

BANOR SIM S.P.A.

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO**

(ai sensi del Decreto legislativo 8 giugno 2001, n. 231)

PARTE GENERALE

Approvato dal Consiglio di Amministrazione

di Banor SIM S.p.A. in data 14.12.2020

INDICE

1. Definizioni e abbreviazioni	4
2. Il Decreto Legislativo 8 giugno 2001, n. 231	6
2.1 I principi generali.....	6
2.2 Il “catalogo” dei reati e degli illeciti amministrativi rilevanti ai fini del Decreto	6
2.3 Il sistema sanzionatorio previsto dal Decreto.....	14
2.4 Il Modello di Organizzazione, Gestione e Controllo come esimente della responsabilità prevista dal Decreto	15
3. Banor SIM S.p.A.	17
3.1 La Corporate Governance di Banor SIM S.p.A.....	17
3.2 Il sistema di controllo interno	19
4. Il Modello di Organizzazione, Gestione e Controllo di Banor SIM S.p.A.	22
4.1 Gli obiettivi e le finalità perseguiti con l’adozione e il conseguente aggiornamento del Modello Organizzativo di Banor SIM S.p.A.	22
4.2 I “Destinatari” del Modello Organizzativo di Banor SIM S.p.A.....	22
4.3 L’aggiornamento del Modello Organizzativo di Banor SIM S.p.A.	23
4.4 La mappa delle attività “sensibili” di Banor SIM S.p.A.	23
4.5 La struttura del Modello Organizzativo di Banor SIM S.p.A.....	24
5. L’Organismo di Vigilanza di Banor SIM S.p.A.	26
5.1 I requisiti dell’Organismo di Vigilanza di Banor SIM S.p.A.	26
5.2 Le cause di ineleggibilità, revoca, sospensione e decadenza.....	27
5.3 I compiti dell’Organismo di Vigilanza di Banor SIM S.p.A.	28
5.4 L’attività di reporting dell’Organismo di Vigilanza di Banor SIM S.p.A.	29
5.5 Obblighi di informativa nei confronti dell’Organismo di Vigilanza di Banor SIM S.p.A.	29
5.6 Whistleblowing – tutela del dipendente e/o del collaboratore che segnala illeciti – art. 6, comma 2-bis del D.Lgs. 231/2001	31
6. Formazione e informazione	33

6.1	Disposizioni generali.....	33
6.2	Comunicazione iniziale.....	33
6.3	Formazione del personale.....	34
6.4	Informativa ai “Terzi Destinatari”	34
7.	Il Sistema Sanzionatorio.....	35
7.1	Profili generali	35
7.2	Le sanzioni nei confronti dei lavoratori Dipendenti.....	35
7.3	Le sanzioni nei confronti dei componenti del Consiglio di Amministrazione e del Collegio Sindacale e dei Revisori	37
7.4	Le sanzioni nei confronti dei “Terzi Destinatari”	38

1. Definizioni e abbreviazioni

Attività sensibili: le attività aziendali nel cui ambito potrebbero potenzialmente crearsi le occasioni, le condizioni e gli strumenti per la commissione dei reati.

Autorità di vigilanza: le Autorità Pubbliche (ex. art. 2638 del codice civile) che svolgono attività di vigilanza nei confronti della Società quali, ad esempio, Banca d'Italia, Consob, il Garante per la Protezione dei Dati Personali, l'Autorità Garante per la Concorrenza e il Mercato, ecc.

CCNL: il Contratto Collettivo Nazionale di Lavoro applicabile ai dipendenti di Banor SIM S.p.A., ovvero:

- per i dipendenti con qualifica non dirigenziale, il Contratto Collettivo Nazionale di Lavoro per i quadri direttivi e per il personale delle aree professionali dipendenti dalle imprese esercenti attività del settore Commercio e Terziario;
- per i dipendenti con qualifica dirigenziale, il Contratto dei dirigenti delle aziende del Commercio e Terziario.

Codice Etico: il Codice Etico adottato dalla Società per definire i principi di condotta nella propria attività, che devono essere osservati da amministratori, dipendenti, fornitori, consulenti e collaboratori.

Collaboratori e/o Consulenti: i soggetti che intrattengono con la Società rapporti di collaborazione senza vincolo di subordinazione, che si concretizzano in una prestazione professionale non a carattere subordinato, sia continuativa sia occasionale nonché quanti, in forza di specifici mandati e procure, rappresentano la Società verso terzi.

Consiglio di Amministrazione o C.d.A.: il Consiglio di Amministrazione di Banor SIM S.p.A.

Decreto o D.lgs. 231/2001: il Decreto Legislativo 8 giugno 2001 n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", nel contenuto di tempo in tempo vigente.

Decreto Antiriciclaggio o D.lgs. 231/2007: il Decreto legislativo 21 novembre 2007, n. 231, in materia di "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminali e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione" e successive modifiche ed integrazioni.

Destinatari: i soggetti ai quali si applicano le disposizioni del presente Modello.

Dipendenti: le persone fisiche sottoposte alla direzione o alla vigilanza di soggetti che rivestono funzioni di rappresentanza, amministrazione o di direzione della Società, ossia tutti i soggetti che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società.

Fornitori: coloro che forniscono beni o servizi in favore di Banor SIM S.p.A.

Incaricato di un pubblico servizio: colui che "a qualunque titolo presta un pubblico servizio", intendendosi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza di poteri tipici di questa (art. 358 c.p.).

Linee Guida Confindustria: documento-guida di Confindustria (approvato il 7 marzo 2002 ed aggiornato successivamente nel 2004, nel 2008 e nel 2014) per la costruzione dei Modelli di Organizzazione, Gestione e Controllo di cui al Decreto.

Linee Guida Assosim: Linee Guida Assosim aggiornate per la redazione dei Modelli di Organizzazione, Gestione e Controllo di cui al Decreto, approvate dal Ministero della Giustizia il 10 settembre 2013.

Modello di Organizzazione, Gestione e Controllo (anche Modello): il presente Modello di Organizzazione, Gestione e Controllo adottato ai sensi degli artt. 6 e 7 del D.Lgs. 231/2001.

Organismo di Vigilanza (anche Organismo o OdV): l'Organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sul funzionamento, sull'osservanza del Modello, nonché di curarne l'aggiornamento.

Procedure: procedure, policy, disposizioni organizzative, ordini di servizio e tutte le altre disposizioni, provvedimenti e atti della Società che attuano i principi di controllo contenuti nel presente documento.

Pubblica Amministrazione, PA o Enti Pubblici: la Pubblica Amministrazione, inclusi i relativi funzionari e i soggetti incaricati di pubblico servizio.

Pubblico ufficiale: colui che "esercita una pubblica funzione legislativa, giudiziaria o amministrativa" (art. 357 c.p.).

Reati: sono le fattispecie di reato alle quali si applica la disciplina prevista dal D.Lgs. 231/2001, anche a seguito di sue successive modificazioni o integrazioni.

Società (anche "Banor" o "Banor SIM S.p.A.): Banor SIM S.p.A. con sede legale ed operativa in Via Dante 15, 20123, Milano.

Soggetti apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione o il controllo della Società.

Soggetti subordinati: persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al punto precedente.

Whistleblower: soggetto che segnala la realizzazione di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o di violazioni del Modello di organizzazione, gestione e controllo di cui è venuto a conoscenza nello svolgimento delle proprie funzioni.

2. Il Decreto Legislativo 8 giugno 2001, n. 231

2.1 I principi generali

Il Decreto legislativo 8 giugno 2001, n. 231 (di seguito il “Decreto” o “D.Lgs. 231/2001”) ha introdotto nel nostro ordinamento la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (di seguito “Enti”) in caso di commissione o tentata commissione di alcune tipologie di reati o di illeciti amministrativi nell’interesse o a vantaggio dell’Ente da parte di:

- soggetti 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 fisiche che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. “Apicali”);
- soggetti “Sottoposti” alla direzione o alla vigilanza delle persone di cui al punto precedente.

Si tratta di una responsabilità che, nonostante sia stata definita dal legislatore “amministrativa”, presenta alcuni caratteri della responsabilità penale perché:

- consegue alla realizzazione di reati;
- è accertata dal giudice penale (nel corso di un procedimento nel quale all’Ente si applicano, ove compatibili, le disposizioni processuali relative all’imputato).

Il Decreto ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l’Italia aveva già da tempo aderito.

La responsabilità dell’Ente, ai sensi del Decreto, si aggiunge e non si sostituisce a quella (penale) dell’autore del reato: tanto la persona fisica quanto quella giuridica saranno, pertanto, sottoposti a giudizio penale.

2.2 Il “catalogo” dei reati e degli illeciti amministrativi rilevanti ai fini del Decreto

La responsabilità dell’Ente sussiste solamente per quei reati (consumati o tentati) espressamente previsti dal legislatore.

