato di un pubblico servizio, ma anche il privato che dà o promette denaro o altra utilità. Ciò avviene, in quanto, in tale fattispecie, non si verifica un totale annullamento della sua volontà.

1.12. Corruzione di persona incaricata di un pubblico servizio (Art. 320 Cod. Pen.)

Le disposizioni di cui all’art. 318 e 319 Cod. Pen. si applicano anche all’Incaricato di un Pubblico Servizio.

1.13. Pene per il corruttore (Art. 321 Cod. Pen.)

La disposizione prevede che le pene stabilite nel primo comma dell’art. 318 Cod. Pen., nell’art. 319 Cod. Pen., nell’art. 319 *bis* Cod. Pen., nell’art. 319 *ter* Cod. Pen., e nell’art. 320 Cod. Pen., in relazione alle suddette ipotesi degli artt. 318 e 319 Cod. Pen. si applichino anche a chi dà o promette al Pubblico Ufficiale od all’Incaricato di un Pubblico Servizio denaro o altra pubblica utilità.

1.14. Istigazione alla corruzione (Art. 322 Cod. Pen.)

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso denaro o altra utilità ad un Pubblico Ufficiale od Incaricato di Pubblico Servizio (per indurlo a compiere, omettere, ritardare ovvero a fare un atto contrario ai doveri del suo ufficio) e tale offerta o promessa non venga accettata.

1.15. Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati Esteri (Art. 322 *bis* Cod. Pen.)

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

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

- (2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- (3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- (4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- (5) a coloro che, nell'ambito di altri Stati membri dell'Unione Europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio.

In aggiunta, le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche 5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale. 5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali; 5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali.

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso: 1) alle persone indicate nel primo comma del presente articolo; 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

1.16. Traffico di influenze illecite (art. 346-bis Cod. Pen.)

Il reato si configura nel caso in cui chiunque, fuori dei casi di concorso nei reati di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri di ufficio o corruzione in atti giudiziari, o dei reati ex art. 322-bis Cod. Pen., sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente si faccia dare o promettere, per sé o per altri, denaro o altro vantaggio patrimoniale, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio.

Tale reato prevede due diverse ipotesi:

1. la condotta di chi vanti dei rapporti privilegiati, in realtà inesistenti, con un pubblico ufficiale o incaricato di un pubblico servizio, per proporsi quale mediatore a pagamento;

2. la condotta di chi effettivamente possiede rapporti con pubblici ufficiali o incaricati di un pubblico servizio.

1.17. Peculato (art. 314 comma 1 Cod. Pen.)

Il reato si configura laddove il pubblico ufficiale o l'incaricato di un pubblico servizio, avendo per ragione del proprio ufficio o servizio, il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria.

Per possesso deve intendersi "la possibilità di disporre, al di fuori dell'altrui sfera di vigilanza, della cosa sia in virtù di una situazione di fatto, sia in conseguenza della funzione giuridica esplicata dall'agente nell'ambito dell'amministrazione". Con ciò si intende che non è necessario un possesso materiale, ma anche la mera possibilità di disporre.

Ai fini della responsabilità amministrativa derivante da reato ex D.lgs. 231/01 non rileva il "Peculato d'uso", previsto e disciplinato dal comma 2 dell'art. 314 Cod. Pen., che sussiste quando il reo agisce al solo scopo di fare un uso momentaneo della cosa, restituendola al termine dell'utilizzo.

1.18. Peculato mediante profitto altrui (art. 316 Cod. Pen.)

Il reato sussiste laddove il pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceva o ritenga indebitamente, per sé o per un terzo, denaro o altra utilità.

Tale delitto si differenzia dal reato di "Peculato" ex art. 314 Cod. Pen., in quanto è l'errore del soggetto privato che determina l'appropriazione da parte del Pubblico Ufficiale.

Va precisato, però, che l'errore non deve essere provocato dal P.U., ma il soggetto passivo deve autonomamente versare in tale condizione. Deve sussistere, dunque, una spontaneità della dazione, di cui il P.U. si approfitta.

1.19. Abuso d'ufficio (art. 323 Cod. Pen.)

Salvo che il fatto non costituisca un più grave reato, tale illecito è posto in essere nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procuri a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arrechi ad altri un danno ingiusto.

2. LE ATTIVITA' A RISCHIO REATO

I reati sopra descritti presuppongono l'instaurazione di rapporti con pubblici ufficiali e/o incaricati di pubblico servizio appartenenti alla Pubblica Amministrazione e/o soggetti ad essa assimilati facenti parte dello Stato italiano, dell'Unione Europea e degli Stati esteri.

Coface SA ha provveduto a svolgere un'analisi finalizzata all'individuazione delle attività a rischio reato, al fine di focalizzare al meglio i presidi necessari per l'eventuale miglioramento del sistema di controllo attualmente esistente.

Vengono, pertanto, definite "**Attività a rischio reato**" tutte quelle attività che – direttamente o indirettamente – presuppongono l'instaurazione di rapporti con gli organismi sopra descritti, che comportano la gestione di strumenti di tipo finanziario e/o mezzi sostitutivi e/o che, pur non comportando l'instaurazione di rapporti diretti con le entità pubbliche sopra menzionate, possono supportare la commissione dei reati di cui ai precedenti paragrafi.

Tenuto conto della peculiarità dell'attività di Coface SA e dei rapporti che la stessa intrattiene con i pubblici ufficiali, gli incaricati di pubblico servizio, i soggetti comunque appartenenti alle Pubbliche Amministrazioni, le attività considerate più specificamente a rischio in relazione ai reati descritti nella presente Parte Speciale sono ritenute le seguenti:

- **Adempimenti verso la Pubblica Amministrazione** Adempimenti previsti da obblighi di legge o regolamentari che impongono alla Compagnia, nei suoi rapporti con la pubblica amministrazione, incluse le ispezioni di cui essa venga fatta oggetto (da parte di autorità giudiziaria, di pubblica sicurezza, di polizia, di vigilanza, o da parte del garante privacy), di compiere determinate attività o di assumere specifici comportamenti.
- **Rapporti contrattuali con coinvolgimento della P.A.: le polizze fidejussorie** Attività commerciale e negoziale svolta nei confronti della Clientela. Conseguente attività assuntiva ed emissione della polizza; liquidazione dei sinistri.
- **Gestione del contenzioso** Decisioni ed attività inerenti la conduzione e la gestione del contenzioso, sia esso stragiudiziale che giudiziale, nei confronti dei dipendenti, della clientela o di terzi.

Di seguito si indicano nello specifico alcuni esempi di attività a rischio reato:

- produzione ed invio alla Pubblica Amministrazione di documenti, anche telematici e/o informatici, contenenti informazioni o dichiarazioni relative alla Società e/o l'attestazione di condizioni per la partecipazione a gare, per ottenere licenze o autorizzazioni, ecc. e/o, in ogni caso, svolgimento di attività, a qualunque titolo e per qualsivoglia finalità, che comportino l'invio di documentazione alla Pubblica Amministrazione;
- produzione ed invio alla Pubblica Amministrazione di documenti, anche telematici e/o informatici, contenenti dati di natura fiscale o previdenziale;
- partecipazione a gare di appalto, ad aste pubbliche, a licitazioni private o a trattative private indette o organizzate dalla Pubblica Amministrazione e svolgimento, in tutto o in parte, di tutti gli adempimenti relativi e connessi;
- negoziazione di contratti e convenzioni con la Pubblica Amministrazione;
- gestione della fatturazione attiva e della fatturazione passiva nei confronti della Pubblica Amministrazione e gestione dei relativi solleciti di pagamento o delle relative contestazioni;
- gestione di pagamenti, in qualsivoglia modalità o forma, e/o, in ogni caso, gestione dei flussi finanziari da e verso la Pubblica Amministrazione;

- gestione delle pratiche volte all’ottenimento o all’utilizzo di finanziamenti, contributi o sovvenzioni pubbliche, mutui agevolati o, in ogni caso, altre erogazioni della Pubblica Amministrazione dello stesso tipo comunque denominate concesse o erogate;
- gestione di rapporti in occasione di verifiche, ispezioni, accertamenti in generale presso la Pubblica Amministrazione o disposti dalla Pubblica Amministrazione presso la Compagnia;
- incontri personali, comunicazioni scritte e/o telematiche e/o informatiche o contatti telefonici con soggetti appartenenti alla Pubblica Amministrazione;
- gestione di rapporti in occasione di verifiche, ispezioni, accertamenti disposti dalla Pubblica Amministrazione per gli aspetti che riguardano la sicurezza e l’igiene sul lavoro;
- gestione di rapporti in occasione di verifiche, ispezioni, accertamenti disposti dalla Pubblica Amministrazione per gli aspetti che riguardano la protezione dell’ambiente; in ogni caso, qualsiasi rapporto con la Pubblica Amministrazione, sia italiana che straniera, con gli enti a natura pubblicistica o, comunque, svolgenti funzioni o attività pubbliche, con i pubblici Dipendenti, con pubblici ufficiali o con persone incaricate di un pubblico servizio;
- gestione delle pratiche di assunzione del personale, ivi compresi gli adempimenti presso INPS, INAIL, ecc.;
- gestione di contenziosi giudiziari e stragiudiziali (es: civili, giuslavoristici, amministrativi, penali ecc.);
- gestione dei contenziosi tributari;
- gestione di ogni altra attività attraverso cui può realizzarsi il reato di corruzione nei confronti di soggetti appartenenti alla PA (attività strumentali):
 - conferimento incarichi di consulenza;
 - gestione delle spese di rappresentanza;
 - gestione dei beni aziendali che possono rappresentare utilità di scambio;
 - gestione delle liberalità in denaro o beni;
 - gestione delle sponsorizzazioni;
 - organizzazione di eventi, convegni, congressi nei quali vengono invitati soggetti appartenenti alla Pubblica Amministrazione;
 - gestione dell’omaggistica, delle regalie in favore di soggetti appartenenti alla Pubblica Amministrazione.

2.1 Possibili modalità attuative.

A titolo meramente esemplificativo e non esaustivo sono riportate di seguito alcune possibili modalità attuative di reati sopra descritti:

- utilizzare fondi/agevolazioni/ mutui concessi dalla Stato o dalla Comunità Europa per scopi diversi da quelli per i quali essi sono stati conferiti;
- stipulare contratti per l’acquisto di beni o servizi con fornitori “suggeriti” da un pubblico ufficiale o dall’incaricato di un pubblico servizio;
- stipulare contratti di consulenza per compensi superiori al valore reale del bene/servizio prestato ed ai prezzi di mercato;
- dare o promettere ad un Pubblico Ufficiale o ad un incaricato di un Pubblico Servizio, regali, omaggi di qualsiasi natura;

- usare la propria posizione per ottenere benefici o privilegi per sé o per altri;
- corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico Funzionario o a PA o altri pubblici funzionari della Comunità Europea o altri organismi pubblici di diritto internazionale;
- corrispondere e/o proporre e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un soggetto di una Società terza in cambio di benefici di qualsiasi genere di carattere commerciale;
- eseguire prestazioni e riconoscere compensi in favore dei Dipendenti che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione e/o dazione di denaro o altra utilità a un Pubblico Funzionario nel caso in cui la Società sia parte di un procedimento giudiziario;
- porre in essere artifici e/o raggiri, tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea o ad organismi di diritto pubblico internazionale) per realizzare un ingiusto profitto;
- ricorrere a forme diverse di aiuti e/o contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze, pubblicità abbiano, invece, finalità vietate;
- sottrarre, alterare e/o manipolare i dati e i contenuti del sistema informatico o telematico, per ottenere un ingiusto profitto e arrecando danni a terzi;
- assumere alle dipendenze della Società persona segnalata da un Pubblico Ufficiale o da un incaricato di un Pubblico servizio;
- concedere ai propri clienti coperture assicurative al fine di ottenere contributi, sovvenzioni o finanziamenti pubblici, con la consapevolezza che la società utilizzerà tali somme per scopi diversi rispetto a quelli per le quali sono state concesso – è evidente come, in tale ipotesi, Coface SA rispondere del reato in concorso con il proprio Cliente. Il vantaggio per la Società consiste nell'incasso del premio assicurativo.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

I *“Reati in danno allo Stato o altro Ente Pubblico”* ex artt. 24 e 25 D.lgs. 231/2001, sopra richiamati e descritti, sono tutti reati a forma libera, potendosi, dunque, come visto, perpetrare nelle modalità più varie. Per queste ragioni, è evidente come, almeno in via teorica, essi potrebbero coinvolgere diverse funzioni aziendali.

Le Funzioni Aziendali all'interno delle quali potrebbero essere poste in essere le attività a rischio, possono essere identificate le seguenti:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione Amministrativa e Finanziaria;
- Direzione Risorse Umane (HR);
- Direzione Commerciale;
- Direzione Marketing;
- Direzione Ramo Cauzione;
- Direzione Fidi;
- Direzione Sistemi Informativi;

- Responsabile Privacy;
- Funzioni di Controllo;
- Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Codice Anticorruzione (Allegato A-bis)**, che individua i principi e le regole di condotta a cui i Destinatari devono attenersi al fine di prevenire e limitare il rischio di consumazione dei “Reati Corruttivi”;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

La Società nella conduzione dei propri affari societari si conforma ai principi di liceità e trasparenza così come comprovato dall’adozione della “***Gifts & Benefits Procedure***” ([Allegato A-ter](#)).

Nello specifico, la procedura traccia le linee guida che i dipendenti, gli amministratori, i dirigenti e i funzionari di Coface SA devono adottare laddove ricevano o intendano offrire regali, benefici o ospitalità a Pubblici Ufficiali, Incaricati di un Pubblico servizio o a soggetti privati.

Più nel dettaglio, la Società ha previsto **il divieto** di offrire a **soggetti pubblici** regali, benefici e ospitalità di alcun tipo e valore economico, a meno che non vi sia l’autorizzazione scritta del *Compliance Officer*, il quale sarà tenuto a valutare l’adeguatezza degli omaggi offerti, analizzando lo **scopo del dono**, il **valore del dono** e la **frequenza dello stesso**.

La Società, inoltre, al fine di garantire la tracciabilità delle regalie effettuate o ricevute dai suoi dipendenti, ha predisposto il “Registro dei Regali e Beneficenze”.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l’implementazione e l’adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all’ [Allegato A](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l’obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Chiunque ne sia informato comunica, dunque, all'OdV, le seguenti informazioni:

- eventuali casi di malversazione, corruzione, truffa e frode di cui sia venuto a conoscenza;
- qualunque criticità o conflitto d'interesse⁶ sorga nell'ambito dei rapporti con la Pubblica Amministrazione;
- condotte commesse in violazione delle norme comportamentali aziendali.

Coloro che svolgono funzioni di controllo e supervisione sugli adempimenti connessi all'espletamento delle suddette attività devono portare a conoscenza dell'OdV, le attività più rilevanti e, in particolare, a titolo meramente esemplificativo e non esaustivo:

- la concretizzazione di appalti, commesse, finanziamenti e/o, in ogni caso, operazioni di qualsivoglia natura e comunque denominate, concluse a livello nazionale ed Europeo, con la Pubblica Amministrazione a seguito di gare, aste pubbliche, licitazioni private o trattative private;
- il conferimento, anche in tempi diversi, purché nell'arco di un anno, di incarichi professionali e/o di consulenza a singoli professionisti o ad associazioni tra professionisti;
- la richiesta di contributi pubblici.

I singoli Responsabili Interni devono, altresì, verificare che i loro sottoposti, delegati a svolgere attività che comportino rapporti con la Pubblica Amministrazione e/o con i soggetti ad essa assimilati dello Stato italiano, dell'Unione Europea e degli Stati esteri rispettino le prescrizioni e le procedure aziendali.

B) DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24-BIS D.LGS. 231/2001)

A seguito del processo di digitalizzazione ed informatizzazione che ha investito l'intero sistema economico e che, inevitabilmente, coinvolge anche il mondo societario, risulta imprescindibile,

⁶ Ai fini del presente documento, si configura un conflitto d'interessi quando uno dei soggetti, coinvolto in taluna delle attività sensibili, si trova a dover scegliere tra l'interesse di Coface SA – o delle altre entità del Gruppo o dei loro Clienti – ed il proprio personale interesse.

nella profilazione dei rischi connessi allo svolgimento delle attività aziendali, predisporre specifiche procedure che vadano a regolamentare la gestione e l'utilizzo dei sistemi informativi aziendali, nonché la sicurezza informatica.

In ragione del fatto che i reati informatici possono essere commessi tramite apparecchiature e mezzi che appartengono alla dotazione di tutte le aree aziendali, essi possono essere realizzati nell'ambito di qualsiasi attività svolta in Compagnia, a prescindere anche dal fatto che essa venga compiuta o meno nell'orbita del ciclo produttivo aziendale. Coface SA ha predisposto presidi organizzativi specifici, e si è dotata di adeguate soluzioni di sicurezza, in conformità con le vigenti disposizioni emanate dal Legislatore, dal Regolatore e dal Garante Privacy, atte a prevenire e controllare i rischi in materia di tecnologia dell'informazione, di tutela del proprio patrimonio informativo, e dei dati personali.

Si precisa che la Direzione Sistemi Informativi fin dalla sua nascita ha operato nell'ambito di Coface SA Service S.p.A., erogando servizi informatici alla Compagnia. A fronte della già citata operazione societaria che, con data effetto 22/12/2010, ha visto la fusione per incorporazione di Coface SA Service S.p.A. in Coface SA Assicurazioni S.p.A., la Direzione Sistemi Informativi è stata inserita tra i servizi di supporto della Compagnia, ed è ora collocata nell'ambito della Direzione Organizzazione e IT.

La gestione della sicurezza informatica è affidata al Dipartimento *Information Technology* (IT), che dirige l'ambito informatico sia per Coface SA che per Coface SA Italia S.r.l., sulla base delle policy dettate dalla Capogruppo francese.

