# MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO IN BLUE FACTOR S.P.A. DECRETO LEGISLATIVO 231/2001

METODOLOGIE DI MAPPATURA E

DI VALUTAZIONE DELLE AREE DI RISCHIO

Approvato dal Consiglio di Amministrazione del 21 luglio 2023

SOMMARIO

PARTE SPECIALE

## Sommario

## PREMESSA

In data 8 giugno 2001 è stato emanato il D.Lgs. 8 giugno 2001 n. 231 che reca disposizioni normative concernenti la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" a fronte della quale gli enti, siano essi soggetti privati o pubblici ovvero dotati o meno di personalità giuridica, nonché loro unità organizzative munite di autonomia finanziaria e funzionale, possono essere

perseguiti e sanzionati per i reati di cui al D.Lgs. 231/2001 commessi, a interesse o a vantaggio dell'ente, ad opera dei soggetti che vi operano.

A seguito dell'emanazione del D.Lgs. 231/2001, Blue Factor S.p.A. ha avviato le attività per la predisposizione del Modello di organizzazione, gestione e controllo idoneo *a prevenire i reati dei previsti nel decreto* di cui agli artt. 6 e 7 del Decreto.

A tale scopo sono state svolte tutta una serie di attività propedeutiche suddivise in differenti fasi e dirette tutte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D.Lgs. 231/2001 ed ispirate, oltre che alle norme in esso contenute, anche alle Linee Guida ABI.

La normativa succitata presuppone infatti che la società si doti di un sistema di vigilanza interna che consenta l'effettivo controllo sia sulle sue scelte strategiche nel suo complesso, sia sull'equilibrio gestionale delle singole componenti.

La suddetta Mappatura è uno strumento avente caratteristiche di aggiornamento e dinamicità ed è indispensabile al fine di dimostrare l'idoneità del Modello quale strumento di prevenzione e repressione e consentire all'Organismo di Vigilanza di svolgere correttamente il proprio compito di vigilanza e monitoraggio secondo una pianificazione che tenga conto delle aree di rischio.

## 1. RIFERIMENTI NORMATIVI

Per la redazione del presente documento si è fatto riferimento:

A) D. Lgs. 8 giugno 2001 n. 231 secondo cui ai sensi dell'art. 5 del Decreto, l'ente è responsabile quando:

- Sia stato commesso uno dei reati tra quelli tassativamente indicati nel Decreto e cui lo stesso collega responsabilità per gli enti;
- Il reato sia stato commesso nell'interesse o a vantaggio dell'ente stesso;
- L'autore del reato sia un soggetto in posizione "apicale" in quanto riveste, formalmente o di fatto, funzioni di rappresentanza, di amministrazione e di direzione dell'ente o di una sua unità organizzativa, ovvero sia un cosiddetto "sottoposto" alla direzione o vigilanza dei soggetti appena sopra elencati.

B) "Linee guida per la costruzione di modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001" elaborate da Confindustria e validate dal Ministero della Giustizia le quali suggeriscono la costruzione di un Modello di Organizzazione, Gestione e Controllo sostanzialmente equivalente ad un sistema di gestione dei rischi (*risk management*), che, in relazione all'estensione dei poteri delegati ed al rischio di commissione dei reati "presupposti" dal Decreto, deve rispondere alle seguenti esigenze:

i. individuare le attività aziendali nel cui ambito possono essere commessi i reati previsti dal Decreto ("processi sensibili");

ii. prevedere specifici "protocolli" diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati previsti dal Decreto da prevenire.

C) Linee guida dell'ABI per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche nella versione aggiornata al 19 marzo 2004, la cui idoneità è stata riscontrata dal Ministero della Giustizia con lettera del 25 febbraio 2004.

D) Linee guida dell'Associazione Italiana del Credito al Consumo e Immobiliare per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle associate ai sensi del D.Lgs. 231/2001– giugno 2003 di Assofin.

E) Provvedimento del 27/10/2019 Decreto Legge convertito con modificazioni dalla Legge del 19 dicembre 2019 n. 157 (in G.U. 24/12/2019, n. 301) che fa riferimento all'estensione della responsabilità amministrativa da reato delle società all'ambito penal-tributario.

F) Legge 9 marzo 2022 n. 22 "Disposizioni in materia di reati contro il patrimonio culturale".

## 2. FINALITA' E SCOPI DEL PRESENTE DOCUMENTO. VALUTAZIONE RISCHI PROSPETTABILI

Ai fini del presente documento, le fasi fondamentali in cui si articola il sistema di gestione dei rischi sono le seguenti:

i. elencazione delle fattispecie di reato che presentino un rischio significativo di commissione nelle funzioni aziendali*;*

ii. identificazione delle aree a rischio o aree sensibili;

iii. rilevazione del sistema di controlli esistente e progettazione nuovi controlli finalizzati alla diminuzione dei rischi da reato;

A tal fine si è fatto riferimento all'attività svolta in concreto dalla Blue Factor S.p.A. rendendosi necessaria la predisposizione di un'elencazione di reati, contenuti nel D.Lgs. 231/2001, il cui rischio di commissione potenziale raggiunge una soglia minima di rilevanza. . A tal fine, nella sezione tre di questa parte speciale, sono riportate le fattispecie di reato significative dal punto di vista dei ***rischi potenziali***.