In particolare, si tratta dei seguenti reati e illeciti amministrativi:

Reati contro la Pubblica Amministrazione e il suo patrimonio (artt. 24 e 25 del Decreto)

- Malversazione a danno dello Stato (art. 316-*bis* c.p.);
- Indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.);
- Frode nelle pubbliche forniture (art. 356 c.p.);
- Truffa in danno dello Stato o di un altro Ente pubblico o delle Comunità Europee (art. 640, comma 2, n. 1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.); Frode informatica in danno dello Stato o di altro Ente pubblico (art. 640-*ter* c.p.);
- Frode ai danni del fondo europeo agricolo (art. 2 Legge 898/1986);
- Peculato (art. 314 c.p.);

- Peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- Concussione (art. 317 c.p.);
- Corruzione per l'esercizio della funzione (artt. 318 c.p.);
- Corruzione per un atto contrario ai doveri di ufficio (artt. 319 c.p.);
- Circostanze aggravanti (art. 319-*bis* c.p.);
- Corruzione in atti giudiziari (art. 319-*ter* c.p.);
- Induzione indebita a dare o promettere utilità (art. 319-*quater* c.p.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);
- Pene per il corruttore (art. 321 c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità Europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri (art. 322-*bis* c.p.);
- Abuso d'ufficio (art. 323 c.p.);
- Traffico di influenze illecite (art. 346-*bis* c.p.).

Delitti informatici e trattamento illecito di dati (art. 24-*bis* del Decreto)

- Documenti informatici (art. 491-*bis* c.p.);
- Accesso abusivo ad un sistema informatico o telematico (615-*ter* c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615-*quater* c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615-*quinquies* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.);
- Frode informatica del certificatore di firma elettronica (art. 640-*quinquies* c.p.);
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 105/2019).

Delitti di criminalità organizzata (art. 24-*ter* del Decreto)

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso anche straniera (art. 416-*bis* c.p.);
- Scambio elettorale politico-mafioso (art. 416-*ter* c.p.);
- Sequestro di persona a scopo di estorsione (art. 630 c.p.);

- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309);
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall'art. 416-*bis* c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91);
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, comma 2, lettera a), numero 5], c.p.p.).

Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis del Decreto)

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.);
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Delitti contro l'industria e il commercio (art. 25-bis.1 del Decreto)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

Reati societari (art. 25-*ter* del Decreto)

- False comunicazioni sociali (art. 2621 c.c.);
- Fatti di lieve entità (art. 2621-*bis* c.c.);
- False comunicazioni sociali delle società quotate (art. 2622 c.c.);
- Impedito controllo (art. 2625, comma 2, c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629-*bis* c.c.);
- Formazione fittizia del capitale sociale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Corruzione fra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635-*bis* c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.).

Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* del Decreto)

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis* c.p.);
- Assistenza agli associati (art. 270-*ter* c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-*quater* c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies* c.p.);
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270-*quinquies*.2 c.p.);
- Condotte con finalità di terrorismo (art. 270-*sexies* c.p.);
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280-*bis* c.p.);
- Atti di terrorismo nucleare (art. 280-*ter* c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-*bis* c.p.);
- Istigazione a commettere alcuno dei delitti previsti dai Capi primo e secondo (art. 302 c.p.);
- Cospirazione politica mediante accordo (art. 304 c.p.);
- Cospirazione politica mediante associazione (art. 305 c.p.);
- Banda armata: formazione e partecipazione (art. 306 c.p.);
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.);
- Finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270 *quinquies* 1 c.p.);
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1);
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2);
- Sanzioni (L. n. 422/1989, art. 3);
- Pentimento operoso (D.Lgs. N. 625/1979, art. 5);

- Convenzione di New York del 9 dicembre 1999 (art. 2).

Reato di pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1 del Decreto)

- Pratiche di mutilazione degli organi genitali femminili (art. 583-*bis* c.p.).

Delitti contro la personalità individuale (art. 25-*quinqües* del Decreto)

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600-*bis* c.p.);
- Pornografia minorile (art. 600-*ter* c.p.);
- Detenzione di materiale pornografico (art. 600-*quater* c.p.);
- Pornografia virtuale (art. 600-*quater* 1 c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinqües* c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.);
- Adescamento di minorenni (art. 609-*undecies* c.p.).

Reati di abuso di mercato

Reati (art. 25-*sexies* del Decreto):

- Abuso di informazioni privilegiate (art. 184, D.Lgs. 58/1998 - TUF);
- Manipolazione del mercato (art. 185, D.Lgs. 58/1998 - TUF).

Illeciti Amministrativi (art. 187-*quinqües* TUF):

- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14, Regolamento UE n. 596/2014);
- Divieto di manipolazione del mercato (art. 15, Regolamento UE n. 596/2014).

Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 25-*septies* del Decreto)

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590 c.p.).

Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies* del Decreto)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-*bis* c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);
- Autoriciclaggio (art. 648-*ter*.1 c.p.).

Delitti in materia di violazioni del diritto d'autore (art. 25-*novies* del Decreto)

- Protezione penale dei diritti di utilizzazione economica e morale (art. 171, comma 1, lett. a)-*bis* e comma 3, L. 633/1941);
- Tutela penale del *software* e delle banche dati (art. 171-*bis*, comma 1 e comma 2, L. 633/1941);
- Tutela penale delle opere audiovisive (art. 171-*ter*, L. 633/1941);
- Responsabilità penale relativa ai supporti (art. 171-*septies*, L. 633/1941);
- Responsabilità penale relativa a trasmissioni audiovisive ad accesso condizionato (art. 171-*octies*, L. 633/1941).

Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies* del Decreto)

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

Reati ambientali (art. 25-*undecies* del Decreto)

Si tratta di reati previsti dal codice penale e da leggi speciali.

- Inquinamento ambientale (art. 452-*bis* c.p.);
- Disastro ambientale (art. 452-*quater* c.p.);
- Delitti colposi contro l'ambiente (art. 452-*quinquies* c.p.);
- Traffico ed abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.);
- Circostanze aggravanti (art. 452-*octies* c.p.);
- Uccisione, distruzione, cattura, prelievo detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-*bis* c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-*bis* c.p.).
- Importazione, esportazione, detenzione utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n. 150/1992, art. 1, art. 2, art.3-*bis* e art. 6);
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs. 152/2006, art. 137);
- Attività di gestione di rifiuti non autorizzata (D.Lgs. 152/2006, art. 256);
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257, D. Lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, D. Lgs. 152/2006);
- Traffico illecito di rifiuti (D.Lgs. 152/2006, art. 259);
- Attività organizzate per il traffico illecito di rifiuti (art. 452-*quaterdecies* c.p.);
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D.Lgs. 152/2006, art. 260-*bis*);
- Sanzioni (D.Lgs. n. 152/2006, art. 279);

- Inquinamento doloso provocato da navi (D.Lgs. N. 202/2007, art. 8);
- Inquinamento colposo provocato da navi (D.Lgs. N. 202/2007, art. 9);
- Cessazione e riduzione dell'impiego delle sostanze lesive (L. n. 549/1993, art. 3).

Delitto di impiego di cittadini di stati terzi il cui soggiorno è irregolare (art. 25-duodecies del Decreto)

- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-bis, 3-ter e comma 5, D.Lgs. n. 286/1998);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. n. 286/1998).

Reati di razzismo e xenofobia (art. 25-terdecies del Decreto)

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 604 bis c.p.).

Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies del Decreto)

- Frodi in competizioni sportive (art. 1, L. n. 40/1989);
- Esercizio abusivo di attività di giuoco o di scommessa (art. 4, L. n. 401/1989).

Reati tributari (art. 25-quinquiesdecies del Decreto)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n.74/2000);
- dichiarazione infedele (art. 4 D.Lgs. n.74/2000)¹;
- omessa dichiarazione (art. 5 D.Lgs. n.74/2000)²;
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);

¹ Il delitto di dichiarazione infedele, punito dall'art. 4 del D.Lgs. 74/2000 e introdotto tra i reati presupposto di cui all'art. 25-quinquiesdecies del D.Lgs. 231/2001 dal D.Lgs. 14 luglio 2020 n. 75, recante "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" (c.d. "Direttiva PIF"), può comportare la responsabilità amministrativa dell'Ente se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di Euro.

² Il delitto di omessa dichiarazione, punito dall'art. 5 del D.Lgs. 74/2000 e introdotto tra i reati presupposto di cui all'art. 25-quinquiesdecies del D.Lgs. 231/2001 dal D.Lgs. 14 luglio 2020 n. 75, recante "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" (c.d. "Direttiva PIF"), può comportare la responsabilità amministrativa dell'Ente se commesso nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di Euro.

- Indebita compensazione (art. 10 – *quater* D.Lgs. n. 74/2000)³;
- sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

Delitti di contrabbando (art. 25-*sexiesdecies* del Decreto), previsti dal titolo VII “Violazioni doganali” del Decreto del Presidente della Repubblica 23 gennaio 1973, n. 43.

Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato [Costituiscono presupposto per gli enti che operano nell’ambito della filiera degli oli vergini di oliva] (art. 12, L. n. 9/2013)

- Impiego, adulterazione e contraffazione di sostanze alimentari (art. 440 c.p.);
- Commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.);
- Commercio di sostanze alimentari nocive (art. 444 c.p.);
- Contraffazione, alterazione o uso di segni distintivi di opere dell’ingegno o di prodotti industriali (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.);
- Frode nell’esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Contraffazione di indicazioni geografiche denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

Reati transnazionali (art. 10 – L. 146/2006)

Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso, anche straniera (art. 416-*bis* c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* del Testo Unico di cui al D.P.R. 23 gennaio 1973, n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al D.P.R. 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-*bis*, 3-*ter* e 5, del Testo Unico di cui al D.Lgs. 286/1998);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (art. 377-*bis* c.p.);
- Favoreggiamento personale (art. 378 c.p.).

³ Il delitto di indebita compensazione, punito dall’art. 10-*quater* del D.Lgs. 74/2000 e introdotto tra i reati presupposto di cui all’art. 25-*quinqüesdecies* del D.Lgs. 231/2001 dal D.Lgs. 14 luglio 2020 n. 75, recante “Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell’Unione mediante il diritto penale” (c.d. “Direttiva PIF”), può comportare la responsabilità amministrativa dell’Ente se commesso nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di Euro.

I reati e gli illeciti amministrativi sopra richiamati possono comportare anche la responsabilità amministrativa dell'Ente che, pur avendo sede principale nel territorio italiano, sono stati commessi all'estero.

2.3 Il sistema sanzionatorio previsto dal Decreto

Le sanzioni previste dal Decreto a carico degli Enti sono: i) sanzioni pecuniarie, ii) sanzioni interdittive, iii) confisca del prezzo o del profitto del reato, iv) pubblicazione della sentenza di condanna.

Le **sanzioni pecuniarie** si applicano ogniqualvolta venga accertata la responsabilità della persona giuridica e sono determinate dal giudice penale attraverso un sistema basato su "quote". Nella commisurazione della sanzione pecuniaria il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti; l'importo della quota è fissato, invece, sulla base delle condizioni economiche e patrimoniali dell'ente.

Le **sanzioni interdittive** possono essere applicate in aggiunta alle sanzioni pecuniarie, ma soltanto se espressamente previste per il reato per cui si procede e solo nel caso in cui ricorra almeno una delle seguenti condizioni:

- l'Ente ha tratto dal reato un profitto rilevante e il reato è stato commesso da un soggetto apicale o da un soggetto subordinato, ma solo qualora la commissione del reato sia stata resa possibile da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Si traducono nell'interdizione dall'esercizio dell'attività aziendale; nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell'illecito; nel divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio); nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli concessi; nel divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l'Ente, prima della dichiarazione di apertura del dibattimento di primo grado, abbia:

- risarcito il danno o lo abbia riparato;
- eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
- messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del reato;
- eliminato le carenze organizzative che hanno determinato il reato, adottando modelli organizzativi idonei a prevenire la commissione di nuovi reati.

La **confisca** consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di danaro, beni o altre utilità di valore equivalente al prezzo o al profitto del Reato: non investe, tuttavia, quella parte del prezzo o del profitto del Reato che può restituirsi al danneggiato. La confisca è sempre disposta con la sentenza di condanna.

La **pubblicazione della sentenza** può essere inflitta quando all'Ente è applicata una sanzione interdittiva. È effettuata mediante affissione nel comune ove l'Ente ha la sede principale nonché mediante la pubblicazione sul sito *internet* del Ministero della Giustizia.

2.4 Il Modello di Organizzazione, Gestione e Controllo come esimente della responsabilità prevista dal Decreto

Se il reato è commesso da soggetti 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 soggetti che esercitano, anche di fatto, la gestione e il controllo dello stesso, l'Ente non risponde se prova che:

- **l'organo dirigente ha adottato e efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;**
- il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento è stato affidato a un Organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo;
- i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo in ordine al Modello.

Nel caso in cui, invece, il reato sia commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, la persona giuridica è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'Ente, prima della commissione del reato, abbia adottato e efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto, dunque, prevede che la società non sia passibile di sanzione se provi di aver adottato e efficacemente attuato **Modelli di organizzazione, gestione e controllo idonei a prevenire la commissione dei reati verificatisi**, ferma restando la responsabilità personale di chi ha commesso il fatto.

Il legislatore, pertanto, ha attribuito un valore esimente ai modelli di organizzazione, gestione e controllo della società nel caso in cui siano idonei alla prevenzione del rischio, nonché adottati e efficacemente attuati. Nel decreto si specificano altresì le esigenze cui devono rispondere i modelli.

Segnatamente:

- individuare le attività nel cui ambito possano essere commessi i reati previsti dal Decreto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
- introdurre un sistema idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;

- prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

3. Banor SIM S.p.A.

Banor SIM S.p.A. è una delle principali società di intermediazione mobiliare, iscritta all'Albo delle SIM con delibera Consob n. 11761 del 22/12/1998.

La Società è autorizzata alla prestazione dei seguenti servizi di investimento:

- negoziazione per conto proprio;
- esecuzione di ordini per conto dei clienti;
- collocamento senza impegno irrevocabile nei confronti dell'emittente;
- gestione di portafogli;
- ricezione e trasmissione di ordini;
- consulenza in materia di investimenti;
- assunzione a fermo e/o collocamento sulla base di un impegno irrevocabile nei confronti dell'emittente.

La SIM svolge inoltre i servizi accessori di consulenza generica (c.d. "Family Office"), avente ad oggetto assistenza per tipologie generali di *asset allocation* e non specifici strumenti finanziari, e di consulenza alle imprese in materia di struttura finanziaria, di strategia industriale e di questioni connesse, nonché la consulenza ed i servizi concernenti le concentrazioni e l'acquisto di imprese (c.d. "Corporate Finance"); entrambe le attività non sono soggette a riserva legale.

Banor è presente sul mercato dal 1989 come veicolo per le attività di *private banking* di un gruppo di banche del nord Italia e viene rilevata nel 2000 da un gruppo di investitori privati e manager, con l'obiettivo di creare un polo indipendente del *private banking* in Italia che attuasse i principi del *value investing*.

La SIM ed i suoi partner partecipano al capitale di Banor Capital Ltd, società di gestione di diritto inglese e Investment Manager della Banor Sicav e della Aristeia Sicav, Società di Investimento multicomparto a Capitale Variabile di diritto lussemburghese.

Banor SIM, inoltre, è advisor di Banor Capital per la gestione dei comparti Banor Sicav e Aristeia Sicav.

3.1 La Corporate Governance di Banor SIM S.p.A.

La Società ha una struttura organizzativa verticistica di tipo tradizionale.

Il **Consiglio di Amministrazione** è l'organo di supervisione strategica ai sensi della normativa tempo per tempo vigente, ed è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società ed ha la facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il conseguimento degli scopi sociali, esclusi soltanto quelli che la legge o lo statuto riservano in modo tassativo all'Assemblea.

Il **Collegio Sindacale** ha il compito di vigilare sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e sull'adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del sistema amministrativo contabile.

La **Società di Revisione** ha l'incarico di revisione e controllo contabile dei conti della Società.

Il **Comitato endoconsiliare per le remunerazioni e le operazioni con parti correlate (in breve, “Comitato Remunerazioni”)** supporta il Consiglio di Amministrazione, con funzioni consultive ed istruttorie in materia di remunerazioni e operazioni con parti correlate. Tale Comitato è nominato dal Consiglio di amministrazione, che sceglie i suoi componenti tra gli amministratori non esecutivi e indipendenti, incluso il Presidente del Consiglio di amministrazione. Il Consiglio di Amministrazione può nominare il Presidente del Comitato al quale spetta convocare il Comitato ogni qualvolta si renda opportuno o necessario.

Il **Comitato di Direzione** ha come obiettivo quello di favorire la circolarità delle informazioni aziendali riguardanti lo stato dell’assetto organizzativo e lo sviluppo del business, consentendo un controllo diffuso dell’efficacia e della complessiva adeguatezza delle soluzioni adottate. Esso è costituito dall’Amministratore delegato, dal Direttore generale, dal Direttore degli investimenti, dal Direttore commerciale e dal Direttore amministrativo.

Tale Comitato viene convocato dall’Amministratore delegato con cadenza almeno bimestrale e riferisce periodicamente al Consiglio di amministrazione per tramite dell’Amministratore delegato.

Il Comitato si riunisce, ferma la presenza dell’Amministratore delegato e del Direttore generale, con la partecipazione di almeno uno degli altri membri, in funzione degli argomenti trattati.

Il **Comitato investimenti** riporta all’Amministratore Delegato ed è responsabile di:

- analizzare lo scenario economico-finanziario e l’andamento delle attività e dei mercati finanziari e, in funzione di una valutazione ciclica, definisce l’asset allocation ottimale dei portafogli;
- analizzare le performance delle linee di gestione e dei relativi benchmark e svolgere attività di monitoraggio sull’andamento del profilo di rischio/ rendimento dei portafogli gestiti;
- analizzare l’andamento complessivo della massa gestita e di quella “under consultancy”.