Al fine di tutelare l'integrità dei dispositivi informatici aziendali e dei dati in esso contenuti (Es. polizze assicurative, dati personali dei Clienti, autorizzazioni e concessioni degli Enti Pubblici), la Società ha implementato specifiche procedure che consentano sempre di individuare gli utenti che operano sui dispositivi, attraverso un sistema di User-id e password.

Ciascun *account* viene creato in base alle necessità del *business*: è infatti possibile introdurre profili specifici per agenti, liquidatori di sinistri, ecc., non essendovi alcuna preclusione in tal senso. La decisione relativa ai nominativi – e alla corrispondente qualifica – da abilitare per la fruizione di una determinata applicazione è demandata agli *owner* del relativo processo, essendo quindi una valutazione connessa a profili di business. Secondo la procedura di Gruppo, la richiesta di attivazione di un *nuovo account* deve essere redatta a mezzo e-mail, così come deve essere comunicata per iscritto l'avvenuta attivazione del profilo; tali informative vengono archiviate nel *repository*.

Di seguito saranno, sinteticamente, descritte le singole fattispecie di reato ex art. 24-bis D.lgs. 231/2001 e individuate alcune possibili modalità attuative.

* * *

Delitti informatici

Appare opportuno premettere che il termine "*crimine informatico*" indica, in genere, qualsiasi reato o violazione del Codice civile o penale, in cui il ricorso alla tecnologia informatica sia stato un fattore determinante per il compimento dell'azione criminosa.

In realtà è opportuno distinguere i reati telematici “veri e propri”, ovvero impossibili da porre in essere senza l’ausilio delle tecnologie informatiche, ed i crimini cosiddetti “tradizionali” o “convenzionali”, in cui l’uso dello strumento informatico è solo un supporto *ad hoc* per il raggiungimento dello scopo.

I reati introdotti nella disciplina della responsabilità amministrativa degli enti dalla Legge 48/2008 sono di seguito elencati e descritti.

1.1 Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis Cod. Pen.)

Se alcuna delle falsità previste dal capo III, Titolo VII del Codice Penale riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

È evidente come sia conferita rilevanza penale alla commissione di reati di falso attraverso l’utilizzo di documenti informatici.

Per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

I reati di falso richiamati dall’art. 491 bis Cod. Pen. sono:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 Cod. Pen.);
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 Cod. Pen.);
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 Cod. Pen.);
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 Cod. Pen.);
- Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 Cod. Pen.);
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità (art. 481 Cod. Pen.);
- Falsità materiale commessa da privato (art. 482 Cod. Pen.);
- Falsità ideologica commessa dal privato in atto pubblico (art. 483 Cod. Pen.);
- Falsità in registri e notificazioni (art. 484 Cod. Pen.);
- Falsità in foglio firmato in bianco. Atto privato (art. 486 Cod. Pen.);
- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 Cod. Pen.);
- Altre falsità in foglio firmato in bianco (art. 488 Cod. Pen.);
- Uso di atto falso (art. 489 Cod. Pen.);
- Soppressione, distruzione o occultamento di atti veri (art. 490 Cod. Pen.);
- Falsità in testamento olografo, cambiale o titolo di credito (art. 491 Cod. Pen.);
- Falsità commesse da pubblici impiegati incaricati di un pubblico servizio (art. 493 Cod. Pen.).

1.2 Accesso abusivo ad un sistema informatico (art. 615 *ter* Cod. Pen.)

La norma punisce 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.

Il reato è più gravemente punito:

- se il fatto è commesso da un Pubblico Ufficiale o da un Incaricato di un Pubblico Servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti 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 aumentata.

Per commettere il reato è necessaria la violazione di idonee misure di sicurezza; pertanto, si ritiene che debbano essere violati sistemi di "*introducing detection*" tali da impedire l'accesso *invito domino*, o, quantomeno, sistemi in grado di identificare l'utente che abbia effettuato l'accesso.

Integra il delitto di introduzione abusiva in un sistema informatico l'accesso ad un sistema che sia protetto da un dispositivo costituito anche soltanto da una parola chiave (c.d. *password*).

L'accesso abusivo si concretizza non appena vengano superate le misure di sicurezza del sistema, in quanto l'art. 615 *ter* Cod. Pen. punisce la semplice intrusione ancor prima di valutare l'ipotesi di danneggiamento o furto dei dati.

Il reato può anche essere causato da soggetti legittimati all'uso del sistema, autorizzati ad accedere solo ad una parte dei dati contenuti in memoria. In tal caso il sistema protetto diviene quella parte di memoria a cui l'accesso non è autorizzato.

La permanenza non autorizzata consiste nel fatto che il soggetto responsabile dell'intrusione si sia trovato non volontariamente in una zona protetta del sistema ma "*vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*".

L'accesso abusivo può concretizzarsi anche attraverso la detenzione o la diffusione *invito domino* di codici di accesso personali. Tale fattispecie è stata espressamente prevista e punita dal legislatore all'art. 615 *quater* Cod. Pen.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe accedere, utilizzando le credenziali di un altro utente, da questo cedutegli, ovvero illegittimamente carpite mediante inganno o raggirò, in un sistema informatico protetto al fine consultare o trattare in qualsivoglia maniera i dati in questo contenuti.

1.3 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* Cod. Pen.)

La norma punisce chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe diffondere indebitamente, ovvero ottenere per mezzo di una condotta fraudolenta, i codici di accesso al sistema informatico di altri utilizzatori autorizzati, chiedendo in cambio dell'informazione riservata una somma di denaro o qualunque altra utilità per sé o per altri soggetti.

1.4. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 *quinquies* Cod. Pen.)

La norma intende preservare il corretto funzionamento delle tecnologie informatiche.

Essa sanziona la condotta di chiunque si procura abusivamente, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o a esso pertinenti, nonché di favorire l'interruzione, totale o parziale, ovvero l'alterazione del suo funzionamento.

Oggetto materiale della condotta possono essere sia software che hardware.

L'ipotesi tipica è quella dalla diffusione di un virus attraverso posta elettronica, attività di navigazione in Internet, o tramite l'inserimento nel PC di supporti esterni, quali dispositivi USB e CD-ROM.

1.5. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* Cod. Pen.)

La norma punisce chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa.

La norma punisce, altresì, chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al precedente periodo.

I delitti prima descritti sono punibili a querela della persona offesa. Tuttavia, si procede d'ufficio se il 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 dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- da chi eserciti anche abusivamente la professione di investigatore privato.

A titolo meramente esemplificativo, si segnala che uno dei Destinatari del Modello potrebbe, con artifici e raggiri, eventualmente sfruttando l'area condivisa, riuscire a venire a conoscenza di comunicazioni o dati riservati, ovvero interromperne il flusso.

1.6. Installazione, diffusione e installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* Cod. Pen.)

Tale norma punisce chiunque, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero al fine di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici o parole chiavi o altri mezzi atti a tali fini.

Rispetto al reato precedente art. 617-quater Cod. Pen., tale delitto offre una tutela anticipata al bene giuridico della segretezza e libertà delle comunicazioni informatiche o telematiche, vietando l'installazione di apparecchiature che possano in qualsiasi modo comprometterle.

Integra il reato de quo, ad esempio, l'utilizzo di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico.

1.7 Danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* Cod. Pen.)

La norma punisce chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Il fatto è più grave se commesso con abuso della qualità di operatore del sistema e si procede d'ufficio.

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

La norma punisce chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Il reato è più grave se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 Cod. Pen. ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

1.9 Danneggiamento di sistemi informatici o telematici (art. 635 *quater* Cod. Pen.)

La norma punisce chiunque, mediante le condotte di cui all'articolo 635 *bis* Cod. Pen. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Il reato è più grave se il fatto è commesso con abuso della qualità di operatore di sistema.

1.10 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* Cod. Pen.)

Il reato di danneggiamento di sistemi informatici o telematici è più grave se:

- il danneggiamento di sistemi è diretto a distruggere, danneggiare, rendere in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento;
- dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile;
- ricorre la circostanza di cui al numero 1) dell'articolo 635 comma II Cod. Pen., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

1.11 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* Cod. Pen.)

La norma punisce il soggetto che prestando servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare un danno ad altri, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Per firma digitale si intende una procedura informatica che sia basata su tecniche crittografiche le quali sono dirette a coniugare un numero binario (la firma) ad un documento informatico, ovvero ad un altro insieme di bit dai quali si evinca l'esistenza di atti o fatti che siano giuridicamente rilevanti.

Il delitto ex art. 640-*quinquies* Cod. Pen. è un reato proprio, che può essere commesso esclusivamente da quei soggetti che prestino servizi di firma elettronica.

È delitto contro il patrimonio che si pone in un rapporto di sussidiarietà rispetto al reato di truffa ex art. 640 Cod. Pen.

2. LE ATTIVITA' A RISCHIO REATO

Come già in precedenza evidenziato, le possibili aree aziendali a rischio consumazione "*Delitti informatici e trattamento illecito dei dati*" sono molteplici, considerando che, potenzialmente, tali reati potrebbero, in astratto, essere perpetrati, in qualsiasi funzioni avente a disposizione dispositivi informatici aziendali, potendo, dunque, essere consumati nell'ambito di qualsivoglia attività aziendale, a prescindere che venga compiuta o meno dell'orbita del ciclo produttivo aziendale.

Al fine di una migliore individuazione e disamina delle aree a rischio e delle Procedure adottate dalla Società al fine di prevenire la consumazione di tali reati, possiamo distinguere 4 differenti aree di attività:

- (1) **Operazione da e verso l'esterno** – utilizzo della rete internet e telematica, nonché dell'e-mail aziendale. Utilizzo delle credenziali assegnate a ciascun utente;
- (2) **Attività che impattano sulla sicurezza fisica** – gestione e protezione delle postazioni di lavoro, sei server e della rete. Acquisto, gestione, manutenzione e utilizzo dei dispositivi informativi. Assistenza del personale.
- (3) **Attività che impattano sulla sicurezza logica** – Utilizzo dei programmi informatici e delle informazioni aziendali. Conservazione della documentazione aziendale. Gestione dei profili utente.
- (4) **Gestione e manutenzione dei sistemi informatici** – Acquisizione, installazione, sviluppo e manutenzione dei programmi. Progettazione e sviluppo della piattaforma IT.

2.1 Possibili modalità attuative.

A titolo meramente esemplificativo e non esaustivo sono riportate di seguito alcune possibili modalità attuative di reati sopra descritti:

- Falsificazione di documenti informatici da trasmettere alla Pubblica Amministrazione e/o Enti Pubblici;
- Inserimento di informazione false e non veritiere in banche dati pubbliche;
- Accesso abusivo e, dunque, non autorizzato in sistemi informatici di un soggetto terzo, quale può essere un competitor, al fine di prendere conoscenza di dati riservati;
- Accesso a data base di un competitor, in cui sono riportati i nominativi e i dati personali dei suoi Clienti, al fine di effettuare uno sviamento della Clientela;
- Accesso abusivo a un sistema informatico della Pubblica Amministrazione e/o Ente Pubblico, al fine di falsificare o sottrarre documentazione e informazioni riservate;
- Intercettare o impedire comunicazioni informatiche o telematiche;
- Installare su dispositivi informatici aziendali altrui virus o spyware, con la finalità di danneggiare il sistema, dati o file in esso contenuti.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

In ragione del fatto che i reati informatici possono essere commessi tramite apparecchiature e mezzi che appartengono alla dotazione di tutte le aree aziendali, essi possono essere realizzati nell'ambito di qualsiasi attività svolta in Compagnia, a prescindere anche dal fatto che essa venga compiuta o meno nell'orbita del ciclo produttivo aziendale.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;

- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

In riferimento a ciascuna delle 4 aree di attività individuate nel paragrafo 2, della presente sezione B, va sottolineato quanto segue:

- (1) **Operazioni da e verso l'esterno**. In merito alla navigazione Internet e all'uso della posta elettronica aziendale, la Società, nel proprio Regolamento Interno, ha recepito specifiche circolari della Capogruppo, finalizzate a disciplinare le modalità di utilizzo delle risorse aziendali. Nello specifico, è stato vietato l'accesso a specifiche categorie di siti internet, contrari all'etica aziendale e riconducibili ad attività di pirateria informatica. L'accesso a tali siti può essere autorizzato solo a fronte di specifica esigenza lavorativa. La restrizione alla navigazione è garantita dal firewall aziendale. Per quanto diversamente attiene l'impatto che – in tale area – hanno i contatti con la Pubblica Amministrazione, la Compagnia ha provveduto al censimento integrale degli applicativi utilizzati sulla cosiddetta Mappa Applicativi e, tramite identificazione in essa del dato "Fornitore", di quelli che consentono una diretta interazione con la Pubblica Amministrazione (ad es. Entratel e Fisconline per il pagamento delle imposte, Postel e Dike per la gestione della firma digitale) o con l'Autorità di Vigilanza.
- (2) **Attività che impattano sulla sicurezza fisica**. I dispositivi informatici ed i supporti di memorizzazione aziendali sono inventariati, in modo da assicurare un controllo costante sul loro utilizzo e funzionamento. Al momento della cessazione del rapporto di lavoro, le apparecchiature restituite sono sottoposte ad un processo di cancellazione dei dati contenuti. Inoltre, ciascuna postazione di lavoro è protetta da un blocco automatico del PC in caso di inattività prolungata dello stesso.
- (3) **Attività che impattano sulla sicurezza logica**. Gli accessi e le abilitazioni sono periodicamente controllati ed aggiornati e sono in vigore procedure per l'assegnazione e la revoca delle credenziali. A ciascun utente viene inoltre resa un'informativa circa il corretto utilizzo e la conservazione di user e password, riferiti a strumenti aziendali. Il firewall in uso garantisce la difesa della struttura software, e dei dati in esso contenuti, da intrusioni illecite dall'esterno. Viene inoltre effettuata la registrazione delle attività eseguite nell'ambito di servizi particolarmente critici, al fine di consentire la ricostruzione di qualsiasi tipo di operazione svolta in tale ambito. La Compagnia ha strutturato controlli ed emanato procedure afferenti alla concessione e le modalità di utilizzo della firma digitale per finalità aziendali (sottoscrizione polizza digitale, depositi registri imprese), ad opera di un limitato numero di dipendenti e procuratori a ciò esplicitamente autorizzati. È in essere un processo di backup delle informazioni e del software applicativo ritenuto critico. Le informazioni e i dati salvati nelle differenti aree-server vengono quotidianamente sottoposti a tale processo di registrazione, il cui risultato è conservato su base settimanale. Il software da utilizzarsi in Compagnia è inoltre testato in un ambiente informatico specifico, distinto da quello di produzione destinato agli utenti, e dedicato alle sole attività di sviluppo e di test. La Compagnia ha regolamentato le attività

di implementazione e modifica software, prevedendo inoltre che l'installazione di quest'ultimo venga effettuata a cura dei soli soggetti dotati delle specifiche abilitazioni.

- (4) **Gestione e manutenzione dei sistemi informatici.** La Compagnia adotta specifici sistemi di gestione dei rapporti con i fornitori di beni e servizi, e ne valuta le prestazioni. Al verificarsi di incidenti, la Compagnia procede con la loro analisi al fine di valutarne cause e ripetitività, e provvede alla loro soluzione: vengono adottati canali gestionali per la loro comunicazione e registrazione. Sono stati inoltre nominati gli Amministratore di Sistema ed è stata adottata una metodologia volta alla regolamentazione ed alla verifica della loro attività. La Compagnia è inoltre in grado di ricostruire il processo decisionale relativo a qualsiasi attività svolta in ambito informatico, anche e soprattutto in ordine alle scelte di gestione e di utilizzo dei sistemi informatici, tramite la consultazione di verbali di riunioni, comunicazioni di autorizzazioni, documentazione di progetto e di requisiti, tutti storicizzati ed archiviati. Coface SA ha anche adottato specifiche soluzioni tecnologiche ed infrastrutturali di continuità operativa finalizzate alla prosecuzione del business anche in presenza di eventi catastrofici e/o di assoluta emergenza (Business Continuity Plan). Gli interventi informatici in genere, le attività di salvataggio dei sistemi operativi, software, dati e configurazioni sono periodicamente pianificati e censiti.

Coface SA, al fine di prevenire e limitare la consumazione di "Reati informatici" e di illeciti in materia di trattamento dei dati personali, ha adottato specifiche procedure in materia di Business Tech.

Nello specifico, la procedura "**Cybersecurity Process**" ([Allegato V](#)), avente come finalità quella di dettare le regole generali da seguire nel processo di gestione dell'accesso delle risorse ai dispositivi informativi e la "**Data Management Policy**" ([Allegato W](#)), finalizzata ad assicurare e garantire la corretta gestione dei dati sensibili della Clientela. Quest'ultima individua le modalità di archiviazione dei dati e i diversi livelli di classificazione che devono essere adottati per la loro protezione, nel rispetto del GDPR.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato B](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di

Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Chiunque ne sia informato comunica, dunque, all'OdV, le seguenti informazioni:

- Indebito utilizzo dei dispositivi informatici aziendali, con accesso a siti internet non consentiti o, comunque, non pertinenti con l'attività lavorativa;
- Accesso abusivo a dispositivi informatici aziendali, non autorizzati;
- Furto di user-id e password personali altrui;
- Installazione di software sui dispositivi informatici aziendali, senza preventiva autorizzazione del Responsabile IT;
- Danneggiamento o manomissione dei dispositivi informatici aziendali;
- Alterazione e falsificazioni di documenti informatici;
- Accesso non autorizzato sui portali della Pubblica Amministrazione e/o di Enti Pubblici.

C) DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER)

È necessario premettere che, considerando l'assetto societario di Coface SA, tra i reati individuati dall'art. 24-ter D.lgs. 231/2001, gli unici che, astrattamente, potrebbero configurarsi sono i delitti di "Associazione per delinquere" ex art. 416 Cod. Pen. e il reato di "Associazione di tipo mafioso" ex art. 416 bis Cod. Pen.