In particolare, per ***rischio potenziale*** di reato a cui è esposta Blue Factor si intende il grado di rischio di commissione del reato tenuto conto del settore di attività in cui opera Blue Factor S.p.A.

Nella sezione quattro vengono valutati i rischi inerenti e il rischio di controllo. Il ***rischio inerente*** si riferisce al grado di rischio di effettiva commissione del reato, tenuto conto del posizionamento di Blue Factor S.p.A. nel mercato, dei suoi principali interlocutori esterni e della sua struttura organizzativa, nonché dal numero di aree operative sensibili alla commissione di tale reato.

Il rischio inerente viene attribuito alla fattispecie di reato secondo una scala da 1 a 5, corrispondente al numero di aree aziendali mappate. In particolare, 1 quando una sola area è sensibile alla commissione di tale reato, 5 quando tutte le aree aziendali sono suscettibili di incorrere in tale reato. Le aree individuate

secondo l'organigramma aziendale sono (i) il CdA; (ii) l'Area Operations; (iii) l'Area Amministrazione e Finanza; (iv) l'Area Legale e (v) l'Area IT. Il rischio inerente basso si verificherà qualora le aree aziendali sensibili alla fattispecie di reato siano <= a 2; medio si verificherà nella situazione in cui le aree coinvolte siano = a 3; e infine il rischio inerente alto si registrerà laddove sono coinvolte da 4 a tutte le aree aziendali tali da rappresentare tutto il business aziendale.

La valutazione del ***rischio di controllo*** è espressa dal grado di rischio che il sistema di controllo interno possa non essere in grado di arginare la commissione dei reati. Anche il rischio di controllo viene attribuito alla specifica fattispecie di reato secondo una scala da 1 a 5. In particolare, il rischio di controllo sarà considerato basso[1] laddove (i) è prevista una specifica funzione con responsabilità di controllo su tale rischio (anche esterna); (ii) sono previste "punizioni" per la persona fisica che commette comportamenti non in linea con le procedure previste; il rischio di controllo sarà considerato medio[2] laddove (i) sono previste regole interne di comportamento e sono altresì previsti controlli periodici su tutte le aree esposte a rischio. Il rischio di controllo sarà considerato alto[3] laddove (i) sono solo previste regole di comportamento interna a presidio di tale reato, (ii) con al limite alcuni controlli a campione.

Anche qualora vi siano rischi inerenti e di controllo bassi, il Modello nella Parte Speciale intende evidenziare le aree a rischio/i soggetti e processi sensibili esposti a tale rischio di reato e nella sezione cinque i controlli dell'Organismo di vigilanza sull'adeguatezza e l'effettività del Modello Organizzativo di Blue Factor.

## 3. ELENCAZIONE DELLE FATTISPECIE DI REATO CON RISCHIO SIGNIFICATIVO DI COMMISSIONE

In via preliminare, le valutazioni dei rischi da reato sono state eseguite al fine di individuare quali, tra le diverse fattispecie riportate nel D.Lg. 231/2001, presentino, per loro natura, un rischio significativo di commissione (sulla base principalmente del settore di attività in cui opera la società) nelle funzioni aziendali operanti nella Blue Factor S.p.A. e, pertanto, siano da sottoporre successivamente ad ulteriore e specifico approfondimento ed analisi.

Non verranno riportati in questo capitolo i reati previsti dal D.Lgs. 231/01 e successive modifiche ed integrazioni, che non risultano applicabili alle attività attualmente svolte dalla Società.

[1] Il rischio di controllo basso corrisponde al punteggio 1 e 2.
[2] Il rischio di controllo medio corrisponde al punteggio 3.
[3] Il rischio di controllo alto corrisponde al punteggio 4 e 5.

### *3.1. Reati contro la pubblica amministrazione*

I reati previsti dall'art. 24 e 25 del D.Lgs. 231/2001 sono configurabili nell'ambito dei rapporti, sia in Italia sia all'estero, con la Pubblica Amministrazione e con tutti quei soggetti che possono essere qualificati pubblici ufficiali o incaricati di pubblico servizio.

In particolare le fattispecie che presentano un rischio significativo di commissione sono:

- Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.): reato che prevede la punibilità di chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità Europee. Tale fattispecie di reato può essere realizzata nell'Area Administration a cui è demandata la direzione risorse umane.