Il **Comitato controlli**, i cui membri permanenti sono stati individuati nei Responsabili delle funzioni di controllo (Internal audit, Compliance, Antiriciclaggio, Risk management) e nel Direttore amministrativo, si occupa di:

- coordinare le funzioni di Controllo nelle loro attività di verifica e monitoraggio dei rischi soggiacenti la prestazione dei servizi di investimento;
- condividere gli esiti delle verifiche svolte e riportate dalle singole funzioni aziendali di Controllo;
- organizzare, sulla base dei fatti aziendali, la pianificazione delle attività di verifica e follow up e individuare gli eventuali ambiti in cui risultano non implementate (o parzialmente implementate) le attività correttive e che pertanto devono trovare oggetto di particolari segnalazioni all’Alta Direzione, al Consiglio di amministrazione e al Collegio Sindacale (“escalation”);
- supportare il Consiglio di amministrazione nell’attività di identificazione dei soggetti rilevanti ai fini della definizione e aggiornamento della policy in materia di incentivazione e remunerazione, con particolare riferimento all’identificazione dei risk takers e dei relativi parametri di misurazione dei rischi in funzione degli incentivi.

3.2 Il sistema di controllo interno

Nella costruzione del Modello di Banor SIM S.p.A. si è tenuto conto degli strumenti di governo dell'organizzazione della Società che ne garantiscono il funzionamento, e segnatamente di:

- **Statuto:** che contempla diverse previsioni relative al governo societario volte ad assicurare il corretto svolgimento dell'attività di gestione;
- **Sistema organizzativo:** composto dalle strutture/posizioni organizzative ed aree di responsabilità, rappresentato nell'Organigramma e che costituisce parte integrante del presente Modello;
- **Codice Etico:** costituito da un insieme di regole di comportamento e principi di carattere generale che tutti i soggetti interni ed esterni, che hanno direttamente o indirettamente una relazione con Banor SIM S.p.A., devono rispettare e la cui violazione comporta l'applicazione delle misure sanzionatorie previste dal sistema sanzionatorio del presente Modello;
- **Sistema procedurale:** composto da *policy* e procedure volte a regolamentare i processi rilevanti ed a fornire modalità operative e presidi di controllo per lo svolgimento delle attività aziendali. La Società osserva, altresì, la normativa di riferimento anche di settore.

Il Sistema di controllo interno della SIM è così strutturato:

- **controlli di "linea" (o di primo livello)** eseguiti al fine di accertare il regolare svolgimento delle quotidiane attività operative. I controlli di "linea", come noto e come previsto dalla normativa, sono effettuati dalle unità operative e consistono nelle verifiche di *routine* svolte sia da chi mette in atto una determinata attività, sia da chi ne ha la responsabilità di supervisione nell'ambito della stessa unità organizzativa o funzione;
- **controlli di secondo livello**, che coprono le diverse tipologie di rischio a cui è o può essere esposta la SIM nello svolgimento delle proprie attività (es.: operativi, di conformità alle norme, legali, di reputazione). Tali controlli sono affidati alle seguenti funzioni:
 - la **Funzione di Risk Management**, che riporta al Direttore Generale e:
 - collabora alla definizione del sistema di gestione del rischio dell'impresa;
 - presiede al funzionamento del sistema di gestione del rischio dell'impresa e ne verifica il rispetto da parte dell'intermediario e dei soggetti rilevanti;
 - verifica l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel sistema di gestione del rischio dell'impresa;
 - identifica le tipologie di rischio cui è esposta la Società, avuto riguardo alle caratteristiche operative e organizzative della Società e ai mercati di riferimento della stessa;
 - determina, per ciascuna tipologia di rischio individuata, la modalità di misurazione più appropriata, coerentemente con la rilevanza del rischio in oggetto e con gli strumenti a disposizione della Società;
 - coordina le altre funzioni aziendali ai fini della corretta attuazione dei processi ICAAP e ILAAP.
 - la **Funzione di Conformità alle norme (Compliance)**, che riporta al Direttore Generale e a cui spetta il compito di:
 - svolgere attività di supporto consultivo alle strutture organizzative della Società, con

- riferimento alle problematiche concernenti lo svolgimento dei servizi, alle procedure interne, alle informazioni e comunicazioni diffuse alla clientela e a terzi, nonché ai conflitti di interessi e ai conseguenti comportamenti da tenere;
- predisporre note informative o circolari sulla normativa rilevante e più in generale sulle evoluzioni legislative, regolamentari e giurisprudenziali concernenti lo svolgimento dei servizi e prestare assistenza continuativa sia telefonica sia via e-mail sulle tematiche specifiche e di routine relative all'attività aziendale che vengano di volta in volta sottoposte alla funzione;
trattare i reclami presentati da clienti o potenziali clienti dalla loro ricezione alla loro composizione, avvalendosi del supporto consultivo degli esponenti aziendali; registrare e conservare in un apposito registro gli elementi essenziali di ogni reclamo pervenuto e delle misure poste in essere per risolvere il problema sollevato.
 - la **Funzione Antiriciclaggio**, che riporta al CdA ed è specificamente deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo. La funzione verifica nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione di norme di etero-regolamentazione (leggi e norme regolamentari) e di autoregolamentazione in materia di riciclaggio e di finanziamento del terrorismo. A tal fine il responsabile della funzione può avvalersi, nell'espletamento dei diversi compiti in cui si articola l'attività, delle strutture organizzative presenti in Società, mantenendo in tal caso un ruolo di coordinamento e supervisione.
 - **controlli di terzo livello**, affidati alla Funzione di Revisione Interna della Società (Internal Audit).
L'Internal Audit riporta al Consiglio di Amministrazione e svolge i seguenti compiti:
 - verifica l'efficacia sia delle modalità operative di prestazione dei servizi sia dei presidi di controllo predisposti dalla Società, nonché la loro adeguatezza rispetto alle disposizioni di legge, ai provvedimenti delle Autorità di vigilanza e alle eventuali norme di autoregolamentazione di cui la Società si sia dotata o si voglia dotare, nonché a qualsiasi altra norma applicabile alle Società;
 - adotta un piano di audit per l'esame e la valutazione dell'adeguatezza e dell'efficacia dei sistemi, dei processi, delle procedure e dei meccanismi di controllo della Società;
 - verifica la idoneità delle procedure interne ad assicurare il rispetto delle disposizioni di cui al Testo Unico della Finanza e ai relativi regolamenti di attuazione tempo per tempo vigenti; inoltre, prevede indagini specifiche sull'adeguatezza di eventuali modifiche al manuale delle procedure, alla struttura organizzativa e al disegno dei controlli, che la Società intenderà effettuare nel tempo; accerta, mediante indagini periodiche e campionarie, che il complesso delle procedure e dei controlli funzioni in maniera efficace rispetto agli obiettivi preposti; verifica annualmente l'attività posta in essere dalle funzioni di Gestione del rischio e Controllo di conformità;
 - formula raccomandazioni basate sui risultati delle verifiche effettuate e ne verifica l'osservanza;
 - svolge attività di revisione in ordine al processo interno di valutazione del capitale regolamentare e della connessa pianificazione patrimoniale, adottato dalla Società, identificando le aree di miglioramento, sia sotto un profilo metodologico sia sul piano

organizzativo, e individuando specificamente le eventuali carenze del processo, le azioni correttive da porre in essere e la pianificazione temporale delle medesime.

Le funzioni di Compliance e di Internal audit si avvalgono di uno strumento operativo – il *Tableau de Bord* – per tracciare sinteticamente, in relazione a ciascuna attività di verifica svolta, la conseguente attività di follow-up e le relative risultanze (in particolare le criticità riscontrate, le azioni di correzione/mitigazione individuate e le relative tempistiche di implementazione; il rischio residuo).

4. Il Modello di Organizzazione, Gestione e Controllo di Banor SIM S.p.A.

Il Consiglio di Amministrazione di Banor SIM S.p.A. ha approvato la prima versione del proprio Modello di Organizzazione, Gestione e Controllo in data 25/06/2012. Tale documento è stato oggetto di successive modifiche con delibere del 19/12/2012, 31/01/2014, 25/03/2014, 16/11/2015 e 31/03/2016.

Nel corso del 2019, alla luce delle novità normative e di alcune modifiche organizzative nel frattempo intervenute, la SIM ha avviato un progetto di integrale revisione del documento in parola, che è stato approvato dal Consiglio di Amministrazione della stessa in data 17/12/2019.

Le modifiche e le integrazioni al presente Modello Organizzativo sono apportate dal Consiglio di Amministrazione, anche su informativa dell'Organismo di Vigilanza che ne cura l'aggiornamento.

Il Consiglio di Amministrazione della Società prende decisioni relativamente all'attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per l'implementazione degli elementi costitutivi dello stesso.

4.1 Gli obiettivi e le finalità perseguiti con l'adozione e il conseguente aggiornamento del Modello Organizzativo di Banor SIM S.p.A.