Inoltre, ai sensi dell'art. 10 Legge 146/2006, considerando la natura transfrontaliera di Coface SA, si ritiene sussistente il rischio di consumazione dei "Reati Transnazionali" di Associazione per delinquere e di Associazione di tipo mafioso.

Ed invero, si definisce reato transnazionale un delitto che è punito con la reclusione non inferiore nel massimo a 4 anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- (a) sia commesso in più di uno Stato;
- (b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
- (c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- (d) ovvero sia commesso in uno Stato ma abbia effetti in un altro Stato.

Le ulteriori fattispecie di reato contemplate e disciplinate dall'art. 24-ter, saranno, per completezza espositiva qui analizzate e, in qualsiasi caso, esse si ritengono presidiate dai principi di cui al Codice di Condotta COFACE, nonché dalle Procedure e Protocolli che compongono il presente Modello di Organizzazione, Gestione e Controllo.

* * *

1.1 Associazione per delinquere (art. 416 Cod. Pen.)

Tale norma punisce chiunque partecipa ad un'associazione per delinquere, intesa quale associazione di tre o più persone, allo scopo di commettere più delitti. Pene maggiori sono previste per coloro che promuovono, costituiscono od organizzano l'associazione.

Gli elementi tipici del reato *de quo* sono la formazione e la permanenza di un vincolo associativo continuativo tra tre o più persone finalizzato a commettere una serie indeterminata di delitti, con la predisposizione comune dei mezzi occorrenti per la realizzazione del programma criminoso e la consapevolezza, di ciascun associato, di fare parte del sodalizio criminoso e di essere disponibile ad operare per l'attuazione del programma stesso.

È importante sottolineare come, al fine della sussistenza del reato in oggetto, non è necessario che i reati programmati siano portati a reale compimento, ma è sufficiente che vi sia un accordo di carattere generale volto all'attuazione di un programma criminoso.

Ciò che differenzia tale reato dal mero concorso di persone in reato continuato è che, mentre in quest'ultimo l'accordo avviene in via del tutto occasionale per la realizzazione di uno o più reati specificatamente predeterminati, nell'associazione per delinquere l'accordo tra i consociati è stabile, mentre i reati che si programma di compiere possono essere anche indeterminati all'origine.

Un esempio potrà meglio chiarire in quale ipotesi tale reato sia rilevante per Coface SA:

- *“tre o più soggetti, di cui almeno uno interno alla Società, si associano allo scopo di commettere più delitti tra quelli richiamati dal D.lgs. 231/01, come reati in materia fiscale (evasione Iva attraverso l'emissione di fatture per operazioni inesistenti) o reati di bancarotta fraudolenta (attraverso, ad esempio, la ricezione di pagamenti da parte del fallito o del fallendo, a danno di altri creditori ugualmente legittimati)”*.

1.2 Associazione di tipo mafioso anche straniera (art. 416 bis Cod. Pen.)

Tale norma punisce chiunque fa parte, promuove, dirige o organizza un'associazione di tipo mafioso formata da tre o più persone.

L'associazione è definita di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione scaturente dal vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, per commettere delitti, 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 altri.

Tale forma di associazione, evidentemente, si distingue da quella prevista e punita dall'art. 416 Cod. Pen., in virtù della forza di intimidazione promanante dal vincolo associativo e per la condizione di assoggettamento ed omertà che ne deriva.

1.3 Scambio elettorale politico-mafioso (art. 416 bis Cod. Pen.)

Tale norma punisce chiunque accetta la promessa di procurare voti, avvalendosi della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva, in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità, ovvero chi promette di procurare voti con le stesse modalità.

Si riportano alcune esemplificazioni relative alle modalità con cui il reato in esame potrebbe manifestarsi:

- la società finanzia, in modo consapevole, direttamente o indirettamente, o comunque concorre nel reato agevolandone l'operato, soggetti che fanno parte di un'associazione mafiosa o che sono collegati a sistemi organizzativi e metodi mafiosi, affinché quest'ultimi si impegnino a far votare un soggetto candidato alle elezioni;
- uno o più soggetti intranei alla Società, in posizione apicale, operano dall'esterno in favore di un'associazione di tipo mafioso, facendo pressione ai propri dipendenti e/o clienti perché orientino il loro voto verso un soggetto candidato alle elezioni in cambio di agevolazioni o altre utilità per la società stessa.

1.4. Sequestro di persona a scopo di estorsione (art. 630 Cod. Pen.)

Tale norma punisce chiunque sequestra una persona al fine di conseguire per sé o altri, un ingiusto profitto come prezzo della liberazione. Sono previste pene aggravate nel caso in cui, quale conseguenza non voluta dal reo, si verifichi la morte della persona sequestrata.

1.5. Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 309/1990)

La norma punisce la condotta di tre o più persone che si associano allo scopo di commettere più delitti tra quelli previsti dal DPR 309/1990, quali cessione o traffico di droga.

Si riportano alcune esemplificazioni relative delle modalità con cui il reato in esame potrebbe manifestarsi:

- tre o più soggetti, di cui almeno uno interno alla società, apicale o dipendente, utilizzando le strutture di proprietà o di pertinenza della stessa Società, si associano allo scopo di commettere più delitti tra quelli previsti dell'art. 73 DPR 309/1990, o promuovono, costituiscono, dirigono, organizzano o finanziano l'associazione;
- la società finanzia consapevolmente direttamente o indirettamente, o comunque concorre nel reato agevolandone l'operato, soggetti o strutture che illecitamente producono o commercializzano le sostanze chimiche di base ed i precursori di cui alle categorie 1, 2 e 3 dell'allegato I al DPR 309/1990, utilizzabili nella produzione clandestina delle sostanze stupefacenti o psicotrope previste nelle tabelle di cui all'art. 15 dello stesso decreto.

1.6. Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di arma da guerra o parti di esse, di esplosivi, di armi comuni da sparo escluse quelle previste dall'art. 2, comma III Legge 110/1975

2. LE ATTIVITA' A RISCHIO REATO

Le attività prestante da Coface SA in favore dei propri Clienti (Assicurazione del Credito, Concessioni di cauzioni e fidejussioni), presentano, indubbiamente, in astratto, un alto rischio di consumazione dei reati ex art. 24-ter D.lgs. 231/2001.

Di seguito si elencano le attività sensibili individuate nell'ambito del reato all'esame:

- l'autorizzazione ed esecuzione di servizi assicurativi;
- la gestione di investimenti quali acquisizioni di aziende o di partecipazioni,

- la negoziazione di accordi di consulenza/collaborazione, di mandato o di intermediazione.

2.1 Possibili modalità attuative.

Le modalità attraverso cui i reati previsti e disciplinati dall'art. 24-ter D.lgs. 231/2001, sono molteplici, trattandosi di reati a forma libera. A titolo meramente esemplificativo e non esaustivo, saranno di seguito elencate alcuni possibili condotte che potrebbero configurare i reati in oggetto:

- costituzione o partecipazione ad un'associazione avente l'intento di compiere attività criminose connesse all'attività aziendale;
- rilascio di garanzia di fideiussorie che risultino utili o necessarie al compimento dei reati;
- assicurare crediti di imprese che ottengono i loro guadagni attraverso il compimento di reati;
- il reato potrebbe configurarsi nell'ipotesi in cui un soggetto di Coface SA si serva di un potenziale partner, dietro il quale si cela un'organizzazione criminale, al fine di entrare in nuovi mercati collegati all'organizzazione citata;
- è possibile – perlomeno in linea teorica – che un dipendente di Coface SA, nell'ambito di un rapporto contrattuale in essere con un operatore economico straniero, dietro cui si celi un'organizzazione criminale, trasferisca denari a tale organizzazione criminale;
- il reato potrebbe configurarsi nell'ipotesi in cui un soggetto che ricopre una posizione apicale in Coface SA si serva di un consulente, dietro il quale si cela un'organizzazione criminale, al fine di entrare in nuovi mercati collegati all'organizzazione citata, finanziando quest'ultima mediante il riconoscimento di un compenso al consulente in eccedenza rispetto al dovuto;
- il reato ex art. 416 c.p. potrebbe configurarsi laddove le consociate appartenenti al Gruppo Coface SA, realizzino una serie di condotte, finalizzate a perpetrare taluno dei delitti previsti e puniti dal Decreto Legislativo 231/2001.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Considerando la natura di tali reati, qualificabili come reati a forma libera e comuni, potendo, dunque, essere, in astratto realizzabili da chiunque, si ritiene che, potenzialmente gli illeciti penali ex art. 24-ter D.lgs. 231/2001, coinvolgono la totalità delle aree aziendali.

Sicuramente le funzioni a maggior rischio sono:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione Commerciale;
- Direzione Marketing;
- Direzione Ramo Cauzione;
- Direzione Fidi;

- Chief Compliance Officer (COO);
Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

Inoltre, Coface SA ha adottato le procedure “**KYC – Know Your Customers procedure**” ([Allegato N](#)) e “**KYS – Know Your Supplier procedure**” ([Allegato O](#)), che, attraverso una attività di *due diligence* sui propri clienti e fornitori, completata da una richiesta documentale accurata, prima della sottoscrizione di contratti di servizi o della stipula di assicurazione del credito, cauzioni o fideiussioni, consentono a Coface SA di conoscere preventivamente le proprie controparti, limitando la possibilità di finanziamento di attività criminali.

La Procedura KYS, attraverso le richieste documentale consente, inoltre, un controllo sulla struttura compliance dei potenziali fornitori. Ad ognuno di essi viene, sulla base di specifici indici (Es. Paese dei fornitori, luogo di esecuzione del contratto, località in cui è aperto il conto corrente del fornitore indicato per i pagamenti) è attribuito un punteggio di rischio, ad ognuno dei quali corrisponde un diverso processo decisionale, basato su più o meno livelli autorizzativi.

La procedura KYC, invece, prevede che per tutti i potenziali nuovi Clienti sia effettuata un’accurata due diligence, che consenta di perimetrare l’attività da essi svolta e i soggetti (persone fisiche e/o giuridiche) con cui intrattengono rapporti commerciali.

Al fine di limitare e prevenire la commissione dei reati previsti in tale sezione, è stato, inoltre, previsto che prima della convalida del pagamento del sinistro, il Responsabile di funzione, attraverso un’attività di *due diligence*, deve verificare che l’assicurato o beneficiario del pagamento del sinistro non sia stato sottoposto a sanzioni o vigilanza commerciale. Sarà, inoltre, necessario accertare che il beneficiario o i debitori non siano situati in Paesi ad altro rischio sanzione – procedura “**Sanctioned Companies and Countries under Sanctions**” ([Allegato Y](#)).

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato C](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Nello specifico, dovranno essere comunicate all'Organismo di Vigilanza tutte le informazioni delle controparti di Coface SA – clienti, fornitori, partners commerciali, agenti – relative alla loro onorabilità e/o coinvolgimento in fattispecie criminose.

D) FALSITA' IN MONETE, IN CARTE DI CREDITO, IN VALORI DI BOLLO E SEGNI DI RICONOSCIMENTO (ART. 25-BIS D.LGS. 231/2001)

Rispetto ai reati previsti e disciplinati dall'art. 25-bis D.lgs. 231/2001, considerando l'attività sociale di Coface SA e la sua struttura organizzativa, si ritiene che gli unici profili di rischio potrebbero sussistere esclusivamente in relazione ai reati di "Spendita di monete falsificate ricevute in buona fede" ex art. 457 c.p. e di "Uso di valori di bollo contraffatti o alterati" ex art. 464 c.p.

Di seguito saranno descritte tali ipotesi delittuose.

* * *

1.1 Spendita di monete falsificate ricevute in buona fede (Art. 457 Cod. Pen.)

La norma in oggetto punisce chiunque spende, o mette altrimenti in circolazione monete contraffatte o alterare, da lui ricevute in buona fede.

È evidente come la norma punisca coloro i quali, non essendo concorso nella falsificazione, abbiamo ottenuto in buona fede una moneta contraffatta, ma poi venuti a conoscenza della loro falsità dopo la ricezione, la utilizzano dolosamente, spendendola o ponendola in circolazione.

Tale fattispecie criminosa si differenzia dai reati ex artt. 453, 453 e 455 c.p., in quanto essi sono caratterizzate da una malafede del soggetto agente anche nel momento della ricezione della moneta.

Nel caso in cui, il soggetto agente conservi la propria buona fede anche nel momento dell'utilizzo della moneta falsa, non essendo, dunque, venuto a conoscenza dell'avvenuta falsificazione, allora egli non sarà punibile.

Allo stesso modo non sarà punibile chi dovesse venire a conoscenza della falsità solo dopo la spendita e la messa in circolazione.

1.2 Uso di valori di bollo contraffatti o alterati

Il reato *de quo* punisce chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo contraffatti o alterati.

Nel caso in cui i valori siano ricevuti in buona fede, si applica la pena previste dall'art. 457 c.p., ridotta di un terzo.

La fattispecie in oggetto sussiste allorquando sia posta in essere una condotta diversa rispetto alla mera messa in circolazione. È necessario, dunque, uno vero e proprio atto di disposizione del valore di bollo, come l'apposizione di una marca da bollo alterata.

2. LE ATTIVITA' A RISCHIO REATO

Tali fattispecie delittuose sopra descritti possono, in astratto, configurarsi ogni qualvolta, nell'esercizio delle attività lavorative, taluno dei Destinatari si trovi a dover maneggiare ed utilizzare denaro contante o valori da bollo.

Le principali funzioni considerate a rischio sono:

- Gestione dei rapporti con i fornitori ed i clienti;
- Gestione degli adempimenti amministrativi, fiscali e tributari.

2.1 Possibili modalità attuative.

Tali fattispecie di reato potrebbero ipoteticamente realizzarsi a seguito della ricezione di denaro contante in pagamento di una spettanza della Compagnia, o dell'acquisizione di valori bollati da utilizzarsi nel normale svolgimento dell'attività lavorativa.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

I soggetti e le funzioni aziendali che potrebbero essere coinvolte nello svolgimento delle attività individuate nel precedente paragrafo e, quindi, direttamente a rischio consumazione reati ex artt. 25- bis D.lgs. 231/2001 sono:

- Rappresentante della Sede Secondaria (Country Manager);

- Direzione Amministrativa e Finanziaria/CFO;
- Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

La Società, inoltre, ha imposto il divieto di utilizzare denaro contante o qualsiasi altro strumento finanziario al portatore per qualunque operazione di incasso, pagamento, trasferimento di fonti o altro utilizzo di disponibilità finanziarie.

Coface SA ha, inoltre, implementato una specifica procedura interna, finalizzata a dettare le linee guida per la corretta gestione della liquidità aziendale, garantendo così la sicurezza dei mezzi di pagamento, la sicurezza dei flussi di cassa all'interno del Gruppo ([Allegato Z](#)).

Nello specifico, sono individuati le circoscritte ipotesi in cui è possibile il pagamento con la piccola cassa e il prelievo presso sportelli o bancomat. Sono, inoltre, individuate le forme di pagamento che dovranno essere utilizzate per le diverse transazioni, nonché le condizioni di apertura e di chiusura di conti correnti, tutto al fine di garantire la tracciabilità dei pagamenti emessi in favore o per conto della Società.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato D](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati

dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Nello specifico, dovrà essere comunicata all'OdV ogni condotta volta a concludere operazioni o transazione per mezzo di contanti.

E) DELITTI CONTRO L'INDUSTRIA ED IL COMMERCIO (ART. 25-BIS 1 D.LGS. 231/2001)

Con riferimento ai "Delitti contro l'industria ed il commercio" le risultanze della mappatura hanno consentito di ritenere che il rischio di compimento dei reati appare teoricamente ipotizzabile, esclusivamente in riferimento ai reati di "Turbata libertà dell'industria o del commercio" ex art. 513 c.p. e di "Illecita concorrenza con minaccia o violenza" ex art. 513-bis c.p.

Di seguito una sintetica descrizione delle fattispecie di reati che potrebbero essere realizzati e delle relative modalità attuative.

* * *

1.1 Turbata libertà dell'industria o del commercio (art. 513 c.p.)

La norma in oggetto punisce chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio.

Per "violenza sulle cose" devono intendersi tutti gli positivi, materiali e fisici esercitati sulle cose, che così vengono danneggiate o trasformate, mutandone la destinazione, impedendo alla cosa di assolvere alla funzione per la quale essa veniva utilizzata. Con tali condotte, di conseguenza, si ostacola materialmente l'attività economica e produttiva altrui.

Per "mezzi fraudolenti" devono intendersi tutte quelle condotte idonee a trarre in inganno e finalizzate a turbare l'esercizio di un'industria e del commercio.

1.2 Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.)

Il reato *de quo* punisce chiunque nell'esercizio di un'attività commercial, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia

Sanzioni maggiori sono previsti nel caso in cui gli atti di concorrenza riguardino un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri Enti Pubblici.

Per "violenza" deve intendersi qualsiasi condotta idonea a privare coattivamente l'offese della libertà di determinazione d'azione.

Per "minaccia", invece, si intendono quei comportamenti idonei ad incutere timore e a suscitare la preoccupazione di un male e/o danno ingiusto, al fine di ottenere dal soggetto passivo l'omissione o la tolleranza di qualcosa.

2. LE ATTIVITA' A RISCHIO REATO

Tenuto conto della peculiarità di Coface SA, le attività considerate più specificatamente a rischio in relazione ai reati descritti sono ritenute le seguenti:

attività di ideazione e di lancio di nuovi prodotti e di gestione del marchio, della comunicazione esterna o pubblicitaria e delle iniziative di marketing. La costituzione di rapporti di natura commerciale con Soggetti Terzi, la gestione dei rapporti con società concorrenti.

Inoltre, tale fattispecie delittuose potrebbero essere poste in essere nell'ambito dei rapporti con gli Agenti che operano nell'interesse della Società.

2.1 Possibili modalità attuative.

Rappresentato possibilità modalità attuative dei reati sopra descritti:

- La predisposizione di atti di concorrenza sleale o di piani volti a porre in essere turbative dell'attività industriale;
- Storno dei dipendenti;
- Sviamento dei Clienti.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Le funzioni e le aree aziendali ritenute maggiormente a rischio consumazione reati ex art. 25-bis 1 D.lgs. 231/2001 sono:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione Commerciale;
- Direzione Vendite;
- Direzione Cauzione;
- Direzione Marketing;
- Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato E](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Nello specifico, dovrà essere data comunicazione all'OdV di ogni condotta che anche solo potenzialmente possa essere lesiva della libera concorrenza.

F) I REATI SOCIETARI (ART. 25 TER)

Con riferimento ai reati societari, le risultanti della mappatura hanno consentito di ritenere che il rischio di compimento dei reati appare teoricamente ipotizzabile in parte delle fattispecie previste.

La Sede secondaria italiana produce dati contabili che vengono trasmessi alla Sede di Parigi e che confluiscono nel bilancio di quest'ultima. Gli illeciti appartenente a tale categoria potrebbero realizzarsi qualora la sede italiana comunicasse fatti non rispondenti al vero, oppure omettesse informazioni la cui comunicazione è obbligatoria per legge e da ciò, derivasse un danno patrimoniale a soci o a creditori.

Le operazioni tramite le quali tali condotte potrebbero realizzarsi attengono la predisposizione del bilancio (ad opera della Sede francese), nel quale potrebbero - a causa delle comunicazioni provenienti dalle differenti Direzioni della sede italiana - essere inserite esposizioni non veritiere circa la posizione economica, patrimoniale o finanziaria dell'Unità italiana, ovvero omessi fatti in grado di rappresentarne le effettive condizioni.

Di seguito una sintetica descrizione delle fattispecie di reato che si potrebbero realizzare nello svolgimento di alcune attività di Compagnia, e delle individuate modalità con cui esse potrebbero essere compiute.

* * *

1.1. False comunicazioni sociali (art. 2621 Cod. Civ.)

La norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo a indurre altri in errore.

Con la riforma del 2015 (Legge n. 69/2015) il Legislatore ha inasprito tale reato, trasformandolo da fattispecie contravvenzionale a delitto punito con la pena da uno a cinque anni di reclusione, introducendo, però, l'art. 2621-bis Cod. Civ. per i fatti di lieve entità, la cui cornice edittale è da sei mesi a tre anni di reclusione. In aggiunta è stato previsto che se i fatti previsti dall'art. 2621 Cod. Civ. riguardano società che non superano i limiti indicati dal comma II dell'art. 1 del Regio Decreto 267/1942, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale.

Tale reato è realizzabile attraverso due differenti condotte: la prima attiva, consistente nell'esposizione di fatti non rispondenti al vero sulla situazione economica, patrimoniale o finanziaria della società o del gruppo a cui appartiene e la seconda omissiva, integrata dalla mancata indicazione di fatti, la cui comunicazione è imposta dalla legge.

Da ultimo va sottolineato come, con la riforma del 2015, il Legislatore abbia previsto, anche per la condotta omissiva, che debba aver per oggetto "fatti materiali rilevanti" e non più mere "informazioni".

1.2. False comunicazioni sociali delle società quotate (art. 2622 Cod. Civ.)

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

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

Alle società sopra indicate sono equiparate: 1) le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea; 2) le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano; 3) le società che

controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea; 4) le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Tale delitto è configurabile nei confronti dei componenti del collegio sindacale di una società quotata in borsa, allorché non provvedano a segnalare la non veritiera rappresentazione, in bilancio, di elementi informativi sulle operazioni di maggior rilievo economico dell'ente, riscontrati nell'esercizio della propria attività di controllo sul rispetto dei principi di corretta amministrazione e sulla adeguatezza degli assetti amministrativi e contabili.

1.3. Impedito controllo (Art. 2625 Cod. Civ.)

I tipi di condotta sanzionati dalla norma sono di due tipologie: l'occultamento di documenti e l'utilizzo di altri idonei artifici per impedire o ostacolare lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali.

L'impedito controllo è un reato proprio; pertanto, il medesimo può essere commesso esclusivamente dagli amministratori.

La sanzione penale è prevista solo nel caso in cui dalla condotta posta in essere derivi un danno ai soci, riqualificando gli altri casi come illecito amministrativo.

Il reato de quo si perfeziona mediante le seguenti condotte tipiche:

- diniego o accesso alla sede o alle scritture contabili;
- alterazione o sottrazione delle scritture contabili;
- occultamento dei libri sociali;
- rifiuto a fornire chiarimenti o notizie su determinate operazioni;
- omessa convocazione dell'assemblea pur in presenza di richiesta di soci come previsto dalla legge, quando tale assemblea sia richiesta per finalità di controllo.

Si tratta, più precisamente, delle attività che influiscono:

- sulle iniziative di controllo dei soci previste dal Codice Civile e dagli altri atti normativi, quali, ad esempio, l'art. 2422 Cod. Civ., che prevede il diritto dei soci di ispezionare i libri sociali;
- sulle attività di controllo del Collegio Sindacale, previste dal Codice Civile e dagli altri provvedimenti normativi, quali, ad esempio, gli artt. 2403 e 2403 bis, che prevedono il potere dei membri del Collegio Sindacale di procedere ad atti di ispezione e di controllo e di richiedere agli amministratori notizie sull'andamento delle operazioni sociali o di determinati affari;
- sulle attività delle società di revisione, previste dalle leggi in materia, quali, ad esempio, quelle disciplinate dagli artt. 2049 da bis a septies Cod. Civ.

La norma prevede, dunque, una tutela del:

- controllo interno operato dal collegio sindacale;

- controllo interno operato dal collegio sindacale (nelle società di capitali, a norma dell'art. 2403 Cod. Civ.) o dai soci (nei casi previsti, ad esempio, dal codice civile).

1.4 Indebita restituzione dei conferimenti (Art. 2626 Cod. Civ.)

Il reato si configura quando gli amministratori, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci, ovvero li liberano dall'obbligo di eseguirli.

La restituzione dei conferimenti può avvenire sia in forma palese, ancorché indiretta (ad esempio, tramite la compensazione di un debito del socio nei confronti della società), che simulata (ad esempio attraverso il riconoscimento ad un socio di un credito in realtà inesistente, la stipulazione di un mutuo fittizio, la concessione di un prestito senza serie prospettive di restituzione, corresponsione di onorari per prestazioni professionali inesistenti o comunque inadeguate), ovvero attraverso una distribuzione di acconti-dividendo o di utili fittizi effettuata con somme prelevate dal capitale sociale.

La seconda ipotesi di condotta consiste nell'esonero dei soci dall'obbligo di eseguire conferimenti rimasti in tutto o in parte inadempiti.

Soggetti attivi del reato possono essere solo gli amministratori (reato proprio): la Legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 Cod. Pen., anche i soci che hanno svolto un'attività di istigazione o di determinazione nei confronti degli amministratori.

1.5. Illegale ripartizione degli utili e delle riserve (Art. 2627 Cod. Civ.)

Il reato si configura in capo agli amministratori che ripartiscono utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Tuttavia, la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estinguono il reato.

La condotta criminosa di tale reato 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.

Quanto alla individuazione della nozione di "utili", si ritiene che il termine vada inteso nella sua accezione più ampia, quale "utile di bilancio", ossia qualsiasi incremento del patrimonio netto rispetto al valore nominale del capitale, anche se indipendente (diversamente dall'utile d'esercizio) dall'esercizio dell'attività economica.

Ai fini della sussistenza del reato deve trattarsi di utili non effettivamente conseguiti (e, dunque, fittizi), ovvero non distribuibili, perché destinati per legge a riserva: rilevano, dunque, le sole

riserve legali, quali, ad esempio, quelle imposte alla società dagli artt. 2423, comma IV, 2426, n. 4 Cod. Civ.

Assume rilievo penale anche la distribuzione di riserve, ancorché non costituite con utili indisponibili per legge, restando controverso se applicabile anche alle riserve da sovrapprezzo, nonché a quelle da rivalutazione.

Quanto all'illegitimo ripartizione di acconti sui dividendi, ossia la distribuzione di acconti su un futuro dividendo in corso di esercizio, il legislatore si limita a sanzionare la ripartizione di acconti sugli utili solo nel caso in cui essi non siano effettivamente conseguiti o siano destinati a riserva legale.

Soggetti attivi del reato sono gli amministratori (reato proprio).

1.6 Illecite operazioni sulle azioni o quote sociali o della società controllante (Art. 2628 Cod. Civ.)

Commettono il reato in esame gli amministratori che, fuori dei casi consentiti dalla Legge (cfr., in particolare, gli artt. 2357, 2359 *bis*, comma I, 2360, 2483 e 2529 Cod. Civ.), acquistano o sottoscrivono azioni o quote sociali, anche della società controllante (cfr. art. 2359 Cod. Civ.), cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Si precisa che il reato si estingue se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio afferente all'esercizio in relazione al quale è stata posta in essere la condotta.

Le operazioni sulle azioni proprie appartengono alla fisiologia della gestione delle società e possono assolvere a varie funzioni sotto il profilo economico-aziendalistico, molte delle quali perseguite nell'interesse o a vantaggio della Società, e dunque idonee, ove sussistano gli estremi del reato di cui all'art. 2628 Cod. Civ., a dar luogo ad una concorrente responsabilità della Società.

Si pensi, ad esempio, ad operazioni di investimento di fondi sociali compiute a fini di speculazione finanziaria; ovvero al rastrellamento delle azioni al fine di fronteggiare la prospettiva di scalate ostili mediante offerte pubbliche di acquisto; ovvero ancora, per le banche quotate in borsa, ad operazioni volte a regolarizzare i propri corsi azionari, evitando le oscillazioni del titolo in caso di assenza di domanda delle azioni della Società.

Più problematica la configurabilità di una concorrente responsabilità dell'ente nell'ipotesi in cui l'operazione di buy-back sia indirizzata più specificamente a fini interni alla compagine sociale, non direttamente riconducibili ad un interesse generale della Società: così, ad esempio, nel caso di acquisto di azioni realizzato al fine di rafforzare il potere di una maggioranza rispetto alle minoranze, oppure di modificare degli assetti di potere esistenti.

Un'ultima considerazione riguarda le operazioni finanziarie di c.d. *leveraged buyout*, finalizzate all'acquisto di attività di un'azienda, o di partecipazioni di società (azioni o quote), finanziate da un consistente ammontare di debiti e da un limitato o nullo ammontare di mezzi propri, consentiti

dall'utilizzo delle attività oggetto dell'acquisizione e dal flusso di cassa che l'investimento genererà in futuro.

La rilevanza penale di tali operazioni – che era stata oggetto di dibattito in passato – è oggi espressamente esclusa dal legislatore: come si legge infatti nella relazione, *“le operazioni di leveraged buyout sono espressamente considerate a parte dalla legge delega, che conferisce ad esse il crisma della legittimità (art. 7, lett. d)”*.

L'art. 2501 *bis* Cod. Civ. – introdotto dalla Riforma del diritto societario (D. Lgs. 6/2003) entrata in vigore il 1° gennaio 2004 – prevede espressamente la possibilità di procedere alla “fusione tra società, una delle quali abbia contratto debiti per acquisire il controllo dell'altra, quando per effetto della fusione il patrimonio di quest'ultima viene a costituire garanzia generica o fonte di rimborso di detti debiti”.

1.7. Operazioni in pregiudizio dei creditori (Art. 2629 Cod. Civ.)

Il reato in esame si configura quando gli amministratori, violando le disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con un'altra società, o scissioni, cagionando danno ai creditori.

Si precisa che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Il bene tutelato è l'integrità del capitale sociale quale generale garanzia dei creditori.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori. Tuttavia, i soci che votino la delibera di riduzione del capitale sociale, consapevoli di indurre gli amministratori al fatto, possono eventualmente concorrere nel reato ex art. 110 Cod. Pen.

1.8. Omessa comunicazione del conflitto d'interessi (Art. 2629 *bis* Cod. Civ.)

La fattispecie è stata introdotta dall'art. 31 della Legge 262/2005, che ha altresì previsto l'introduzione dell'art. 2629 *bis* Cod. Civ. tra i reati che, a norma dell'art. 25 *ter* del Decreto 231, possono comportare, ove commessi nell'interesse o a vantaggio dell'ente, la sua responsabilità amministrativa.

La condotta esecutiva del reato è imperniata sulla violazione del precetto civilistico previsto dall'art. 2391 Cod. Civ. nell'ipotesi in cui ne derivi un danno alla società o a terzi.

Tale norma – al fine dichiarato di assicurare il valore della trasparenza nella gestione – impone oggi ai componenti del Consiglio di Amministrazione di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione e, ove si tratti di Amministratore delegato, astenersi dal compiere l'operazione.

La norma si applica esclusivamente a:

- “società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea”;

- “società con titoli [...] diffusi tra il pubblico in misura rilevante ai sensi dell’art. 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58”;
- “soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385”, ossia banche, gruppi bancari e intermediari finanziari;
- “soggetto sottoposto a vigilanza ai sensi del Testo unico di cui al decreto legislativo n. 58 del 1998”, ossia le imprese di investimento (SIM e imprese di investimento comunitarie ed extracomunitarie), le società di gestione del risparmio (SGR), le società di gestione armonizzate, le società di investimento a capitale variabile (SICAV), gli intermediari finanziari iscritti nell’elenco previsto dall’art. 107 del T.U. bancario e le banche autorizzate all’esercizio dei servizi di investimento;
- “soggetto sottoposto a vigilanza ai sensi del d. lg. 7 settembre 2005, n. 209”;
- “soggetto sottoposto a vigilanza ai sensi del decreto legislativo 21 aprile 1993, n. 124”.

1.9. Formazione fittizia del capitale (Art. 2632 Cod. Civ.)

Tale ipotesi di reato mira a tutelare la integrità del capitale sociale, punendo gli amministratori ed i soci conferenti che:

- formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all’ammontare del capitale sociale. Trattasi di condotta che impedisce la integrale copertura del capitale nominale;
- effettuano una sottoscrizione reciproca di azioni o quote. Il carattere della reciprocità non richiede necessariamente la contestualità temporale delle operazioni, né la loro connessione. La sottoscrizione reciproca può, infatti, concernere sia operazioni omogenee (relative, ad esempio, all’aumento del capitale) sia operazioni tra loro eterogenee (concernenti, ad esempio, la costituzione della società e l’aumento del capitale). Ciò che rileva è la previa sussistenza di uno specifico accordo (anche tacito), non casuale incentrato su di un’intesa *ad hoc*, avente appunto ad oggetto lo scambio di azioni o quote. Si tratta di un reato necessariamente plurisoggettivo;
- effettuano una sopravvalutazione rilevante dei conferimenti di beni in natura e dei crediti ovvero del patrimonio sociale nel caso di trasformazione. La terza condotta incriminata dalla norma in esame può essere realizzata sia in fase genetica di costituzione della società che in quella successiva di aumento di capitale sociale. Oggetto della sopravvalutazione sono, alternativamente, i beni, i crediti ed il patrimonio.

Soggetti attivi del reato sono gli amministratori e i soci conferenti. Soggetto attivo può essere anche l’esperto nominato dal Tribunale che redige la relazione giurata di stima da allegare all’atto costitutivo o di aumento del capitale sociale.

1.10. Indebita ripartizione dei beni sociali da parte dei liquidatori (Art. 2633 Cod. Civ.)

Tale ipotesi di reato si configura nei casi in cui il liquidatore cagioni un danno ai creditori sociali per aver ripartito i beni della società tra i soci prima ancora di aver soddisfatto i creditori sociali stessi ovvero di aver accantonato le somme necessarie per soddisfarli.

Il reato si estingue se, prima del giudizio, ai creditori venga rifuso il danno dagli stessi patito a seguito della suddetta condotta illecita.

Soggetti attivi del reato sono esclusivamente i liquidatori (reato proprio).

1.11. Illecita influenza sull'assemblea (Art. 2636 Cod. Civ.)

Tale ipotesi di reato si configura nel caso in cui chiunque (gli amministratori, i direttori generali, il dirigente preposto, i sindaci, i liquidatori e/o i responsabili della revisione), con atti simulati o fraudolenti, determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.

Si precisa che la norma si applica anche alle società con socio unico o, comunque, quasi totalitario, in quanto anche in tali casi è evidentemente possibile l'alterazione della volontà del socio espressa in assemblea.

La norma mira ad evitare che, attraverso condotte fraudolente (come, ad esempio, la cessione fittizia delle quote a persona di fiducia al fine di ottenerne il voto in assemblea oppure la fittizia sottoscrizione di un prestito con pegno delle quote, in modo da consentire al creditore pignoratizio l'esercizio del diritto di voto in assemblea) si influisca illegittimamente sulla formazione della maggioranza assembleare.

Ai fini della norma in esame vengono in considerazione le condotte volte alla convocazione dell'assemblea, all'ammissione alla partecipazione all'assemblea e al computo dei voti per la deliberazione, nonché le relative attività di supporto.

È opportuno ricordare che la responsabilità della Società è configurabile solo quando la condotta prevista dall'articolo in esame sia realizzata nell'interesse di Coface SA

Ciò rende difficilmente ipotizzabile il reato in questione che, di norma, viene realizzato per favorire interessi di parte e non della Società.

1.12. Aggiotaggio (Art. 2637 Cod. Civ.)

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

Anche questo reato è un reato comune, che può essere commesso da chiunque.

1.13. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (Art. 2638 Cod. Civ.)

Si tratta di una fattispecie generale che, a fini di coordinamento e di uniformità sanzionatoria, si sostituisce alle diverse figure di falsità nelle comunicazioni, di omissione di comunicazioni e di ostacolo nello svolgimento delle funzioni delle Autorità di Vigilanza previste fuori dal Codice civile (ad esempio, Banca d'Italia, U.I.F., Ivass).