Con l'adozione del Modello di Organizzazione, Gestione e Controllo e il successivo aggiornamento la Società si propone di:

- rendere consapevoli tutti coloro che lavorano in nome e per conto della Società, con particolare riferimento a coloro che operano nelle c.d. "aree sensibili", di poter incorrere, in caso di violazioni delle disposizioni riportate nel Modello, nella commissione di illeciti passibili di sanzioni penali nei loro stessi confronti e di sanzioni "amministrative" irrogabili alla Società;
- rendere consapevoli tali soggetti che i comportamenti illeciti sono condannati con forza dalla Società, in quanto gli stessi sono sempre e comunque contrari alle disposizioni di legge, alla cultura aziendale e ai principi etici assunti come proprie linee guida nell'attività d'impresa;
- consentire alla Società di intervenire tempestivamente per prevenire o contrastare la commissione di reati o quanto meno di ridurre sensibilmente il danno dagli stessi arrecato;
- migliorare la *governance* societaria e l'immagine della Società.

La predisposizione del presente Modello è ispirata alle Linee Guida emanate da **Confindustria** e da **Assosim** così come nel tempo aggiornate.

4.2 I "Destinatari" del Modello Organizzativo di Banor SIM S.p.A.

I principi e le disposizioni del presente documento devono essere rispettati da:

- Componenti del Consiglio di Amministrazione, Sindaci e Revisori;
- Dipendenti;

- Consulenti, collaboratori, fornitori ed eventuali *partner commerciali*, agenti e promotori finanziari nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati presupposto di cui al Decreto;
- quanti agiscono sotto la direzione o la vigilanza dei vertici aziendali nell'ambito dei compiti e delle funzioni assegnate.

I soggetti così individuati sono di seguito definiti "Destinatari".

4.3 L'aggiornamento del Modello Organizzativo di Banor SIM S.p.A.

L'attività di lavoro finalizzata all'aggiornamento del Modello si è concretizzata:

- nell'identificazione di settori/attività/aree sensibili, con riferimento ai reati richiamati dal Decreto attraverso l'analisi dei più rilevanti documenti aziendali (a titolo esemplificativo: statuto, visura camerale, ecc.);
- nell'esame analitico delle aree sensibili, con prefigurazione delle modalità e degli strumenti attraverso i quali sarebbe possibile commettere i reati elencati nel Decreto da parte dell'impresa, dai suoi organi amministrativi, dai dipendenti e, in generale, dalle figure contemplate dall'art. 5 del Decreto (anche attraverso incontri e colloqui con i soggetti interessati);
- nell'individuazione delle regole interne e dei protocolli esistenti – siano essi formalizzati o meno – in riferimento alle sole aree individuate come a rischio di reato;
- nella definizione di *standard* di comportamento e di controllo ovvero per le attività che, concordemente con la Società, si è ritenuto opportuno regolamentare;
- nella disciplina delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- nell'individuazione del/i soggetto/i incaricato/i di vigilare sulla concreta applicazione del presente Modello (di seguito "Organismo di Vigilanza" o OdV) con contestuale predisposizione del sistema di *reporting* da e verso l'Organismo di Vigilanza stesso;
- nella previsione di un sistema idoneo a sanzionare sia il mancato rispetto delle misure indicate nel Modello, sia le violazioni del Codice Etico.

4.4 La mappa delle attività "sensibili" di Banor SIM S.p.A.

In conformità a quanto previsto dal Decreto e con le modalità delineate precedentemente, sono state individuate le attività "sensibili" della Società, tenendo conto dell'attuale operatività di Banor SIM S.p.A. e della struttura organizzativa esistente.

Le principali attività e i processi aziendali che possono costituire occasione o modalità di realizzazione delle fattispecie di reato di cui al Decreto sono:

- *Gestione dei rapporti con la clientela;*
- *Gestione dei servizi di investimento;*
- *Gestione dei servizi di Family Office;*

- *Gestione dei servizi di Corporate Finance;*
- *Gestione dei rapporti con soggetti pubblici e Autorità di Vigilanza;*
- *Gestione degli adempimenti amministrativi e relative attività ispettive;*
- *Gestione dei reclami, contenziosi e dei rapporti con l’Autorità Giudiziaria;*
- *Gestione degli acquisti di beni e servizi (incluse le consulenze);*
- *Selezione del personale e sistema incentivante;*
- *Gestione delle note spese;*
- *Gestione dei flussi finanziari;*
- *Predisposizione del bilancio e gestione della fiscalità;*
- *Gestione delle attività assembleari, operazioni sul capitale ed altre operazioni non routinarie;*
- *Gestione dei rapporti con il collegio Sindacale e la Società di Revisione;*
- *Gestione della sicurezza informatica;*
- *Gestione del sistema di prevenzione e protezione;*
- *Gestione delle attività ad impatto ambientale;*
- *Gestione degli omaggi, sponsorizzazioni e liberalità.*

4.5 La struttura del Modello Organizzativo di Banor SIM S.p.A.

Il Modello si compone di una Parte Generale e delle seguenti Parti Speciali finalizzate al presidio delle attività a rischio precedentemente individuate:

- **Parte Speciale A:** Reati contro la Pubblica Amministrazione e il suo Patrimonio, reati di corruzione fra privati ed istigazione alla corruzione tra privati e reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria;
- **Parte Speciale B:** Delitti informatici e trattamento illecito di dati e reati in materia di violazione del diritto d’autore;
- **Parte Speciale C:** Delitti di criminalità organizzata;
- **Parte speciale D** Delitti contro l’industria ed il commercio e delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- **Parte Speciale E:** Reati societari;
- **Parte Speciale F:** Delitti contro la personalità individuale e reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare.
- **Parte Speciale G:** Abusi di mercato;
- **Parte Speciale H:** Delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro;
- **Parte Speciale I:** Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio e delitti con finalità di terrorismo o di eversione dell’ordine democratico;
- **Parte Speciale J:** Reati ambientali;
- **Parte Speciale K:** Reati tributari.

Sulla base delle analisi effettuate, non sembra sussistano profili di rischio rispetto alle "famiglie" di reato di seguito indicate:

- reati transnazionali (art. 10 L. 146/2006);
- pratiche di mutilazione degli organi genitali femminili (art. 25 *quater 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*);
- delitti di contrabbando (art. 25- *sexiesdecies* D.Lgs. 231/2001)

Nondimeno, tali illeciti si reputano complessivamente presidiati dalle disposizioni di cui al presente Modello di Organizzazione, Gestione e Controllo e dai presidi generali di cui al Codice Etico

5. L'Organismo di Vigilanza di Banor SIM S.p.A.

La Società ha attribuito il compito di vigilare sul funzionamento e sull'osservanza dello stesso all'**Organismo di Vigilanza** (anche "OdV"), dotato dei requisiti di seguito indicati e volto ad assicurare un'effettiva e efficace attuazione del Modello.

5.1 I requisiti dell'Organismo di Vigilanza di Banor SIM S.p.A.

I componenti dell'Organismo di Vigilanza devono essere dotati dei requisiti dettati dalle Linee Guida Confindustria. In particolare:

AUTONOMIA E INDIPENDENZA: l'Organismo deve restare estraneo ad ogni forma di interferenza e pressione da parte dei vertici operativi e non essere in alcun modo coinvolto nell'esercizio di attività operative e decisioni gestorie. L'Organismo di Vigilanza non deve trovarsi in situazione di conflitto di interesse e non devono essere attribuiti all' Organismo nel suo complesso, ma anche ai singoli componenti, compiti operativi che ne possano minare l'autonomia.

Il requisito dell'autonomia e dell'indipendenza deve intendersi anche quale assenza di legami parentali e vincoli di dipendenza gerarchica con il vertice della Società o con soggetti titolari di poteri operativi all'interno della stessa.

L'Organismo di Vigilanza deve riportare al massimo vertice operativo aziendale e con questo deve poter dialogare "alla pari".

PROFESSIONALITÀ: ovvero possesso del bagaglio di strumenti e tecniche necessari per lo svolgimento concreto e efficace dell'attività assegnata. La professionalità e l'autorevolezza dell'Organismo sono poi connesse alle sue esperienze professionali. In tal senso, la Società ritiene di particolare rilevanza l'attento esame dei *curricula* dei possibili candidati e le precedenti esperienze, privilegiando profili che abbiano maturato una specifica professionalità in materia.

CONTINUITÀ D'AZIONE: l'OdV svolge in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine, riunendosi con cadenza almeno trimestrale.

ONORABILITÀ: in relazione alla previsione di cause di ineleggibilità, revoca, sospensione o decadenza dalla funzione di Organismo di Vigilanza come di seguito specificate.

I requisiti sopra descritti devono essere verificati in sede di nomina da parte del Consiglio di Amministrazione.

La Società conformemente alle prescrizioni normative contenute nel Decreto, si è orientata nella scelta di un Organismo collegiale composto da **tre membri** individuati tra soggetti particolarmente qualificati ed esperti nelle materie rilevanti ai fini del D.Lgs. n. 231/2001, in modo da garantire all'Organismo adeguata competenza in materia di sistemi di controllo interno, legale, contabile, di *risk assessment* ed *internal auditing*, nonché in possesso dei necessari requisiti di onorabilità.