La norma individua due distinte ipotesi di reato:

- la prima si realizza attraverso l'esposizione nelle comunicazioni alle Autorità di Vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima;
- la seconda, che configura un reato di evento a forma libera, si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza, attuato consapevolmente, in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità di vigilanza.

La fattispecie *de qua* individua un'ipotesi di reato proprio, per cui soggetti attivi sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione di documenti contabili societari, i sindaci, i liquidatori di società ed enti e gli altri soggetti per legge alle Autorità pubbliche di vigilanza, o tenuti a obblighi nei loro confronti.

1.14. False o omesse dichiarazioni per il rilascio del certificato preliminare (Art. 54 D.lgs. 19/2023)

Tale norma punisce chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'art. 29 D.lgs. 19/2023 (*certificato rilasciato dal notaio alle società italiane partecipanti a fusioni transfrontaliere, attestante il regolare adempimento degli atti e delle formalità preliminari al progetto di fusione*), forma documenti, in tutto o in parte falsi, altera documenti verdi, rende dichiarazioni falsi oppure omette informazioni rilevanti.

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

Tale norma punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

Tale reato si applica anche a chi, nell'ambito organizzativo della società o dell'ente privato, esercita funzioni direttive da quelle sopra indicate.

È prevista una pena inferiore laddove il fatto sia commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

Le stesse pene si applicano, inoltre, a chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuta alle persone sopra indicate.

Con la riforma del 2017, il Legislatore ha incluso tra gli autori del reato anche coloro che svolgono attività lavorativa mediante l'esercizio di funzioni direttive presso società o enti privati.

1.16. Istigazione alla corruzione tra privati (art. 2635 bis Cod. Pen.)

È punito chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata.

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

2. LE ATTIVITA' A RISCHIO REATO

Tenuto conto della peculiarità di Coface SA, le attività considerate più specificatamente a rischio in relazione ai reati descritti sono ritenute le seguenti:

- predisposizione dei dati contabili che confluiranno nel bilancio della Sede, nonché delle comunicazioni relative alla situazione economica patrimoniale e finanziaria della Società;
- predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse
- Tenuta della contabilità, predisposizione dei bilanci, relazioni, comunicazione sociali in genere, nonché i relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza;
- gestione dei rapporti con la Società di Revisione;
- Operazioni relative al capitale e operazioni sulle azioni.

Di seguito si indicano nello specifico alcuni esempi di attività a rischio reato:

- redazione del bilancio, delle relazioni periodiche infrannuali e di qualsivoglia comunicazione prevista dalla legge nei confronti dei soci o del pubblico, anche se effettuata in via indiretta, ma tale da incidere su detti documenti;
- gestione di documenti utili all'esercizio delle attività di controllo o di revisione e/o redazione ed invio di relazioni e comunicazioni agli organi sociali;
- fatturazione attiva e passiva;
- gestione delle contestazioni, da parte degli assicurati sulla conformità o sulla qualità della polizza fornita;
- gestione dei rapporti con i clienti privati, società concorrenti e partner;
- gestione di ogni altra attività attraverso cui può realizzarsi il reato di corruzione nei confronti dei soggetti di cui sopra (attività strumentale);
- gestione degli omaggi aziendali;
- conferimento incarichi di consulenza, collaborazione e agenzia;
- gestione acquisti di prodotti e servizi;
- gestione dei beni aziendali che possono rappresentare utilità di scambio;

- gestione delle spese di rappresentanza/rimborsi spese;
- gestione delle pratiche di assunzione del personale;
- sponsorizzazioni;
- gestione di pagamenti, in qualsivoglia modalità o forma, e/o, in ogni caso, gestione dei flussi finanziari da o verso terzi.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- modifica o alterazione dei dati contabili presenti sul sistema informatico al fine di dare una rappresentazione della situazione economica, patrimoniale e finanziaria della Società difforme dal vero, anche in concorso con altri soggetti;
- fatturazione per prestazioni inesistenti;
- contabilizzazione di costi o ricavi fittizi;
- collaborazione di un funzionario della Società con la società di revisione in sede di valutazione di cespiti patrimoniali della Società in modo da occultarne le gravi perdite, così rappresentando una situazione economica, patrimoniale e finanziaria che eviti forte deprezzamento nel valore dell'azienda;
- mancato rispetto da parte degli amministratori della richiesta di informazioni, ad esempio, proveniente dal collegio sindacale in tema di applicazione alla Società di una specifica normativa, mediante l'occultamento, anche accompagnato da artifici, della documentazione utile a rappresentare i processi applicativi in sede aziendale di tale legge (es.: esibizione parziale o alterata di detta documentazione);
- restituzione dei conferimenti mediante qualsiasi forma negoziale in grado di garantire al socio un'effettiva attribuzione patrimoniale con conseguente depauperamento della Società;
- liberazione dall'obbligo di conferimento quando il capitale non è ancora integralmente versato e la Società rinuncia al credito vantato nei confronti dei soci;
- formazione dei prospetti di Bilancio in modo da alterare la rappresentazione di utili e riserve distribuibili;
- partecipazione degli amministratori a una delle operazioni straordinarie contemplate dalla norma in situazione di conflitto di interessi con la Società;
- partecipazione degli amministratori a una delle operazioni contemplate dalla norma fuori dei casi di cui agli articoli 2357 Cod. Civ., 2359-bis Cod. Civ., cagionando in tal modo una lesione all'integrità del capitale sociale;
- conclusione di un affare da parte di un amministratore che abbia anche un proprio interesse coinvolto nell'operazione, terzi creditori (es. fornitori, prestatori di garanzie etc.) e pregiudizio conseguente al creditore della propria pretesa creditoria;
- attribuzione di azioni nel complesso superiore all'ammontare del capitale sociale;
- reciproca sottoscrizione di azioni che, per l'entità delle risorse impiegate, vanno a intaccare il capitale sociale;
- rilevante sopravvalutazione dei conferimenti o del patrimonio.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

La funzione ed aree aziendali ritenute a rischio consumazione reati ex art. 25-ter D.lgs. 231/2001 sono:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione Amministrativa e Finanziaria/CFO
- Direzione del Personale e delle Risorse Umane (HR)
- Direzione Commerciale;
- Direzione Marketing;
- Direzione Tecnica;
- Direzione Ramo Cauzione;
- Direzione Ramo Credito;
- Direzione Fidi;
- Direzione Sistemi Informativi;
- Direzione Enhanced;
- Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Codice Anticorruzione (Allegato A-bis)**, che individua i principi e le regole di condotta a cui i Destinatari devono attenersi al fine di prevenire e limitare il rischio di consumazione dei “Reati Corruttivi”;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

Coface SA nella predisposizione dei documenti contabili e nella registrazione dei movimenti economico-finanziari, adotta i Principi Contabili Internazionali e, nello specifico, il principio “**IFRS 17**” – sistema di contabilizzazione tipico delle società di assicurazioni che consente di differire il costo di acquisizione dei clienti per l’intero periodo di durata della polizza assicurativa, il principio “**IFRS 15**” – avente ad oggetto i Ricavi provenienti con i Clienti - , “**IFRIC 23**” – avente ad oggetto l’incertezza in merito alla tassazione di una componente di reddito o di un’operazione.

La Società ha implementato e adottato specifiche procedure, aventi la funzione di guidare i propri dipendenti e le consociate (Es. Coface Italia S.r.l.) nell’applicazione di tali principi – [Allegato P](#), [Allegato Q](#), [Allegato R](#).

Allo stesso modo, le società appartenenti al Gruppo Coface e, dunque, la stessa Coface SA, saranno tenute al rispetto delle policy di Gruppo inerenti i “Costi e Disposizioni per la Gestione dei Sinistri di Recupero” ([Allegato S](#)), il “Calcolo delle imposte differite” ([Allegato T](#)) e le “Operazioni in valuta estera” ([Allegato U](#)).

L’insieme di tali procedure di Gruppo detta, quindi, le regole fondamentali che le consociate e la branch italiana Coface SA devono rispettare nella gestione della loro contabilità e tenuta dei documenti contabili.

Il Gruppo Coface, inoltre, al fine di limitare e prevenire condotte corruttive poste in essere dai propri dipendenti, amministratori o dirigenti (sia verso soggetti pubblici che privati) ha implementato la “*Gifts e Benefits Procedure*” ([Allegato A-ter](#)).

Nello specifico, tale procedura detta le regole e i protocolli che i Destinatari devono adottare laddove ricevano o offrano doni, benefici o ospitalità a Pubblici Ufficiali, Incaricati di un Pubblico servizio o soggetti privati.

In particolare, la procedura prevede che, entro determinati limiti, siano i Destinatari siano autorizzati ad offrire regali e benefici ai soggetti privati (clienti, fornitori, partner economici), purché il Responsabile della funzione di riferimento ed il Compliance Officer siano preventivamente informati.

La Società, al fine di garantire la tracciabilità delle regalie offerte o ricevute dai propri dipendenti ha predisposto il “Registro dei Regali e Beneficenze”, che deve essere continuamente aggiornato.

In merito, invece, ad eventuali donazioni di beneficenza, esse sono ammesse purché non destinate ad organizzazioni o partiti politici e purché siano preventivamente autorizzate dal *Regional Compliance Officer*.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l’implementazione e l’adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all’ [Allegato F](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l’obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell’esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all’Organismo di

Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Nello specifico, **il Responsabile della Direzione Amministrativa e Finanziaria** comunica all'OdV:

- pagamenti, anticipi di cassa o rimborsi verso soci;
- operazioni di finanziamento verso soci;
- cessione a titolo gratuito di cespiti e beni mobili aziendali a soci;
- eventuali rilievi mossi dalla società di revisione in merito alla predisposizione dei dati contabili che confluiscono del Bilancio.

La **società di revisione** comunica all'OdV eventuali rilievi mossi nello svolgimento della propria attività.

Tutti coloro i quali svolgono funzioni di controllo o supervisione sugli adempimenti connessi all'espletamento delle suddette attività devono riferire immediatamente all'OdV eventuali situazioni di irregolarità.

G) ABUSI DI MERCATO (ART. 25-SEXIES D.LGS. 231/2001)

Con riferimento all'attività societaria esercitata da Coface SA e considerando che essa è una società quotata sul mercato, si ritiene che, almeno in astratto, i reati ex art. 25-sexies D.lgs. 231/2001, siano a rischio consumazione.

Di seguito una sintetica descrizione delle fattispecie di reato che si potrebbero realizzare nello svolgimento di alcune attività di Compagnia, e delle individuate modalità con cui esse potrebbero essere compiute.

* * *

1.1 Manipolazione del mercato (Art. 185 D.lgs. 58/1998)

La norma in oggetto punisce chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

La fattispecie in esame è un reato di pericolo e, pertanto, ai fini della sua configurabilità e punibilità non è necessaria l'effettiva lesione ed alterazione del prezzo né, tantomeno, l'eventuale profitto dell'agente, essendo sufficiente che la condotta posta in essere, sia, anche solo potenzialmente a determinare l'evento.

1.2. Abuso o comunicazione illecita di informazioni privilegiate (Art. 184 D.lgs. 58/1998)

È punito chiunque, essendo in possesso di informazioni privilegiate, in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione anche pubblica, o di un ufficio:

- a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari, utilizzando le informazioni medesime;
- b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'art. 11 del regolamento (UE) n. 596/2014 del Parlamento Europeo e del Consiglio, del 16 aprile 2014;
- c) raccomanda o induce altri, sulla base di tali informazioni, al compimento di taluna delle operazioni indicate nella lettera a).

Allo stesso modo è punito chiunque, essendo in possesso di informazioni privilegiate a motivo della preparazione o dell'esecuzione di attività delittuose, commette taluno dei fatti precedentemente elencati.

Al di fuori dei casi di concorso nelle precedenti ipotesi, è punito, chiunque essendo in possesso di informazioni privilegiate per ragioni diverse da quelle sopra indicate e conoscendo il carattere privilegiate, commette taluno dei fatti sopra elencati.

Nello specifico, tale norma punisce tra diverse condotte:

- La condotta dell'*insider*, che "acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari, utilizzando le informazioni medesime" - lettera a)
- La condotta di *tipping*, che consiste nella "comunicazione dell'informazione privilegiata ad altri al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato", a prescindere dell'utilizzo che questo ne possa fare.
Il reato *de quo* non si configura laddove la comunicazione sia avvenuta in modo fortuito o quando l'agente ignori il carattere privilegiato dell'informazione in suo possesso;
- La condotta di *tuyautage*, che consiste nel "raccomandare o indurre altri al compimenti di operazioni in borsa, sulla base della conoscenza di informazioni privilegiate".

Fondamentale è chiarire la definizione di "Informazione Privilegiata", i cui elementi essenziali vengono individuati dall'art. 7, paragrafi 1 a 4 del Regolamento UE n. 956/2014.

Un'informazione affinché possa definirsi privilegiata deve essere:

1. precisa;
2. di natura non pubblica;
3. capace di incidere sensibilmente sui prezzi di strumenti finanziari.

Più specificatamente, può essere definita come "precisa" l'informazione che si riferisce ad un complesso di circostanze, o ad un evento, già in atto o di verifica ragionevolmente prevedibile e, dunque, caratterizzato da un elevato grado di oggettività e di certezza.

Essa, inoltre, deve essere sufficientemente specifica, circostanziata e determinata, in modo che chi la impiega sia posto in condizione di ritenere che dall'uso potranno effettivamente verificarsi effetti sul prezzo di strumenti finanziari.

È fondamentale, inoltre che essa sia “*price sensitive*” e, cioè, in grado di influire in modo sensibile sul prezzo degli strumenti finanziari.

Si distinguono tre diverse figure di *insider*:

- Insider primario, quali gli amministratori, sindaci, dirigenti e revisori, ossia coloro che vengono in possesso di un'informazione privilegiata in ragione della propria qualità istituzionale o della propria attività o della propria partecipazione al capitale emittente;
- Insider secondario, ossia colui che riceve l'informazione privilegiata da un insider primario;
- Insider criminale, colui che viene in possesso delle informazioni privilegiate attraverso un'attività delittuosa (Es. Accesso abusivo ad un sistema informatico).

2. LE ATTIVITA' A RISCHIO REATO

Attesa la natura dell'attività esercitata da Coface SA e la sua peculiarità strutturali, le attività considerate maggiormente a rischio rispetto alla consumazione dei “Reati di Abuso di mercato” sono quelle che comportano la conoscenza di informazioni privilegiate concernenti strumenti finanziari e quelle afferenti agli investimenti finanziari effettuati dalla Compagnia o per conto della stessa.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- compiere operazioni finanziarie simulate o diffondere notizie false al fine di alterare l'andamento del mercato finanziaria, al fine di avvantaggiare gli investimenti della Società o delle sue controllate;
- le informazioni eventualmente raccolte da un assunto nei confronti di un'azienda quotata, vengano utilizzate dalla Direzione Amministrativo e Finanziaria per compiere operazioni sul mercato finanziario.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

La funzione ed aree aziendali ritenute a rischio consumazione reati ex art. 25-sexies D.lgs. 231/2001 sono:

- Rappresentante della Sede Secondaria;
- Direzione Amministrativa e Finanziaria/CFO.
- Direzione Commerciale;
- Direzione Tecnica;
- Direzione Fidi;
- Direzione Enhanced;
- Agenti.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato G](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA

Nello specifico, la **Direzione Amministrativa e Finanziaria**, annualmente deve segnalare all'OdV le diverse tipologie di investimento operate.

Inoltre, al fine di limitare la possibile alterazione e manipolazione del mercato, è indispensabile che le comunicazioni dirette al pubblico, che anche solo potenzialmente possano generare ripercussioni sul presso di strumenti finanziari, siano preventivamente comunicate all'OdV, il quale potrà esprimere un parere non vincolante su di esse.

H) REATI DI OMICIDIO COLPOSO E LESIONI GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO (ART. 25-SEPTIES D.LGS. 231/2001)

I reati di seguito descritti presentano un elevato rischio di consumazione, considerando che Coface SA ha più di 150 Lavoratori alle proprie Dipendenze.

Coface SA si impegna a garantire un ambiente di lavoro salubre e sicuro, con l'intento di ridurre al minimo il rischio di infortuni sul lavoro.

* * *

1.1 Omicidio colposo (art. 589 Cod. Pen.)

La norma in oggetto punisce chiunque cagiona per colpa la morte di una persona con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Sono soggetti attivi di tale reato coloro che rivestono il ruolo di "garanti" ex art. 40 cpv, cioè i titolari di una c.d. posizione di controllo.

Il Testo unico per la sicurezza del lavoro ha individuato, quali soggetti titolari di tale posizione di garanzia, rispetto all'incolumità fisica dei lavoratori: il datore di lavoro, il dirigente ed il preposto. Inoltre, in virtù del principio di effettività, viene qualificato come garante anche colui che, pur sprovvisto di regolare investitura, eserciti in concreto i poteri giuridici riferiti a ciascuno dei soggetti prima indicati.

Va precisato, inoltre, come il D.lgs. 81/2008 ha introdotto l'istituto della "delega di funzioni", con conseguente subentro del preposto nella posizione di garanzia e, quindi, soggetto agli obblighi di prevenzione, assicurazione e sorveglianza originariamente gravanti sul Datore di Lavoro. È, però, necessario che tale delega risulti da atto scritto, recante data certa e inerente a un ambito ben definito, effettivo ed espresso e non l'intera gestione aziendale.

In qualsiasi caso va ricordato come la delega di funzioni non esenta il Datore di Lavoro da un potere e/o obbligo di vigilanza sull'operato del preposto.

1.2 Lesioni colpose gravi o gravissime (art. 590 Cod. Pen.)

Il reato si configura nel caso in cui siano cagionate per colpa ad una persona lesioni gravi o gravissime; il Legislatore ha definito le lesioni come una malattia nel corpo o nella mente, differenziandole profondamente dalle semplici percosse.

Le lesioni si considerano gravi nel caso in cui (art. 583, comma I, Cod. Pen.):

- dal fatto derivi una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a giorni 40;
- il fatto produce l'indebolimento permanente di un senso o di un organo.

Le lesioni si considerano gravissime nel caso in cui (art. 583, comma II Cod. Pen.):

- dal fatto derivi una malattia certamente o probabilmente insanabile;
- la perdita di un senso;
- la perdita di un arto o una mutilazione che lo renda inservibile;
- la perdita dell'uso di un organo o della capacità di procreare;
- una permanente e grave difficoltà della favella;
- la deformazione, ovvero lo sfregio permanente del viso.

Anche ai fini della configurabilità del reato di lesioni colpose, non è necessario che il soggetto agente abbia agito con la coscienza e volontà di cagionare l'evento lesivo (*animus necandi*) essendo sufficiente la negligenza, l'imprudenza, l'imperizia dello stesso, ovvero l'inosservanza di norme, regolamenti, ordini o discipline.

Entrambi i reati sopra richiamati rilevano, ai fini della responsabilità amministrativa della Società, unicamente nel caso in cui sia ascrivibile al soggetto agente, sotto il profilo dell'elemento soggettivo, la c.d. "colpa specifica", consistente nella violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene ed alla salute sul lavoro.

Atteso che, in forza di tale circostanza, assume rilevanza la legislazione prevenzionistica vigente, ai fini della presente Parte Speciale si intende integralmente richiamato il D. Lgs. 81/2001 (c.d. Testo Unico della Sicurezza, di seguito "Testo Unico") come da ultimo modificato dal D. Lgs. 106/2009 (e, comunque, come modificato tempo per tempo).

2. LE ATTIVITA' A RISCHIO REATO

Per quanto attiene l'individuazione e l'analisi dei rischi potenziali, la quale dovrebbe considerare le possibili modalità attuative dei reati in seno all'azienda, si rileva, con riguardo alle fattispecie previste dal D. Lgs. 81/2008, che l'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dall'azienda sulla scorta della legislazione prevenzionistica vigente, e, in particolare, degli artt. 28 e ss. del Testo Unico, come modificati dal D. Lgs. n. 106/2009.

Con precipuo riferimento ai reati oggetto della presente Parte Speciale, si sottolinea che non è possibile escludere aprioristicamente alcun ambito di attività, poiché tali reati potrebbero interessare la totalità delle componenti aziendali.

Alcune delle attività a rischio consumazione reati ex art. 25-septies D.lgs. 231/2001 sono:

- l'utilizzo di apparecchiature in movimento;
- utilizzo di sostanze chimiche potenzialmente pericolose (Es. solventi);
- l'utilizzo di mezzi di trasporto aziendali per motivi connessi all'attività lavorativa;
- l'utilizzo di scale e ascensori;
- l'utilizzo di impianti di erogazioni dei servizi tecnici per il funzionamento dello stabile.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- la mancata o insufficiente valutazione dei rischi connessi all'attività lavorativa;
- la mancata o insufficiente attuazione della legislazione antinfortunistica;
- la mancata osservanza delle segnalazioni del RSPP;
- la mancata manutenzione e revisioni degli impianti elettrici e dei dispositivi elettronici;
- la mancata adozione di misure sufficienti a garantire condizioni di lavoro dignitose e confortevoli.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

La tutela della salute e della sicurezza su Lavoro coinvolte, inevitabilmente, tutte le aree aziendali e, pertanto, è richiesto a tutti i Responsabili delle Funzioni una collaborazione nel garantire che tutti i dipendenti assegnati alla loro direzione, rispettino i principi di comportamento dettati dalla Società.

Le funzioni aziendali maggiormente a rischio rispetto la consumazione dei reati oggetto della presente sezione sono:

- Rappresentante della Sede Secondaria (County Manager);
- Datore di Lavoro;
- Responsabile del Servizio di Prevenzione e Protezione;
- Preposto.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

A presidio di tale area, la Compagnia ha stabilito specifiche norme comportamentali descritte sia nel *Regolamento Interno* che nel *Piano di Emergenza*, documenti entrambi resi disponibili a tutto il personale della Compagnia sulla intranet aziendale

È stata inoltre predisposta, nel Documento di Valutazione dei Rischi (DVR), una procedura atta a delineare tutti gli interventi che devono essere attuati per eliminare, ridurre o controllare rischi e pericoli presenti all'interno dei luoghi di lavoro. Tra di essi il legislatore ha individuato il cosiddetto stress lavoro correlato, la cui misurazione non ha evidenziato condizioni organizzative tali che possano determinare la presenza di stress correlato al lavoro.

Così come sancito dalla vigente normativa, Coface SA ha nominato, incaricato e ove necessario, curato la formazione delle seguenti figure chiave, avendo avuto cura di evidenziare per ciascuna di esse le responsabilità e i compiti sia organizzativi che operativi: Responsabile del Servizio di Prevenzione e Protezione (RSPP), Medico Competente, Delegato del Datore di Lavoro, Preposto, Rappresentante dei Lavoratori per la Sicurezza (RLS), Addetti alle Emergenze (antincendio e primo soccorso).

Tale organigramma della sicurezza è portato a conoscenza del Personale a tutti i livelli aziendali.

Annualmente la Compagnia, con la collaborazione dei RSPP, Medico Competente, ed RLS, esamina il DVR, l'andamento degli infortuni e delle malattie professionali, i programmi di formazione, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale.

Nel caso in cui la Compagnia assegni in appalto attività da compiersi all'interno delle proprie sedi, sono acquisiti i documenti atti a certificare il rispetto della normativa da parte dell'appaltatore; ove necessario viene predisposto il Documento Unico per la Valutazione dei Rischi interferenziali (DUVRI), contenente la valutazione dei rischi in cui può incorrere il personale dell'appaltatore prestando la propria opera presso Coface SA, e le misure preventive adottate. In ottemperanza agli obblighi di formazione ed informazione previsti dal D.Lgs. 81/08 la Compagnia organizza periodicamente corsi sulla sicurezza destinati ai neoassunti.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato H](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Più concretamente, come previsto dall' appendice A delle Linee Guida INAIL del 20 gennaio 2023, l'Organismo di Vigilanza deve essere tempestivamente informato circa:

- Eventuali aggiornamenti del DVR;
- Verbali delle riunioni periodiche ex art. 35 D.lgs. 81/2008;
- Rapporti di controlli ispettivi interni o segnalazioni dai preposti;

- Verbali dei sopralluoghi del RSPP;
- Adempimenti tecnico-amministrativi e documentali attestanti la conformità ai requisiti di sicurezza di luoghi di lavoro, postazioni di lavoro, macchine, impianti ed attrezzature di lavoro;
- Certificazione di conformità CE di attrezzature, macchine, impianti o documentazione alternativa attestante la conformità normativa;
- Evidenza della scelta degli appaltatori;

Allo scopo di svolgere i propri compiti, l'OdV può:

- partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

L'OdV, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; gli Addetti al Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso, il responsabile per la sicurezza a terra e a bordo).

Laddove l'OdV riscontri situazioni di non applicazione delle procedure adottate mediante il Modello, ne dà comunicazione all'Organo Amministrativo per l'avvio degli eventuali procedimenti disciplinari nonché verifica le cause che hanno determinato la non applicazione e definisce gli adeguati interventi correttivi.

Laddove l'OdV riscontri situazioni di non efficacia delle procedure adottate, ne verifica le cause e predispone le necessarie azioni correttive sottoponendo le relative proposte all'Organo Amministrativo per la conseguente adozione.

La Società istituisce – con il coinvolgimento del RSPP, laddove nominato – a favore dell'OdV i flussi informativi idonei ad acquisire le informazioni utili per il monitoraggio degli infortuni, dei dati e dell'organizzazione della sicurezza, nonché notizie di eventuali malattie professionali accertate o presunte, con particolare riferimento alle ipotesi di contagio da malattie infettive.

In conformità a quanto previsto nella Procedura di Whistleblowing, adottata dalla Società, i Destinatari del Modello, che nell'esercizio delle proprie attività lavorative, dovessero riscontrare violazioni delle Procedure e dei Protocolli, nonché venire a conoscenza di condotte illecite, rilevanti ai sensi e per gli effetti del Decreto Legislativo 231/2001, devono darne immediata comunicazione all'Organismo di Vigilanza.

I) REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA NONCHÉ DI AUTORICICLAGGIO E TERRORISMO (ARTT. 25-OCTIES E 25-QUATER D.LGS. 231/2001)

Si è ritenuto opportuno trattare congiuntamente le tipologie dei reati di riciclaggio e terrorismo, quantunque ledano interessi differenti, in quanto dall'analisi svolta si è rilevato come gli illeciti di cui all'art. 25-octies del D.Lgs. 231/01 risultino essere gli strumenti utilizzati per finanziare o supportare i reati di cui all'art. 25-quater D.Lgs. 231/01.

Ad ogni modo, si ritiene che in riferimento ai "Reati con finalità di terrorismo", gli unici che, ipoteticamente, potrebbero essere consumati sono i reati ex artt. 270, 270-bis, 270-ter, 270-quater, 270-quinques e 380 c.p.

Con riferimento ai reati all'esame le risultanze della mappatura hanno consentito di ritenere che il rischio di compimento dei reati appare teoricamente realizzabile.

Di seguito una sintetica descrizione della fattispecie di reato che potrebbe essere realizzato e delle relative modalità attuative.

* * *

1.1 Ricettazione (art. 648 Cod. Pen.)

Fuori dei casi di concorso nel reato, è punito chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o, comunque, si intromette nel farle acquistare, ricevere od occultare.

Con la riforma del 2021 è stata previsto che si configuri il reato ex art. 648 Cod. Pen. anche quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi.

Va sottolineato che tale reato si ritiene sussistente anche laddove l'autore del reato presupposto non sia imputabile o non sia punibile, ovvero quando manchi una condizione di procedibilità riferita a tale reato.

Per la configurabilità della ricettazione non è richiesto un accertamento giudiziale in merito alla sussistenza del delitto presupposto. La provenienza delittuosa del bene può essere desunta dalla natura e dalla caratteristica del bene stesso.

In egual modo non è necessario che sia noto l'autore del delitto presupposto.

1.2 Riciclaggio (art. 648-bis Cod. Pen.)

Fuori dei casi di concorso nel reato, è punito chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Con la riforma del 2021 è stato previsto che il delitto ex art. 648-bis Cod. Pen. si configuri anche laddove il fatto riguardi denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi.

Come per la ricettazione, anche per il riciclaggio non è necessaria la precisa individuazione del delitto presupposto, né la precisa indicazione delle persone offese, essendo sufficiente che venga raggiunta la prova logica della provenienza illecita delle utilità oggetto delle operazioni compiute.

1.3 Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter Cod. Pen.)

La norma sanziona chi, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis Cod. Pen., impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Con la riforma del 2021 è stato previsto che tale reato si configuri anche laddove il fatto riguardi denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi.

I reati di "Ricettazione", "Riciclaggio" e "Impiego di denaro, beni o utilità di provenienza illecita" si pongono in un rapporto di specialità, che scaturisce dal diverso elemento soggettivo richiesto dalle tre fattispecie.

Ed invero, pur essendo comune l'elemento materiale della disponibilità di denaro o altra utilità di provenienza illecita, il delitto ex art. 648 Cod. Pen. richiede una generica finalità di profitto, quello di cui all'art. 648 bis Cod. Pen. lo scopo ulteriore di far perdere le tracce dell'origine illecita e quello ex art. 648 ter Cod. Pen. che tale scopo sia perseguito mediante l'impiego delle risorse in attività economiche o finanziarie.

Quanto alla nozione di "attività economica o finanziaria", con essa non ci si riferisce alle sole attività produttive, ma anche alle attività di scambio e distribuzione dei beni sul mercato, nonché ad ogni altra attività che possa rientrare in una di quelle indicate negli artt. 2082, 2135 e 2195 Cod. Civ.

1.4 Autoriciclaggio (art. 648-ter.1 Cod. Pen.)

La norma punisce chiunque, avendo commesso o concorso a commettere un delitto, 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.

Con la riforma del 2021 è stato previsto che tale reato si configuri anche laddove il fatto riguardi denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Prima dell'introduzione della punibilità dell'autoriciclaggio, le condotte successive alla commissione del reato e dirette ad assicurare il profitto rientravano nella categoria del post factum non punibile.

La determinazione delle condotte punibili viene circoscritta a quei comportamenti che rendono obiettivamente difficoltosa l'identificazione della provenienza delittuosa del bene.

1.5. Associazioni sovversive (Art. 270 Cod. Pen.)

La norma in esame punisce chiunque nel territorio dello Stato promuove, costituisce, organizza o dirige associazioni dirette e idonee a sovvertire violentemente gli ordinamenti economici o sociali costituiti nello Stato ovvero a sopprimere violentemente l'ordinamento politico e giuridico dello Stato.

È punito, inoltre, anche chi partecipi solamente a tali associazioni o chi ricostituisca, anche sotto falso nome o forma simulata, le associazioni di tal guida, di cui sia stato ordinato lo scioglimento.

1.6. Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (Art. 270 bis Cod. Pen.)

Il reato *de quo* punisce chiunque promuova, costituisca, organizzi, diriga o finanzi associazioni aventi come obiettivo il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

È punito anche chi partecipi solamente a tali associazioni.

La norma in oggetto precisa che ai fini della legge penale, ricorrono le "finalità di terrorismo" anche quanto gli atti di violenza siano rivolti contro uno Stato estero, un'istituzione e un organismo internazionale

1.7. Assistenza agli associati (Art. 270 ter Cod. Pen.)

Ai sensi e per gli effetti di tale articolo è punito chiunque, fuori dai casi di concorso nel reato o di favoreggiamento, da rifugio o fornisce vitto, ospitalità, mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni previste e punite dagli artt. 270 e 270 bis c.p.

Ad ogni modo, non è punibile chi commette il fatto in favore di un prossimo congiunto.

1.8. Arruolamento con finalità di terrorismo anche internazionale (Art. 270 quater Cod. Pen.)

La norma in oggetto punisce chiunque arruola una o più persone al fine di compiere atti di violenza ovvero sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale.

1.9. Addestramento ad attività con finalità di terrorismo anche internazionale (Art. 270 quinquies Cod. Pen.)

Il reato *de quo* punisce chiunque addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, anche se rivolti contro uno Stato estero, un'istituzione o un organismo internazionale.

1.10. Attentato per finalità terroristiche o di eversione (Art. 280 Cod. Pen.)

La norma in oggetto punisce chiunque, per finalità di terrorismo o di eversione dell'ordine democratico, attenta alla vita od alla incolumità di una persona.

Sono previsti aumenti di pena se tali condotte sino rivolte contro persone che esercitano funzioni giudiziarie o penitenziarie ovvero di sicurezza pubblica nell'esercizio o a causa delle loro funzioni.

Ulteriore aggravio di pena sussiste laddove dal fatto derivi la morte della persona.

* * *

Va precisato che si ritiene che Coface SA, potrebbe rispondere dei reati previsti dai paragrafi da 1.5. a 1.10., esclusivamente a titolo di concorso, nel caso in cui, nell'espletamento delle proprie attività, non compiendo una accurata attività di due diligence sui propri clienti e/o fornitori finanzia, direttamente o indirettamente, tali tipologie di associazioni.

2. LE ATTIVITA' A RISCHIO REATO

Considerato l'oggetto sociale di Coface SA e le attività da essa esercitate, si ritiene che le attività maggiormente a rischio consumazione dei reati sopra descritti sono:

- negoziazione, stipulazione ed esecuzione di contratti di acquisto;
- transazioni finanziarie, investimenti e/o sponsorizzazioni con soggetti terzi;
- investimenti con società controllate o con società controllante;
- gestione dei beni della Società;
- gestione dei flussi finanziari e dei pagamenti e/o, comunque, svolgimento di operazioni, di qualsivoglia tipo e con qualsivoglia modalità, su denaro, beni o altri strumenti della Società;
- gestione della fatturazione;
- gestione dei rapporti e/o esecuzione di depositi, trasferimenti, cambi, acquisti di strumentifinanziari o altri beni con banche ed intermediari finanziari.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- La **gestione del processo di Bilancio e della fiscalità** (es.: presentazione delle dichiarazioni fiscali) potrebbe essere strumentale alla commissione del reato di **autoriciclaggio** nell'ipotesi in cui, ad esempio, un soggetto apicale o sottoposto della Società, avvalendosi di fatture o altri documenti per operazioni inesistenti al fine di evadere le imposte sui redditi o sul valore aggiunto, indichi in una delle dichiarazioni annuali relative a dette imposte elementi passivi fittizi e costituisca così una provvista di

provenienza illecita impiegata, sostituita, trasferita dallo stesso soggetto in attività economiche, finanziarie, imprenditoriali in modo da ostacolare concretamente l'identificazione della provenienza delittuosa;

- Gli organi dirigenti della Società trasferiscono denaro o altri beni, di provenienza delittuosa, ad altre società del Gruppo, nel tentativo di ostacolare la loro illecita provenienza;
- La Società eroga un prestito ad altre società del Gruppo, garantito da un pegno costituito da un bene, uno strumento finanziario rubato o comunque frutto di attività illecite;
- Finanziamento tramite messa a disposizione di fonti (tra i quali rientrano le garanzie fideiussorie) o di risorse economiche.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Le principali funzioni e aree aziendali all'interno delle quale il rischio di consumazione dei reati individuati in tale sezione sono:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione Amministrativa e Finanziaria;
- Direzione Commerciale;
- Direzione Vendite;
- Direzione Tecnica;
- Direzione Ramo Cauzione;
- Direzione Ramo Credito.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

Pur non essendo Coface SA, in quanto operante nei soli rami danni, destinataria degli obblighi derivanti dalla vigente normativa Antiriciclaggio, la Compagnia non si è limitata ad attenersi alla residuale disciplina inerente la gestione degli assegni e dei contanti (cui ciascun soggetto giuridico deve ordinariamente attenersi) vietando per esempio a priori qualsiasi genere di transazione in contanti ma, sulla scorta delle disposizioni rese dalla Sede Centrale del Gruppo, che è invece soggetta alla normativa nazionale derivante dalla III Direttiva Europea n. 60 del

26/10/2005 (Prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo) effettua periodicamente controlli volti a verificare il rispetto della normativa internazionale e nazionale sul tema (c.d. Progetto Color), ne applica le procedure di riferimento e nello specifico le procedure “**KYC – Know Your Customers procedure**” ([Allegato N](#)) e “**KYS – Know Your Supplier procedure**” ([Allegato O](#)), che attraverso una attività di *due diligence* sui propri clienti e fornitori, completata da una richiesta documentale accurata, prima della sottoscrizione di contratti di servizi o della stipula di assicurazione del credito, cauzioni o fideiussioni, consentono a Coface SA di conoscere preventivamente le proprie controparti, limitando la possibilità di finanziamento di attività criminali.