In particolare, la SIM, in considerazione della complessità organizzativa che ne contraddistingue l'operatività, ha nominato un Organismo composto dai seguenti membri:

- un esponente del Collegio sindacale;

- un rappresentante del sistema dei controlli interni della Società;
- una figura professionale esterna alla Società.

5.2 Le cause di ineleggibilità, revoca, sospensione e decadenza

Nel nominare i componenti dell'Organismo di Vigilanza, il Consiglio di Amministrazione della Società ha espressamente stabilito le seguenti cause di **ineleggibilità** per i medesimi membri dell'OdV.

Non possono dunque essere eletti:

- coloro i quali siano stati condannati con sentenza ancorché non definitiva, o con sentenza di applicazione della pena su richiesta (c.d. "patteggiamento") e anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
 1. alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal R. D. 267/ 1942;
 2. a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
 3. alla reclusione per un tempo non inferiore ad un anno per un delitto contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;
 4. per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;
 5. per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del D.Lgs. 61/2002;
 6. per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
 7. per uno o più reati tra quelli tassativamente previsti dal Decreto, anche se con condanne a pene inferiori a quelle indicate ai punti precedenti;
- coloro nei cui confronti sia stata applicata in via definitiva una delle misure di prevenzione previste dall'art. 10, comma 3, della L. 575/1965, come sostituito dall'art. 3 della L. 55/1990 e successive modificazioni;
- coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* D.Lgs. 58/1998.

I componenti dell'Organismo di Vigilanza devono autocertificare con dichiarazione sostitutiva di notorietà di non trovarsi in alcuna delle condizioni suindicate, impegnandosi espressamente a comunicare eventuali variazioni rispetto al contenuto di tali dichiarazioni.

L'eventuale revoca dei componenti dell'Organismo dovrà essere deliberata dal Consiglio di Amministrazione della Società e potrà esclusivamente disporsi per ragioni connesse a gravi inadempimenti rispetto al mandato assunto, ivi comprese le violazioni degli obblighi di riservatezza di seguito indicati, oltre che per le intervenute cause di decadenza di seguito riportate.

I componenti dell'Organismo di Vigilanza **decadono** inoltre dalla carica nel momento in cui successivamente alla loro nomina:

- siano condannati con sentenza definitiva o di patteggiamento per uno dei reati indicati ai numeri 1, 2, 3, 4, 5, 6 e 7 delle condizioni di ineleggibilità innanzi indicate;
- allorquando abbiano violato gli obblighi di riservatezza strettamente connessi allo svolgimento del loro incarico.

I componenti dell'Organismo di Vigilanza sono inoltre sospesi dall'esercizio delle funzioni nelle ipotesi di:

- condanna con sentenza non definitiva per uno dei reati indicati nei numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;
- applicazione su richiesta delle parti di una delle pene di cui ai numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;
- applicazione di una misura cautelare personale;
- applicazione provvisoria di una delle misure di prevenzione previste dall'art. 10, comma 3, della L. 575/1965, come sostituito dall'art. 3 della L. 55/1990 e successive modificazioni.

L'Organismo di Vigilanza dura in carica tre anni, decade con la data di approvazione del bilancio relativo al terzo anno di esercizio ed è rieleggibile. La retribuzione dell'Organismo viene determinata dal Consiglio di Amministrazione all'atto della nomina per l'intero periodo di durata dell'ufficio.

5.3 I compiti dell'Organismo di Vigilanza di Banor SIM S.p.A.

Per lo svolgimento dei propri compiti il Consiglio di Amministrazione attribuisce all'Organismo di Vigilanza un *budget* di spesa annuo. Tuttavia, l'Organismo di Vigilanza può autonomamente impegnare risorse che eccedano i propri poteri di spesa, nel rispetto delle procedure aziendali, qualora l'impiego delle stesse sia necessario per fronteggiare situazioni eccezionali e urgenti. In questi casi l'Organismo deve informarne senza ritardo il Consiglio di Amministrazione.

L'Organismo di Vigilanza per l'espletamento dei compiti ad esso demandati si avvale di tutte le funzioni aziendali.

L'Organismo di Vigilanza svolge le seguenti attività di:

- vigilanza sull'effettività del Modello, verificando in particolare la coerenza tra il Modello medesimo e le concrete regole adottate nelle aree a rischio;
- verifica periodica che il Modello sia rispettato da parte di tutte le singole unità/aree aziendali a rischio, al fine di accertare che le regole definite e i presidi approntati siano seguiti nel modo più fedele possibile e risultino in concreto idonei a prevenire i rischi della commissione dei reati evidenziati;
- vigilanza affinché il Codice Etico e tutte le disposizioni in esso contenute siano rispettate da tutti i soggetti a qualsiasi titolo operanti nella Società;

- segnalazione al Consiglio di Amministrazione degli eventuali aggiornamenti e adeguamenti del Modello in conformità alle evoluzioni della legge e della giurisprudenza, oltre che in conseguenza di modifiche intervenute all'organizzazione aziendale;
- vigilanza sul corretto funzionamento delle attività di controllo per ciascuna area a rischio, segnalando tempestivamente anomalie e disfunzioni del Modello, previo confronto con le aree/funzioni interessate;
- valuta e propone l'irrogazione di eventuali sanzioni disciplinari, previo il necessario coordinamento con i responsabili delle competenti funzioni/aree aziendali.

5.4 L'attività di reporting dell'Organismo di Vigilanza di Banor SIM S.p.A.

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riporta direttamente al Consiglio di Amministrazione della Società e riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità attraverso due linee di *reporting*:

- I. la prima su **base continuativa**;
- II. la seconda a **cadenza annuale**, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale, attraverso una relazione scritta che dovrà indicare con puntualità l'attività svolta nell'anno, sia in termini di controlli effettuati e degli esiti ottenuti che in ordine alle eventuali necessità di aggiornamento del Modello.

L'OdV deve, altresì, predisporre annualmente un piano di attività previste per l'anno successivo, in cui si individuano le attività da svolgere e le aree che saranno oggetto di verifiche, oltre alle tempistiche e alla priorità degli interventi.

L'Organismo di Vigilanza può, comunque, effettuare, nell'ambito delle attività aziendali sensibili e qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, controlli non previsti nel piano di intervento (c.d. "controlli a sorpresa").

L'Organismo potrà chiedere di essere sentito dal CdA ogniqualvolta ritenga opportuno interloquire con detto organo; del pari, all'OdV è riconosciuta la possibilità di chiedere chiarimenti e informazioni al Consiglio di Amministrazione.

D'altra parte, l'Organismo di Vigilanza potrà essere convocato in ogni momento dal Consiglio di Amministrazione per riferire su particolari eventi o situazioni inerenti al funzionamento e al rispetto del Modello.

I predetti incontri devono essere verbalizzati e copia dei verbali deve essere custodita dall'OdV (nonché dagli organismi di volta in volta coinvolti).

5.5 Obblighi di informativa nei confronti dell'Organismo di Vigilanza di Banor SIM S.p.A.

L'OdV è destinatario di qualsiasi informazione, documentazione e/o comunicazione, proveniente anche da terzi attinente il rispetto del Modello.

Tutti i Destinatari del presente Modello sono tenuti ad un obbligo di informativa verso l'Organismo di Vigilanza, da svolgersi a seguito di:

- i) segnalazioni;**
- ii) informazioni.**

L'Organismo di Vigilanza assicura la **massima riservatezza** in ordine a qualsiasi notizia, informazione, segnalazione, **a pena di revoca del mandato e delle misure disciplinari di seguito definite**, fatte salve le esigenze inerenti allo svolgimento delle indagini nell'ipotesi in cui sia necessario il supporto di consulenti esterni all'OdV o di altre strutture societarie.

Ogni informazione e segnalazione di cui al presente Modello è conservata dall'Organismo di Vigilanza in un apposito archivio informatico e cartaceo, in conformità alle disposizioni in materia di protezione dei dati personali.

i) Le segnalazioni

Tutti i Destinatari sono tenuti a segnalare prontamente all'Organismo di Vigilanza di Banor SIM S.p.A. ogni deroga, violazione o sospetto di violazione di propria conoscenza di norme comportamentali di cui al Codice Etico della Società nonché dei principi di comportamento e delle modalità esecutive di svolgimento delle attività identificate "a rischio" e disciplinate nel Modello.

Le segnalazioni, qualora indirizzate all'Organismo di Vigilanza di Banor SIM S.p.A., possono essere effettuate sia a mezzo di posta fisica all'indirizzo:

Organismo di Vigilanza di Banor SIM S.p.A.
Via Dante, 15 – 20123 Milano

che di posta elettronica all'indirizzo:

odv@Banor.it

La casella di posta elettronica dell'Organismo di Vigilanza garantisce la riservatezza dell'identità del segnalante.

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute e intraprende le conseguenti iniziative a sua ragionevole discrezione e responsabilità nell'ambito delle proprie competenze, ascoltando eventualmente l'autore della segnalazione e il responsabile della presunta violazione. Ogni conseguente decisione deve essere motivata; gli eventuali provvedimenti conseguenti sono applicati in conformità a quanto previsto al capitolo sul Sistema Sanzionatorio.