La Procedura KYS, attraverso le richieste documentale consente, inoltre, un controllo sulla struttura compliance dei potenziali fornitori. Ad ognuno di essi viene, sulla base di specifici indici (Es. Paese dei fornitori, luogo di esecuzione del contratto, località in cui è aperto il conto corrente del fornitore indicato per i pagamenti) è attribuito un punteggio di rischio, ad ognuno dei quali corrisponde un diverso processo decisionale, basato su più o meno livelli autorizzativi.

La procedura KYC, invece, prevede che per tutti i potenziali nuovi Clienti sia effettuata un'accurata due diligence, che consenta di perimetrare l'attività da essi svolta e i soggetti (persone fisiche e/o giuridiche) con cui intrattengono rapporti commerciali.

Il Gruppo ha peraltro messo a disposizione della Compagnia la Black List fornita dall'azionista Natixis, aggiornata su base mensile e contenente le informazioni relative a soggetti coinvolti nelle indicate attività.

Tale banca dati alimenta il sistema di informazioni della Compagnia, assicurando così un sicuro filtro nella fase di individuazione dei prospect. La Compagnia effettua inoltre periodiche classificazioni della clientela, al fine di misurare il proprio rischio antiriciclaggio.

Nel caso in cui, al termine del processo di KYC, dovesse emergere che un Cliente ha come attività la vendita di articoli a “duplice uso”, Coface SA, secondo quanto previsto da specifica *policy* dettata dalla Capogruppo francese, dovrà richiedere all'Assicurato tutte le autorizzazioni necessarie per l'esportazione e commercializzazione di tali beni o servizi.

Tale procedura – “**Claims Group Rules on dual use items**” ([Allegato X](#)) – si applica limitatamente alle attività di Assicurazione del credito e di Cauzioni Sinistri e individua tutti gli adempimenti che l'Ufficio sinistri deve compiere quando le attività del Cliente rientrano nell'ambito normativo dei beni a duplice uso.

Al fine di limitare e prevenire la commissione dei reati previsti in tale sezione, è stato, inoltre, previsto che prima della convalida del pagamento del sinistro, il Responsabile di funzione, attraverso un'attività di *due diligence*, deve verificare che l'assicurato o beneficiario del pagamento del sinistro sia stato sottoposto a sanzioni o vigilanza commerciale. Sarà, inoltre,

necessario accertare che il beneficiario o i debitori non siano situati in Paesi ad altro rischio sanzione – procedura “**Sanctioned Companies and Countries under Sanctions**” ([Allegato Y](#)).

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l’implementazione e l’adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all’ [Allegato I](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l’obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell’esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all’Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

J) INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES D.LGS. 231/2001)

Il reato di “Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria”, considerando il contingente numero di dipendenti e collaboratori di cui Coface SA si avvale nella gestione e attuazione della propria attività societaria, si ritiene che sia ad elevato rischio di consumazione.

Di seguito si riporta una sintetica descrizione della fattispecie di reato ex art. 25-decies D.lgs. 231/2001.

* * *

1.1. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Art. 377 bis Cod. Pen.)

Il reato in oggetto si configura allorquando taluno, con violenza, minaccia, ovvero con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci alla persona chiamata a rendere, davanti all’autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

Facendo riferimento al procedimento penale nella sua interezza, si ritiene che tale reato possa avere ad oggetto anche le dichiarazioni da rendere nel corso delle indagini preliminari, pienamente utilizzabili dinanzi al Giudice per le indagini preliminari, in giudizio abbreviato ed in casi eccezionali in dibattimento.

2. LE ATTIVITA' A RISCHIO REATO

Le attività considerate maggiormente a rischio rispetto la possibile consumazione del reato ex art. 377 bis c.p. sono:

- La gestione del personale;
- Gestione dei rapporti con gli Agenti;
- Gestione del contenzioso in generale;
Gestione dei procedimenti penali in cui è coinvolta la Società e in cui sono richieste dichiarazioni da parte di qualunque persona interessata ai fatti.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- l'offerta di denaro o altra utilità a dipendenti o ad altri soggetti che prestano la loro attività professionale in favore di Coface SA (Es. Agenti), al fine di evitare che questi, nel corso di procedimenti penali, rendano dichiarazioni che possano arrecare un pregiudizio a Coface SA o a sua società controllate (Es. una figura apicale offre denaro ad un dipendente affinché quest'ultimo, citato come testimone o persona informata sui fatti in procedimento penale, dichiari il falso o ometta circostanze potenzialmente dannose per la Società);
- minacciare un Agente che presta la propria attività professionale in favore della Società, di un mancato rinnovo del contratto di agenzia, laddove deponga su fatti o circostanze eventualmente pregiudizievoli per Coface SA;
- minacciare un dipendente di un immediato licenziamento nel caso in cui non ometta, nel corso della sua testimonianza in un procedimento penale, circostanze o informazioni che possano arrecare un pregiudizio a Coface SA.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Considerando le peculiarità di tale reato, che può coinvolgere tutti i Dipendenti di Coface SA, è evidente come tutte le funzioni e le aree aziendali sono da considerarsi a rischio rispetto alla consumazione di tale illecito penale.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato J](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

K) REATI AMBIENTALI (ART. 25-UNDECIES D.LGS. 231/2001)

Il rischio di consumazione dei reati previsti e disciplinati dall'art. 25-*undecies* D.lgs. 231/2001, rispetto alla realtà aziendale di Coface SA, risulta di basso profilo, considerando che la Società produce, prevalentemente, rifiuti urbani, smaltibili attraverso il sistema di raccolta cittadino, mentre i rifiuti speciali sono limitati ai dispositivi informativi in disuso.

Nonostante ciò, è, comunque, indispensabile che la Società adotti Procedure e Protocolli tesi a limitare il rischio di realizzazione di tali illeciti penali.

Di seguito saranno descritti esclusivamente i "Reati ambientali" che potenzialmente potrebbero configurarsi all'interno della Compagnia, tralasciando, invece, le fattispecie che nemmeno in via del tutto ipotetica potrebbero essere consumati nell'interesse o vantaggio di Coface SA.

* * *

1.1. Inquinamento ambientale (art. 452 *bis* Cod. Pen.)

La norma punisce chiunque abusivamente cagiona una compromissione o un deterioramento significativo e misurabile:

1. delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo;
2. di un ecosistema, della biodiversità anche agraria, della flora o della fauna.

Quando l'inquinamento è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.

Tale delitto è un reato di evento consistente in una compromissione o deterioramento significativo e misurabile delle acque o dell'aria o di porzioni di estese o significative del suolo o del sottosuolo, oppure di un ecosistema, della biodiversità, anche agraria, della flora e della fauna.

Per deterioramento va intesa la riduzione della cosa in uno stato tale da diminuire in modo apprezzabile il valore o da impedirne anche parzialmente l'uso, ovvero da rendere necessaria, per il ripristino, un'attività non agevole.

Per compromissione, invece, si intende uno squilibrio funzionale che incide sui processi naturali correlati alla specificità della matrice o dell'ecosistema medesimo.

Acchè possa ritenersi configurato il reato in oggetto è, inoltre, necessario che l'evento inquinamento sia significativo e misurabile.

Il primo presupposto viene valutato in riferimento alle Concentrazioni soglie di rischio (CSR), mentre la "misurabilità" va intesa quale oggettiva possibilità di quantificazione del danno prodotto.

1.2. Disastro ambientale (art. 452 *quater* Cod. Pen.)

La norma punisce chiunque abusivamente cagiona un disastro ambientale. Costituiscono disastro ambientale alternativamente:

1. l'alterazione irreversibile dell'equilibrio di un ecosistema;
2. l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali;
3. l'offesa alla pubblica incolumità in ragione della rilevanza del fatto per l'estensione della compromissione o dei suoi effetti lesivi ovvero per il numero delle persone offese o esposte a pericolo.

Quando il disastro è prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette, la pena è aumentata.

Il reato *de quo* si configura non solo quando l'alterazione dell'equilibrio di un ecosistema sia irreversibile, ma anche quando, pur essendo possibile una bonifica, essa richiederebbe tempi così ampi da non poter esser rapportabile all'agire umano.

Tale delitto si configura, inoltre, anche quando l'alterazione possa essere rimossa solo con interventi particolarmente onerosi o provvedimenti eccezionali. Tale evento è da considerarsi quale linea di confine con il reato di inquinamento ambientale ex art. 452 bis Cod. Pen., integrato da alterazione reversibili con costi non particolarmente gravosi.

Si configura il reato di "Disastro ambientale", infine, quando l'agente ha provocato un'offesa alla pubblica incolumità. In tal caso, il danno all'ambiente viene in rilievo come evento prodromico alla successiva messa in pericolo dell'incolumità pubblica. È comunque indispensabile che il danno alla pubblica incolumità avvenga come diretta conseguenza di un'aggressione all'ambiente.

1.3. Delitti colposi contro l'ambiente (art. 452 *quinquies* Cod. Pen.)

Tale articolo prevede che laddove i reati di "Inquinamento ambientale" e di "Disastro ambientale" siano commessi per colpa, sia prevista una riduzione di pena.

Ulteriore diminuzione di pena è prevista laddove i fatti di cui agli artt. 452-bis e 452-quater, siano commessi per colpa, causando un mero pericolo di inquinamento ambientale o di disastro ambientale e non una concreta lesione.

1.4. Attività di gestione di rifiuti non autorizzata (art. 256 D.lgs. 152/2006)

La norma punisce:

- chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti (sia non pericolosi che pericolosi) in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 del D.lgs. 152/2006.
- i titolari di imprese ed i responsabili di enti che abbandonano o depositano in modo incontrollato i rifiuti ovvero li emettono nelle acque superficiali o sotterranee, in violazione del divieto di cui all'art. 192 comma II e II;
- chiunque realizzi o gestisca una discarica non autorizzata;
- chiunque realizzi o gestisca una discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi;
- chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti;
- chiunque effettui il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b).

1.5. Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 D.lgs. 152/2006)

La norma punisce chiunque:

- cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti D.lgs. 152/2006;
- omette la comunicazione di cui all'articolo 242 D.lgs. 152/2006.

Pene maggiori sono previsti laddove le condotte sopra menzionate abbiano ad oggetto sostanze pericolose.

Tale contravvenzione punisce i danni all'ecosistema derivanti dalla totale inosservanza dell'obbligo di bonifica, ripristino o messa in sicurezza imposta dal progetto approvato dall'Autorità competente ex art. 242.

Allo stesso modo viene punito chi impedisce la comunicazione all'autorità competente di un evento dannoso all'ambiente.

1.6. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 D.lgs. 152/2006)

La norma punisce gli operatori che, a titolo professionale, effettuano attività di raccolta e trasporto di rifiuti, i commercianti e gli intermediari di rifiuti, le imprese e gli enti che effettuato operazione di recupero e smaltimento di rifiuti, i Consorzi e i sistemi riconosciuti, gli istituti per il recupero e riciclaggio dei imballaggi e di particolari tipologie di rifiuti, nonché le imprese e gli enti produttori iniziali di rifiuti pericolosi e le imprese e gli enti produttori iniziali di rifiuti non pericolosi di cui all'art. 184, comma III lett. c), d) e g) che:

- non comunicano alla Camera di Commercio, Industria, Artigianato e Agricoltura, territorialmente competente, le quantità e le caratteristiche qualitative dei rifiuti oggetto delle loro attività, dei materiali prodotti all'esito delle attività di recupero nonché i dati relativi alle autorizzazioni ed alle comunicazioni inerenti alle attività di gestione; allo stesso modo sono puniti coloro che effettuano tali comunicazioni in modo incompleto o inesatto.

È punito, inoltre, chiunque omette di tenere ovvero tiene in modo incompleto il registro di carico e scarico di cui all'art. 190 comma I del Codice dell'Ambiente.

Lo stesso articolo punisce, in aggiunta, chiunque effettua il trasporto di rifiuti senza il formulario di identificazione (FIR), ovvero indica in esso dati incompleti o inesatti.

Viene punito anche chi, nella predisposizione di un certificato di analisi rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, ovvero chi fa uso di un certificato falso.

Se tali indicazioni sono formalmente incomplete o inesatte, ma i dati riportati nella comunicazione al catasto, nei registri di carico e scarico, nei formulari di identificazione dei rifiuti trasportati e nelle altre scritture contabili tenute per legge, consentono di ricostruire le informazioni dovute, sono previste sanzioni ridotte.

1.7. Traffico illecito di rifiuti (art. 259 D.lgs. 152/2006)

La norma punisce chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del Regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato Regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del Regolamento stesso.

La condotta è aggravata in caso di spedizione di rifiuti pericolosi.

Nonostante il Regolamento (CEE) n. 259/1993 sia stato abrogato dal Regolamento (CE) n. 1013/2006, il Legislatore non ha modificato il testo normativo dell'art. 259 del Codice dell'Ambiente.

Ad oggi, stando al nuovo Regolamento comunitario in materia, la locuzione "traffico illecito di rifiuti" è stata sostituita dalla nozione di "spedizione illegale di rifiuti".

Il reato de quo, stando alla nuova normativa, si configura quando i soggetti obbligati omettono di eseguire le dovute notifiche alle autorità competenti o non richiedono le relative autorizzazioni.

Tale contravvenzione, inoltre, sussiste allorché gli operatori agiscono esibendo autorizzazioni ottenute con falsa documentazione, con frode oppure con documentazione incompleta.

La spedizione illegale di rifiuti sussiste, inoltre, quando vi è una violazione degli artt. 36 (che sancisce il divieto di esportazione dei rifiuti verso paesi ai quali non si applica la decisione OCSE), 39 (che vieta le esportazioni di rifiuti verso l'Antartico), 40 (che vieta l'esportazione di rifiuti verso i paesi d'oltremare), nonché quando il trasporto di materiale di risulta avviene in violazione degli artt. 41 e 43 del Regolamento (CE) n. 1013/2006 (che vietano l'importazione nell'Unione Europea di rifiuti destinati allo smaltimento e provenienti da Paesi terzi ad eccezione dei rifiuti provenienti da paesi aderenti alla convenzione di Basilea o da paesi con i quali è in vigore un accordo o da altri territori in situazione di crisi o in caso di guerra).

1.8. Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies Cod. Pen.)

La norma punisce chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti. La condotta è aggravata se si tratta di rifiuti ad alta radioattività.

Tale norma ha come obiettivo quello di colpire le forme più gravi di gestione abusiva di rifiuti, ossia quelle caratterizzate da un'attività di tipo imprenditoriale, costituita dall'allestimento di mezzi e attività continuative e organizzate idonee a gestire ingenti quantitativi di rifiuti.

Nonostante tale norma sia stata introdotta dal Legislatore con il fine di reprimere le Ecomafie, di fatto si è resa molto efficiente nell'inibizione della criminalità d'impresa.

1.9. Sistema informatico di controllo della tracciabilità dei rifiuti

La norma punisce:

- chi nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti;

- il trasportatore che omette di accompagnare il trasporto dei rifiuti con la copia cartacea della scheda SISTRI - area movimentazione e, ove necessario sulla base della normativa vigente, con la copia del certificato analitico che identifica le caratteristiche dei rifiuti. La condotta è aggravata in caso di trasporto di rifiuti pericolosi;
- colui che, durante il trasporto, fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati;
- il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata. La condotta è aggravata nel caso di rifiuti pericolosi.

1.10. Sanzioni (art. 279 co. 5 D.lgs., 152/2006)

La norma punisce chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabilite dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del D.lgs. 152/2006, dai piani e dai programmi o dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente, che determini anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

1.11. Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3 co. 6 L. 549/1993)

La norma punisce chi viola le disposizioni che prevedono la cessazione e la riduzione dell'impiego (produzione, utilizzazione, commercializzazione, importazione ed esportazione) di sostanze nocive per lo strato di ozono.

2. LE ATTIVITA' A RISCHIO REATO

Le attività considerate maggiormente a rischio rispetto la possibile consumazione dei reati sopra descritti sono:

- gestione dei rifiuti urbani e speciali;
- attività di selezione, gestione e controllo dei fornitori di servizi di analisi, trasporto e smaltimento dei rifiuti, del gestore degli impianti di depurazione delle acque reflue, del gestore dell'impianto di riscaldamento e raffreddamento e di scarico fumi;
- gestione degli adempimenti e dichiarazioni obbligatorie per legge in materia ambientale.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- scarsa o inadeguata manutenzione degli impianti idrici o elettrici dello stabile;
- mancata o inadeguata inosservanza nei confronti dell'azienda a cui è affidato il servizio di scarico dei rifiuti;
- erronea conservazione e/o deposito dei rifiuti, senza alcuna distinzione tra le diverse tipologie;
- deposito incontrollato dei rifiuti;
- erroneo smaltimento dei rifiuti speciali prodotti dalla Società (Es. Toner stampanti, lampade/lampadine, Computer o cellulari aziendali dismessi);

- omessa verifica delle autorizzazioni necessarie alla raccolta, trasporto e smaltimento dei rifiuti da parte della società a cui è affidata la gestione dei rifiuti prodotti da Coface SA.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Le funzioni e le aree aziendali maggiormente esposte al rischio di consumazione dei reati descritti in tale sezione sono quelle strettamente connesse alla gestione dei rifiuti e, nello specifico, quelle connesse alla gestione dell'insediamento dal quale originano i reflui liquidi o gassosi o i rifiuti:

- Rappresentante della Sede Secondaria (Country Manager);
- Responsabile della gestione dei rifiuti.

La Società al fine di prevenire tale tipologia di reati dovrà avviare una politica di sensibilizzazione nei confronti dei propri Dipendenti, affinché essi si facciano parte diligente nel rispetto della normativa di settore e dell'ambiente.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

Per assicurare l'attuazione e l'osservanza delle norme e delle misure a tutela dei reati ambientali, così come previsti dall'art. 25-bis del D.Lgs. 231/2001 e dalle leggi speciali, Coface SA si avvale di un Servizio specifico coordinato da persona appositamente designata sulla base dei requisiti professionali, tecnici e formativi necessari per osservare le disposizioni legislative.

Oltre al Servizio appositamente designato è organizzata una scala di riporto gerarchico e funzionale (vedi allegato organigramma) allo scopo di verificare che l'attività espletata sia efficiente, che non vengano compiuti reati o negligenze e allo scopo di consigliare ulteriori eventuali azioni migliorative.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato K](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

L) IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE (ART. 25-DUODECIES D.LGS. 231/2001)

Rispetto a reati previsti dall'art. 25-duocesies, considerando la natura e la tipologia di attività societaria esercitata da Coface SA, si ritiene sussistente il rischio di consumazione del reato di "Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare" ex art. 22 comma 12 bis D.lgs. 286/1998.

Di seguito riportata una sua breve descrizione.

* * *

1.1. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 bis D.lgs. 286/1998)

Tale disposizione punisce il Datore di Lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dallo stesso art. 22, ovvero il cui permesso sia scaduto o del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato.

Più precisamente tale delitto rileva ai fini della Responsabilità Amministrativa derivante da reato ex D.lgs. 231/01 quando:

- i lavoratori occupati sono in numero superiore a tre;
- i lavoratori occupati sono minori in età non lavorativa;
- i lavoratori occupati sono sottoposti alle condizioni lavorative di particolare sfruttamento di cui all'art. 603 bis comma III Cod. Pen.:
 1. la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

2. la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
3. la sussistenza di violazione delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
4. la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o situazioni alloggiative degradanti.

Il reato in oggetto si applica esclusivamente alle forme di lavoro subordinato, mentre sono escluse dal suo cono d'ombra tutti i rapporti di lavoro che non implicino un vincolo subordinazione.

2. LE ATTIVITA' A RISCHIO REATO

Le attività considerate maggiormente a rischio rispetto la possibile consumazione dei reati sopra descritti sono:

- selezione e gestione del personale;
- impiego di personale interinale;
- gestione dei rapporti con fornitori che impiegano alle loro dipendenze personale proveniente da Paesi Extracomunitari.

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- l'assunzione di dipendenti senza regolare permesso di soggiorno;
- il mancato controllo dei termini di scadenza dei permessi di soggiorni di dipendenti extra-comunitari;
- affidare attività a società terze che impiegano alle loro dipendenze lavoratori irregolari e senza regolare contratto di lavoro.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Le funzioni e le aree aziendali nel cui ambito sussiste il rischio di consumazione del reato di "Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare" sono quelle direttamente coinvolte nei processi di selezione e gestione del personale, nonché nell'individuazione dei soggetti terzi a cui affidate specifiche funzioni o attività interne:

- Datore di Lavoro;
- Direzione Risorse Umane.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato L](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

A titolo esemplificativo, i Destinatari sono tenuti a trasmettere all'Organismo informazioni in merito a:

- assunzione di una risorsa sprovvista del permesso di soggiorno;
- comunicazione immediata al datore di lavoro ed all'OdV dell'eventuale omessa richiesta di rinnovo del permesso di soggiorno nei termini di legge da parte del lavoratore straniero alle sue dipendenze;
- in ogni caso, il lavoratore straniero è tenuto a comunicare immediatamente al datore di lavoro e all'OdV l'intervenuta scadenza, revoca o annullamento del permesso di soggiorno; a seguito di tale eventuale comunicazione, il datore di lavoro provvede nei termini di legge, comunicando all'OdV le attività svolte a mezzo di apposita nota informativa.

- Servizio di fornitura con società che non rispettano la normativa vigente, come meglio sopra esplicitata.

In conformità a quanto previsto nella Procedura di Whistleblowing, adottata dalla Società, i Destinatari del Modello, che nell'esercizio delle proprie attività lavorative, dovessero riscontrare violazioni delle Procedure e dei Protocolli, nonché venire a conoscenza di condotte illecite, rilevanti ai sensi e per gli effetti del Decreto Legislativo 231/2001, devono darne immediata comunicazione all'Organismo di Vigilanza.

M) REATI TRIBUTARI (ART. 25-QUINQUESDECIES D.LGS. 231/2001)

Inevitabilmente i reati previsti e disciplinati dall'art. 25-quinquesdecies D.lgs. 231/2001 (c.d. "Reati Tributari), rientrano di diritto tra gli illeciti penali a rischio consumazione rispetto alla realtà aziendale di Coface SA.

Di seguito sarà descritte ed analizzate le singole fattispecie di reato rientranti in tale categoria.

* * *

1.1 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. 74/2000)

Tale disposizione punisce chiunque, per evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi. Ai sensi del comma 2 della norma, deve trattarsi di fatture o documenti registrati nelle scritture contabili obbligatorie ovvero detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

Tale reato si consuma al momento della presentazione della dichiarazione fraudolenta.

È fondamentale sottolineare come nel "fine di evadere le imposte" vada intesa anche come il conseguimento di un indebito rimborso o il riconoscimento di un inesistente credito d'imposta.

Per operazioni inesistenti si intendono le operazioni mai avvenute o avvenute solo in parte (inesistenza oggettiva), le operazioni effettuate, ma per le quali è stato indicato in fattura un importo diverso, generalmente superiore e le operazioni effettuate ma tra soggetti diversi rispetto a quelli indicati in fattura (Es. la Società effettua realmente un acquisto, ma il reale fornitore è diverso da quello indicato in fattura).

Come chiarito dalla Giurisprudenza, inoltre, al fine della sussistenza del reato in oggetto è irrilevante se le fatture o i documenti che attestano operazioni inesistenti siano creati da terzi o dalla stessa persona che presenta la dichiarazione.

1.2. Dichiarazione fraudolenta mediante altri artifici (art. 3 D. Lgs. 74/2000)

La fattispecie si applica fuori dai casi previsti dall'art. 2 sopra citato e sanziona chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate, oggettivamente o soggettivamente, ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi o crediti e ritenute fittizie quando, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a 30.000 Euro;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a 1,5 milioni di euro, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a 30.000 Euro.

Tale delitto si differenzia dal reato ex art. 2 D.lgs. 74/2000, in quanto non richiede che vengano impiegate fatture o altri documenti analoghi relativi ad operazioni inesistenti, ma che venga posto in essere un qualsiasi atto fraudolento idoneo ad ostacolare l'accertamento o ad indurre in errore l'amministrazione finanziaria.

1.3. Dichiarazione infedele (art. 4 D. Lgs. 74/2000)

Va premesso che, come previsto dall'art. 25 quinquiesdecies comma I bis, tale reato rileva ai fini della responsabilità amministrativa della Società esclusivamente laddove sia commesso al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegue o passa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

La norma in oggetto punisce chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni. 1-bis.

Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali. 1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette.

Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b).

Condotta tipica di tale reato è l'indicazione, in dichiarazione, di elementi passivi inesistenti ovvero la mancata manifestazione di elementi attivi di reddito. Entrambe tali azioni sono idonee a falsare la rappresentazione della base di reddito su cui calcolare le aliquote fiscali e, quindi, le imposte dovute.

1.4. Omessa dichiarazione (art. 5 D. Lgs. 74/2000)

Va premesso che, come previsto dall'art. 25 quinquiesdecies comma I bis, tale reato rileva ai fini della responsabilità amministrativa della Società esclusivamente laddove sia commesso a fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegue o passa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

Tale norma punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

È punito, inoltre, chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Secondo recente Giurisprudenza non integra il reato di omessa dichiarazione la presentazione, nei termini prevista dalle leggi tributarie e nel rispetto delle soglie individuate, di una dichiarazione incompleta, dal momento che la rigorosa ed esaustiva individuazione normativa della condotta incriminata, consistente nella mancata presentazione tout court agli Uffici competenti della dichiarazione, non è suscettibile di lettura analogica, ponendosi altrimenti in contrasto con il principio di legalità.

1.5. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D. Lgs. 74/2000)

La norma sanziona chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

L'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo d'imposta si considera come un unico reato.

Riduzione di pena sono previste laddove l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a € 100.000,00.

La condotta prevista e punita dall'art.8 D.lgs. n. 74/2000 è strettamente legata al reato ex art. 2 D.lgs. 74/2000 dall'unicità del fine, in quanto il primo costituisce il mezzo normale per realizzare

il secondo. Ed invero, spesso accade che chi emette la falsa fattura, intestandola ad un determinato soggetto (il potenziale utilizzatore), si è preventivamente accordato con lo stesso, o, comunque, accolto la sua istigazione

1.6. Occultamento o distruzione di documenti contabili (art. 10 D. Lgs. 74/2000)

Tale fattispecie punisce colui che, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

Tale norma punisce esclusivamente l'occultamento o la distruzione, anche parziale, delle scritture contabili e non anche la mancata tenuta, sanzionata con mera sanzione amministrativa dall'art. 9 del d.lgs. 471/1997.

Il reato non si configura allorché il risultato economico contenuto nelle scritture contabili o in altri documenti, possa essere accertato in base ad altra documentazione conservata dall'imprenditore e senza necessità di reperire altrove elementi di prova.

Allo stesso modo, il delitto de quo non si configura se è possibile ricostruire il reddito e il volume di affari tramite la documentazione restante che venga esibita o rintracciata presso la sede del contribuente oppure presso il suo domicilio ovvero grazie alle comunicazioni fiscali che il contribuente stesso ha fatto all'Amministrazione Finanziaria (dichiarazione dei redditi, dichiarazioni IVA, bilanci depositati).

1.7. Inedita compensazione (art. 10 *quater* D. Lgs. 74/2000)

Va premesso che, come previsto dall'art. 25 quinquiesdecies comma I bis, tale reato rileva ai fini della responsabilità amministrativa della Società esclusivamente laddove sia commesso a fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegue o passa conseguire un danno complessivo pari o superiore a dieci milioni di euro.

Tale norma punisce chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.

È punito, inoltre, chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

È evidente come tale norma si componga due diverse condotte: la prima avente ad oggetto la compensazione di "crediti non spettanti", mentre la seconda avente ad oggetto la compensazione di "crediti inesistenti".

Acchè un credito possa essere definito inesistente, secondo quanto previsto dall'art. 13 comma V del D.lgs. 471/1997:

- a) Deve mancare il presupposto costitutivo del credito;
- b) L'inesistenza non deve emergere dai controlli disposti dall'Amministrazione Finanziaria ed in forza dei quali quest'ultima procede a ridurre il credito di imposta in base a quanto

previsto dalla legge, o dichiarato dal contribuente, o risultante dai documenti allo stesso richiesti.

Viceversa, laddove manchi una di tali due condizioni e vi sia stata un erroneo utilizzo della procedura di compensazione, il credito deve essere qualificato come “non spettante”.

1.8. Sottrazione fraudolenta al pagamento di imposte (art. 11 D. Lgs. 74/2000)

Tale norma sanziona la condotta di chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore a euro 50.000 Euro, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

È punito, inoltre, chiunque al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Un aumento di pena è previsto laddove l'ammontare complessivo sia superiore ad euro duecentomila.

Da quanto sopra discende che la condotta penalmente rilevante può, dunque, consistere, rispettivamente:

- a) nell'alienare simulatamente o nel compiere altri atti fraudolenti sui propri o su altrui beni (quindi un'attività di materiale sottrazione di disponibilità, comma 1, art. 11 D.lgs. n. 74/2000);
- b) nell'indicare, nella documentazione presentata ai fini della procedura di transazione fiscale, elementi attivi o passivi diversi da quelli reali (quindi un'attività di falsificazione della consistenza patrimoniale, comma 2).

In riferimento al momento della consumazione del reato, per entrambe le ipotesi si tratta di un reato a consumazione istantanea in quanto, rispettivamente:

- a) per le ipotesi di cui al 1 comma dell'art. 11 in commento, rileva in tal caso il momento in cui si aliena simulatamente o si compiono altri atti fraudolenti sui propri o su altrui beni;
- b) per le ipotesi di cui al 2 comma dell'art. 11 in commento, deve guardarsi al momento in cui si presenta la documentazione ai fini della procedura di transazione fiscale corredandola di elementi attivi/passivi diversi da quelli reali.

2. LE ATTIVITA' A RISCHIO REATO

Le attività considerate maggiormente a rischio rispetto la possibile consumazione dei reati sopra descritti sono:

- *gestione dei flussi finanziari in entrata e in uscita;*
- *contratti di acquisto e/o di vendita con controparti;*
- *gestione delle consulenze e degli incarichi professionali;*
- *gestione della documentazione contabile;*
- *gestione della fiscalità;*
- *gestione della piccola cassa;*
- *gestione del processo di bilancio.*

2.1 Possibili modalità attuative.

Rappresentato possibili modalità attuative dei reati sopra descritti:

- Inclusione in dichiarazione (previa contabilizzazione) di fatture e altri documenti relativi a operazioni inesistenti, sotto il profilo oggettivo o soggettivo, o aventi un valore superiore a quello effettivo; ad esempio, la Società potrebbe ricevere una prestazione da un soggetto diverso da quello indicato in fattura (inesistenza soggettiva) oppure emettere una fattura per un'operazione mai effettuata o per un'operazione effettuata per quantitativi o per corrispettivi inferiori rispetto a quelli indicati in fattura (inesistenza oggettiva);
- Realizzazione di operazioni simulate o utilizzo di documentazione falsa o di altri mezzi fraudolenti idonei a ostacolare l'accertamento e a indurre in errore l'Amministrazione Finanziaria;
- Occultamento o distruzione (totale o parziale) delle scritture contabili o dei documenti la cui conservazione è obbligatoria per legge.

3 FUNZIONI E AREE AZIENDALI A RISCHIO REATO

Le funzioni e le aree aziendali nel cui ambito sussiste il rischio di consumazione dei "Reati Tributari" sono:

- Rappresentante della Sede Secondaria (Country Manager);
- Direzione amministrativa e finanziaria/CFO;
- Consulenti esterni.

4 I PROTOCOLLI PER MITIGARE IL RISCHIO

4.1. Protocolli Generici

Coface SA, al fine di limitare e prevenire la consumazione dei reati presupposto, descritti in tale sezione, ostacolando, così, condotte anche solo potenzialmente illecite, come già ampiamente descritto nella Parte Generale (Paragrafo 4.2), ha implementato dei Protocolli Generici, funzionali a tali fine:

- **Codice di Condotta COFACE**, che individua i principi e le regole di condotta cui attenersi nello svolgimento delle attività sensibili;
- **Sistema di Controllo Interno**, che consente di analizzare le singole funzioni aziendali, valutando che esse sia svolte in conformità alle linee guida e policy provenienti dalla Capogruppo francese, assicurando una separazione dei ruoli ed una tracciabilità delle operazioni.

4.2. Protocolli Specifici:

Oltre ai protocolli di carattere generale, la Società, con l'implementazione e l'adozione del Modello 231 ha deciso di introdurre dei Protocolli Specifici, individuando le norme di comportamento, divieti e obblighi ai quali i Destinatari devono attenersi nello svolgimento delle proprie attività e funzioni.

Si rinvia, a tal fine, all' [Allegato M](#) del presente Modello 231.

Si ricorda che tali Protocolli potranno essere, in qualsiasi momento, oggetto di revisione e/o modifiche, le quali dovranno essere tempestivamente divulgate tra tutti i Destinatari, i quali, a loro volta, avranno l'obbligo di prenderne conoscenza e di rispettarne i termini e modalità.

5. CONTROLLI E FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

I Responsabili delle Funzioni Aziendali, nella cui competenza ricadano le Aree Sensibili sopra richiamate, o chiunque, nell'esercizio delle proprie funzioni e attività, venga a conoscenza di violazioni o tentativi di elusione dei Protocolli sopra individuati, o dei principi fondamentali dettati dal Codice di Condotta COFACE, dovrà darne immediata comunicazione all'Organismo di Vigilanza, secondo le modalità previste nella Procedura di Whistleblowing, adottata da Coface SA.

Le verifiche dell'OdV concernenti l'osservanza e l'efficacia del Modello in materia di "Reati Tributari", con riferimento all'attività ed ai rapporti che si vengono ad instaurare tra la Società ed i soggetti terzi, devono concentrarsi sul rispetto, da parte della Società, di procedure e/o prassi che garantiscano il controllo sui seguenti aspetti e l'implementazione dei seguenti presidi:

- prezzo dei beni acquistati in linea con quello di mercato;
- *due diligence* fornitori (verifiche su visura camerale, fatturato, addetti);
- coerenza tra l'attività tipica del fornitore e la prestazione oggetto di fatturazione;
- esatta individuazione del soggetto referente all'interno della struttura aziendale della controparte (e-mail, posizione, ecc.);
- corrispondenza tra le operazioni in concreto effettuate e quanto documentato nelle fatture;
- genuinità della documentazione sottesa alle operazioni poste in essere;
- tenuta e custodia delle scritture contabili e fiscali;
- individuazione delle funzioni aziendali incaricate e legittimate alla tenuta e alla movimentazione delle scritture contabili e fiscali;
- effettuazione di verifiche periodiche sulle scritture contabili;
- disciplina delle modalità di segnalazione agli organi competenti in caso di eventi accidentali che possono deteriorare le scritture.