L'Organismo agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti di Banor SIM S.p.A. o delle persone accusate erroneamente o in mala fede.

ii) Le informazioni

L'Organismo di Vigilanza stabilisce nella propria attività di controllo la documentazione che, su base periodica, deve essere sottoposta alla sua attenzione.

All'Organismo di Vigilanza debbono essere obbligatoriamente trasmessi:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti per le fattispecie di reato previste dal Decreto, riguardanti la Società;
- visite, ispezioni e accertamenti avviati da parte degli enti competenti (Autorità di Vigilanza, enti statali, regioni, enti regionali, enti locali, altro) e, alla loro conclusione, eventuali rilievi e sanzioni comminate;
- richieste di assistenza legale avanzate dai soggetti interni alla Società, in caso di avvio di un procedimento giudiziario per uno dei reati previsti dal Decreto;
- rapporti predisposti dalle strutture aziendali nell'ambito della loro attività di controllo, dai quali emergano elementi di criticità rispetto alle norme del Decreto;
- in via periodica, notizie relative all'effettiva attuazione del Modello in tutte le aree/funzioni aziendali a rischio;
- in via periodica, notizie relative all'effettivo rispetto del Codice Etico a tutti i livelli aziendali;
- informazioni sull'evoluzione delle attività attinenti le aree a rischio;
- il sistema delle deleghe e delle procure adottato dalla Società;
- verbali di accertamento di infrazioni amministrative, regolamentari o fiscali.

In caso di informazioni e/o notizie, anche ufficiose, relative alla commissione dei reati previsti dal Decreto o comunque riguardanti possibili violazioni del Modello e del Codice Etico, ciascuno deve rivolgersi immediatamente all'OdV.

I flussi informativi debbono pervenire all'Organismo, mediante le modalità e gli indirizzi precedentemente indicati.

5.6 Whistleblowing – tutela del dipendente e/o del collaboratore che segnala illeciti – art. 6, comma 2-bis del D.Lgs. 231/2001

Gli articoli 52-*bis* e 52-*ter* del Testo Unico Bancario (TUB), 4-*undecies* e 4-*duodecies* del Testo Unico della Finanza (TUF), 48 del D.Lgs. n. 231/2007, 6 del D. Lgs. 231/2001, la Circolare n. 285 del 17 dicembre 2013 e i successivi aggiornamenti obbligano banche, soggetti abilitati e imprese di assicurazione, soggetti sottoposti alla disciplina sulla prevenzione del riciclaggio e del finanziamento al terrorismo, società dotate di Modello di organizzazione e gestione *ex* D. Lgs. 231/2001, all'adozione di specifiche procedure per la segnalazione al proprio interno, **da parte del personale**, di fatti o atti che possano costituire una violazione delle norme disciplinanti:

- l'attività bancaria (TUB);
- le attività svolte in qualità di soggetti abilitati ai sensi del TUF, o in qualità di imprese di assicurazione per quanto disciplinato dallo stesso TUF;
- la prevenzione del riciclaggio e del finanziamento del terrorismo (D.Lgs. n. 231/2007);
- la responsabilità amministrativa delle società e il Modello di Organizzazione, Gestione e Controllo (D. Lgs. 231/2001).

BANOR si è dotata di un documento denominato “*WHISTLEBLOWING – Procedura per la gestione delle segnalazioni*”, allegato al presente Modello (ALL. 1), che ha l’obiettivo di regolare il processo di gestione delle segnalazioni aventi ad oggetto:

- condotte illecite, rilevanti ai sensi del D.Lgs. 231/2001;
- violazioni del Modello, del Codice Etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- sospetti di violazioni del Modello, del Codice Etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- operazioni societarie o di business o condotte illecite per cui si sospetta possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto, del Testo Unico della Finanza, del Testo Unico Bancario e/o della Circolare;
- condotte in violazione, potenziale o effettiva, delle disposizioni dettate a fini di prevenzione del riciclaggio e del finanziamento del terrorismo.

Tali segnalazioni vengono gestite secondo modalità atte a garantire la riservatezza o l’anonimato del Segnalante nei confronti del personale aziendale non autorizzato a conoscere tali dati, ai sensi della normativa di riferimento.

La Società garantisce la tutela del segnalante da qualsiasi forma di ritorsione e/o discriminazione.

In particolare, è vietato porre in essere atti di ritorsione o discriminazione, diretti o indiretti, nei confronti del segnalante (o *whistleblower*) per motivi collegati direttamente o indirettamente alla segnalazione, in ossequio alle disposizioni normative di cui all’art. 6, comma 2-*bis*, del D.lgs. 231/2001.

L’adozione di misure discriminatorie nei confronti dei soggetti che effettuano segnalazioni può essere denunciata all’Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall’organizzazione sindacale.

Si chiarisce, in conformità alle disposizioni vigenti, che il licenziamento ritorsivo o discriminatorio del soggetto segnalante è da ritenersi nullo, come allo stesso modo sono nulli il mutamento di mansioni, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei suoi confronti.

L’onere della prova grava sul datore di lavoro, il quale dovrà dimostrare che, in caso di controversie legate all’irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Rispetto a segnalazioni effettuate da soggetti che abbiano dichiarato le proprie generalità e che siano in malafede e/o che si dimostri abbiano contenuto calunnioso/diffamatorio saranno attivate le misure previste dal sistema disciplinare aziendale (disciplinato dall’apposita “*Procedura Sistema Sanzionatorio Disciplinare*”) e dal successivo Par. 6 “*Il sistema sanzionatorio*”, nonché valutate appropriate azioni di tutela legale. Fuori dai casi di responsabilità a titolo di calunnia o diffamazione, la presentazione di una segnalazione nell’ambito della presente procedura non costituisce violazione degli obblighi derivanti da rapporto di lavoro.

Come riportato nel documento “*WHISTLEBLOWING – Procedura per la gestione delle segnalazioni*”, colui che desidera effettuare una segnalazione può inoltrarla, preferibilmente avvalendosi del modulo allegato alla citata Procedura, all’indirizzo di posta certificata: whistleblowing.banor@legalmail.it.

Le credenziali di accesso alla casella *e-mail* dedicata, esterna alla rete intranet aziendale per garantirne la separazione dai sistemi informatici della Società, sono fornite al Responsabile dei Sistemi interni di segnalazione.

Al fine di scongiurare possibili manipolazioni delle segnalazioni ricevute (ad esempio mediante la cancellazione manuale delle *e-mail*), le credenziali di accesso alla casella *e-mail* dedicata sono rese note anche ai membri dell’Organismo di Vigilanza; inoltre, è attivata la funzione di inoltro automatico di tutte le *e-mail* ricevute nella casella verso gli indirizzi email dei membri dell’OdV, che abbiano dominio diverso da @banor.it.

Le segnalazioni devono essere fondate su elementi di fatto precisi e concordanti; pertanto, il Segnalante è invitato ad allegare tutta la documentazione comprovante i fatti segnalati, astenendosi dall’intraprendere autonome iniziative di analisi e approfondimento.

6. Formazione e informazione

6.1 Disposizioni generali

La Società intende garantire una corretta e completa conoscenza del Modello, del contenuto del Decreto e degli obblighi dallo stesso derivanti tra quanti operano per la Società.

Sessioni formative saranno organizzate nel tempo dalla Società, in forza dei criteri di obbligatorietà e reiterazione, nonché di quello eventuale della diversificazione.

Al termine delle attività formative è effettuata una verifica del grado di apprendimento e del livello di soddisfazione dei partecipanti.

La formazione e l’informativa sono gestite dal Responsabile della funzione di Compliance, in stretto coordinamento con i responsabili delle aree/funzioni coinvolte nell’applicazione del Modello.

6.2 Comunicazione iniziale

Il presente Modello è comunicato a tutte le risorse aziendali dall’Amministratore Delegato.

Tutti i Dipendenti e gli Apicali devono sottoscrivere un apposito modulo tramite cui attestano l’avvenuta conoscenza e accettazione del Modello, di cui hanno a disposizione una copia cartacea o documenti su supporto informatico.

Ai nuovi assunti viene consegnato un *set* informativo contenente il Modello e il Codice Etico, con il quale vengono assicurati agli stessi le conoscenze considerate di primaria rilevanza.

Tutte le successive modifiche e informazioni concernenti il Modello saranno comunicate alle risorse aziendali attraverso i canali informativi ufficiali.

6.3 Formazione del personale

La **partecipazione alle attività formative** finalizzate a diffondere la conoscenza della normativa di cui al Decreto, del Modello di Organizzazione, Gestione e Controllo e del Codice Etico è da ritenersi **obbligatoria**.

La formazione terrà conto, nei contenuti e nelle modalità di erogazione dei relativi corsi, della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'attribuzione o meno di funzioni di rappresentanza.

L'assenza non giustificata alle sessioni formative è considerata illecito disciplinare, in accordo con quanto previsto dal Sistema Sanzionatorio di seguito enucleato.

Banor SIM S.p.A. prevederà l'attuazione di corsi di formazione che illustreranno, secondo un approccio modulare:

- il contesto normativo;
- il Codice Etico e il Modello di Organizzazione, Gestione e Controllo adottato dalla Società comprensivo delle Parti Speciali;
- il ruolo dell'Organismo di Vigilanza e i compiti ad esso assegnati dalla Società.

L'Organismo di Vigilanza cura che i programmi di formazione siano qualitativamente adeguati ed efficacemente attuati.

La Società provvederà ad istituire una specifica sezione della *intranet* aziendale, dedicata al tema - e aggiornata periodicamente - al fine di consentire ai soggetti interessati di conoscere in tempo reale eventuali modifiche, integrazioni o implementazioni del Codice Etico e del Modello.

6.4 Informativa ai “Terzi Destinatari”

La Società impone la conoscenza e l'osservanza del Modello e del Codice Etico tra i c.d. “Terzi Destinatari”, quali consulenti, collaboratori, fornitori, *partner* e ulteriori soggetti esterni che operano per conto della Società.

L'informativa è assicurata attraverso la circolarizzazione di una comunicazione ufficiale o con l'esplicito riferimento all'interno dei contratti in merito all'esistenza del Modello e del Codice Etico.

Banor SIM S.p.A. provvede ad inserire nei contratti con le terze parti con cui opera apposite clausole che prevedono, in caso di inosservanza dei principi etici stabiliti, la risoluzione degli obblighi negoziali.

7. Il Sistema Sanzionatorio

7.1 Profili generali

La previsione di un sistema sanzionatorio idoneo a sanzionare il mancato rispetto delle regole indicate nel Modello è condizione richiesta dal D.Lgs. 231/2001 per l'esenzione della responsabilità amministrativa degli Enti e per garantire l'effettività del Modello medesimo.

È fatto divieto alla Società, ed agli esponenti di questa, di porre in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. A tale riguardo si chiarisce che sono previste sanzioni disciplinari:

- in caso del mancato rispetto delle misure e dei principi indicati nel Modello;
- nei confronti di chi viola le misure di tutela del segnalante;
- di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano tali segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale.

Si chiarisce, in conformità alle disposizioni vigenti, che il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo.

Sono, altresì, nulli il mutamento di mansioni, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

L'irrogazione di sanzioni disciplinari per violazione dei principi e delle regole di comportamento indicati nel Modello Organizzativo prescinde dall'eventuale instaurazione di un procedimento penale e dall'esito del conseguente giudizio per la commissione di una delle condotte illecite previste dal Decreto.

A seguito della comunicazione dell'OdV della violazione del Modello, viene avviata una procedura d'accertamento in conformità a quanto stabilito dal CCNL di riferimento del dipendente; tale procedura d'accertamento è condotta dagli organi sociali preposti all'irrogazione delle sanzioni disciplinari, tenuto conto della gravità del comportamento, della eventuale recidiva della mancanza o del grado della colpa.

Banor SIM S.p.A., attraverso gli organi e le funzioni a ciò appositamente preposte, provvede dunque ad irrogare con coerenza, imparzialità, e uniformità, sanzioni proporzionate alle rispettive violazioni del Modello e conformi alle vigenti disposizioni in materia di regolamentazione dei rapporti di lavoro; le misure sanzionatorie per le diverse figure professionali sono di seguito indicate.

7.2 Le sanzioni nei confronti dei lavoratori Dipendenti

I comportamenti tenuti dai lavoratori dipendenti che determinano:

- la violazione delle singole regole comportamentali dedotte nel presente Modello, nel Codice Etico, nelle regole e nei protocolli aziendali adottati dalla Società;
- la violazione delle misure poste a tutela dei *whistleblower*;
- la presentazione di segnalazioni infondate con dolo o colpa grave;

costituiscono illeciti disciplinari.

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono adottate nel rispetto delle procedure previste dalla normativa applicabile.

Si fa espresso riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui al CCNL di riferimento.

Si precisa che nell'ambito di detti dipendenti, quelli con qualifica non dirigenziale sono soggetti al Contratto Collettivo Nazionale di Lavoro per i quadri direttivi e per il personale delle aree professionali dipendenti dalle imprese esercenti attività del settore Commercio e Terziario (di seguito "CCNL") e quelli con qualifica dirigenziale sono soggetti al Contratto dei dirigenti delle aziende del Commercio e Terziario (di seguito "CCNL Dirigenti Commercio").

In applicazione del principio di proporzionalità, a seconda della gravità dell'infrazione commessa, sono previste le seguenti sanzioni disciplinari:

Ammonizione verbale si applica nel caso delle più lievi inosservanze dei principi e delle regole di comportamento previsti dal presente Modello, correlandosi detto comportamento ad una **lieve inosservanza** delle norme contrattuali o delle direttive e istruzioni impartite dalla direzione o dai superiori.

Ammonizione scritta: si applica in caso di recidiva delle infrazioni di cui al punto precedente.

Multa o sospensione dal servizio e dalla retribuzione: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello, rispetto ad un comportamento **non conforme o non adeguato** alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva. Tra tali comportamenti rientra la violazione degli obblighi di informazione nei confronti dell'Organismo di Vigilanza in ordine alla commissione dei reati, ancorché tentati, nonché ogni violazione del Modello.

La stessa sanzione sarà applicata in caso di mancata reiterata partecipazione (fisica o in qualunque modo richiesta dalla Società), senza giustificato motivo alle sessioni formative che nel tempo verranno erogate dalla Società relative al Decreto, al Modello di organizzazione, gestione e controllo adottato dalla Società o in ordine a tematiche ad essi relative.

La multa non può superare l'importo di quattro ore di retribuzione. La sospensione dal servizio e dalla retribuzione non può essere disposta per più di dieci giorni e va applicata per le mancanze di maggior rilievo.

Licenziamento per motivi disciplinari: si applica in caso di adozione di un **comportamento consapevole in contrasto con le prescrizioni** del presente Modello che, **ancorché sia solo suscettibile di configurare uno dei reati sanzionati** dal Decreto, **leda l'elemento fiduciario** che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche

provvisoria. Tra le violazioni passibili della predetta sanzione rientrano i seguenti comportamenti intenzionali:

- redazione di documentazione incompleta o non veritiera (ad esempio, documenti indirizzati alla Pubblica Amministrazione, documenti contabili, ecc.);
- omessa redazione della documentazione prevista dal Modello;
- violazione o elusione del sistema di controllo previsto dal Modello in qualsiasi modo effettuata, incluse la sottrazione, distruzione o alterazione della documentazione inerente alla procedura, l'ostacolo ai controlli, l'impedimento di accesso alle informazioni e alla documentazione da parte dei soggetti preposti ai controlli o alle decisioni;
- violazione delle misure indicate nel modello e delle misure previste nel medesimo modello e nelle norme di legge a tutela del segnalante di una condotta illecita ai sensi della l.n. 179/2017;
- effettuazione con dolo o colpa grave di segnalazioni di condotte illecite che si rivelino infondate;
- adozione di misure discriminatorie nei confronti dei soggetti che effettuano segnalazioni di condotte illecite ai sensi della l. n. 179/2017.

7.3 Le sanzioni nei confronti dei componenti del Consiglio di Amministrazione e del Collegio Sindacale e dei Revisori

Nei confronti degli Amministratori che abbiano:

- commesso una violazione del presente Modello;
- violato le misure poste a tutela del *whistleblower*;
- presentato, con dolo o colpa grave, segnalazioni infondate;

il Consiglio di Amministrazione, prontamente informato unitamente al Collegio Sindacale dall'OdV, può applicare ogni idoneo provvedimento consentito dalla legge, fra cui le seguenti sanzioni, determinate a seconda della gravità del fatto e della colpa, nonché delle conseguenze che sono derivate:

- richiamo formale scritto;
- sanzione pecuniaria, tenuto conto della gravità del fatto, pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;
- revoca, totale o parziale, delle eventuali procure.

Il Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea l'adozione dei provvedimenti di competenza e provvede agli ulteriori incumbenti previsti dalla legge.

In caso di violazione da parte del Collegio Sindacale o dei Revisori, l'OdV deve darne immediata comunicazione al Presidente del Consiglio di Amministrazione, mediante relazione scritta. Il Presidente del Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, convoca l'Assemblea inoltrando preventivamente ai soci la relazione dell'Organismo di Vigilanza. L'adozione del provvedimento conseguente la predetta violazione spetta comunque all'Assemblea.

7.4 Le sanzioni nei confronti dei “Terzi Destinatari”

Ogni violazione delle prescrizioni di cui al Modello da parte di consulenti, collaboratori, fornitori, *partner* commerciali, agenti, promotori finanziari e da quanti siano di volta in volta contemplati tra i “Destinatari” dello stesso, è sanzionata dagli organi competenti in base alle regole societarie interne, secondo quanto previsto dalle clausole contrattuali inserite nei relativi contratti, e in ogni caso con l’applicazione di penali convenzionali, che possono comprendere anche l’automatica risoluzione del contratto (ai sensi dell’art. 1456 c.c.), fatto salvo il risarcimento del danno.

ALLEGATI:

- ALL. 1 *“WHISTLEBLOWING – Procedura per la gestione delle segnalazioni”*.