Con specifico riferimento all'attività svolta da Blue Factor, essa può prevedere l'erogazione di contributi o finanziamenti pubblici, e quindi l'utilizzo delle opportunità previste dalle leggi in tema di sgravi di oneri di contributi previdenziali.

- Concussione (art. 317 c.p.): reato che prevede la punibilità del pubblico ufficiale che, abusando della sua qualità o dei suoi poteri costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

- Corruzione per l'esercizio della funzione (art. 318 c.p.): reato che prevede la punibilità del pubblico ufficiale che per l'esercizio della sua funzione o dei suoi poteri, indebitamente riceve per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa.

- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.): reato che prevede la punibilità del pubblico ufficiale che, per omettere o ritardare o per aver omesso 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.

- Istigazione alla corruzione (art. 322 ter c.p.) reato che prevede la punibilità di chiunque offre o promette denaro o altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di pubblico servizio per l'esercizio delle sue funzioni o dei suoi poteri; od anche quando l'offerta o la promessa è fatta al pubblico ufficiale o all'incaricato di pubblico servizio per far omettere o ritardare un atto del suo ufficio ovvero fare un atto contrario ai suoi doveri, qualora l'offerta o la promessa non siano accettate.

- Corruzione in atti giudiziari (art. 319 ter c.p.): reato che prevede la punibilità dei reati di cui agli artt. 318 e 319 c.p. quando commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Tale fattispecie può essere commessa solo nelle ipotesi in cui vi siano procedimenti giudiziari pendenti nei confronti della Società.

- Truffa (art. 640, comma 2, n. 1 c.p.): reato che prevede la punibilità di chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. Il comma 2, n. 1 disciplina l'ipotesi in cui il fatto sia commesso a danno dello Stato o di un altro ente pubblico.

- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.): reato che disciplina l'ipotesi in cui la truffa riguardi contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità Europee. Tale fattispecie costituisce un'ipotesi autonoma del reato di truffa in cui l'oggetto materiale della stessa consiste in ogni attribuzione economica agevolata erogata da enti pubblici, comunque denominata e può essere realizzata nell'Area Amministrazione e Finanza. Per questa specifica fattispecie di rischio, l'attività svolta dalla Società può comportare l'erogazione di contributi o finanziamenti pubblici. In particolare, la Società utilizza le opportunità previste dalle leggi in tema di sgravi di oneri di contributi previdenziali. In considerazione della tipologia limitata delle agevolazioni usufruibili e della non elevata significatività degli importi delle agevolazioni stesse Blue Factor non è capillarmente esposta a tale rischio.

### *3.2. Reati informatici*

- Reati di falsità in documenti informatici (art. 491 bis c.p.): se alcuna delle falsità previste dagli artt. 476 – 493 bis c.p. riguardano un documento informatico pubblico o privato, si applicano le disposizioni delle citate norme concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli. La condotta illecita consiste nella falsificazione di un documento informatico pubblico o privato ovvero di qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli.
- Accesso abusivo ad un sistema informatico o telematico (615 ter c.p.): reato che prevede la punibilità di chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si introduce contro la volontà espressa o tacita di chi ha il diritto di escludere l'accesso di terzi. La pena comminata è aggravata se il fatto è commesso da un incaricato di un pubblico servizio con violazione dei doveri inerenti alla funzione o al servizio, se il reo nel commettere il fatto usa violenza sulle cose o sulle persone, 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 o delle informazioni o dei programmi in esso contenuti. Con tale fattispecie di reato il legislatore ha inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court. Ai fini della punibilità della condotta non assume quindi rilevanza la circostanza che all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando

alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.): tale fattispecie di reato prevede la punibilità di chi diffonde, comunica o consegna un programma informatico redatto dal reo o da altri il cui scopo o effetto sia il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Tale delitto potrebbe ad esempio configurarsi qualora un dipendente si procuri un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.): tale fattispecie di reato prevede la punibilità di chi intercetta, interrompe o impedisce fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Il reato potrebbe configurarsi, ad esempio, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara, con conseguente vantaggio per la società.

- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.): tale fattispecie di reato prevede la punibilità di chi installa, al di fuori dei casi consentiti dalla legge, apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

La condotta vietata dall'art. 617 *quinquies* c.p. è integrata dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.

Il reato risulta, ad esempio, integrato nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione, con conseguente vantaggio della società.

- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.): tale fattispecie di reato prevede la punibilità di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Il danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei files o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di

contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

- 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.): tale fattispecie di reato prevede la punibilità di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.

- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.): tale fattispecie di reato prevede la punibilità di chi distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui oppure ostacola gravemente il loro funzionamento attraverso l'introduzione o la trasmissione di dati, informazioni o programmi ovvero mediante le condotte di cui all'art. 635 bis.

Qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema sussisterà il delitto di danneggiamento di sistemi informatici.

- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.): tale fattispecie di reato prevede la punibilità di chi distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ne ostacola gravemente il funzionamento.

A differenza di quanto previsto dall'art. 635 ter in materia di danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, ciò che rileva è in primo luogo che il danneggiamento abbia ad oggetto un intero sistema e, in secondo luogo, che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

### *3.3. Reati contro il patrimonio: ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita*

- Ricettazione (art. 648 c.p.): tale fattispecie di reato prevede la punibilità di 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. Le disposizioni di cui all'art. 648 c.p. si applicano anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto. Per "acquisto" deve intendersi l'effetto di un attività negoziale, a titolo gratuito od oneroso, mediante la quale l'agente

consegue il possesso del bene. Il termine "ricevere" starebbe ad indicare ogni forma di conseguimento del possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.
Per "occultamento" dovrebbe intendersi il nascondimento del bene, dopo averlo ricevuto, proveniente dal delitto. La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa.
- Riciclaggio (art. 648 bis c.p.): tale fattispecie di reato prevede la punibilità di chi sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa. E' previsto un aumento di pena quando il fatto è commesso nell'esercizio di un'attività professionale. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. La disposizione è applicabile anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto. E' rilevante il fatto di chi ponga ostacoli alla identificazione dei beni suddetti dopo che essi sono stati sostituiti o trasferiti.
- Impiego di denaro, beni o utilità di provenienza illecita (648 ter c.p.): tale fattispecie di reato prevede la punibilità di chi, fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto. E' previsto un aumento di pena quando il fatto è commesso nell'esercizio di un'attività professionale. Il riferimento specifico al termine "impiegare", di accezione più ampia rispetto a "investire" che suppone un impiego finalizzato a particolari obiettivi, esprime il significato di "usare comunque". Il richiamo al concetto di "attività" per indicare il settore di investimento (economia o finanza) consente viceversa di escludere gli impieghi di denaro od altre utilità che abbiano carattere occasionale o sporadico.

### *3.4. Reati societari*

Con la locuzione "reati societari" si indicano le disposizioni penali, per lo più contenute nel codice civile, finalizzate a reprimere con la pena (reclusione o multa) talune condotte realizzate dagli organi sociali sia di società di persone, sia di capitali. Il legislatore ritiene, infatti, che vi sia una determinata categoria di beni giuridici (come, ad esempio, il capitale sociale, gli interessi dei creditori, l'insussistenza di un confitto di interessi) legati all'esercizio dell'attività di impresa in forma societaria che meritino di essere tutelati in via privilegiata attraverso il ricorso alla sanzione penale. Sono reati societari inclusi nel D.Lgs 231/2001: il delitto di false comunicazioni sociali previsto dall' art. 2621 c.c.; il delitto di false comunicazioni sociali previsto dall'art. 2622 c.c.; il delitto di false comunicazioni sociali in danno dei soci o dei creditori previsto dall'art. 2622, comma 3 c.c.; la contravvenzione di falso in prospetto (art. 2623, comma 1 c.c.); il delitto di falso in prospetto (art. 2623, comma 2 c.c.); la contravvenzione di falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624, comma 1 c.c.); il delitto di falsità nelle relazioni o nelle

comunicazioni delle società di revisione (art. 2624, comma 2 c.c.); per il delitto di impedito controllo, (art. 2625, comma 2, c.c.); il delitto di formazione fittizia del capitale, (articolo 2632 del codice civile); il delitto di indebita restituzione dei conferimenti (art. 2626 c.c.); la contravvenzione di illegale ripartizione degli utili e delle riserve (art. 2627 c.c.); il delitto di illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.); il delitto di operazioni in pregiudizio dei creditori (art. 2629 c.c.); il delitto di indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.); il delitto di illecita influenza sull'assemblea (art. 2636 c.c.); il delitto di aggiotaggio (art. 2637 c.c.); il delitto di omessa comunicazione del conflitto d'interessi previsto (art. 2629-bis c.c.); i delitti di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2 c.c.); il delitto di corruzione tra privati (art. 2635 comma 1 e 3 c.c.); istigazione (art. 2635-bis comma 1 c.c.).

### *3.5. Delitti contro la personalità individuale*

I delitti contro la personalità individuale sono disciplinati nella sezione I del capo III del titolo XII del libro II del codice penale. I delitti contro la personalità individuale richiamati dall'articolo 25-quinques del D.Lgs. 231/2001 sono: la riduzione o mantenimento in schiavitù o in servitù (Art. 600 c.p.); la prostituzione minorile (Art. 600-bis c.p); la pornografia minorile (Art. 600–ter c.p.); la detenzione di materiale pornografico (Art. 600–quater c.p.); la pornografia virtuale (Art. 600-quater.1. c.p.); le iniziative turistiche volte allo sfruttamento della prostituzione minorile (Art. 600–quinquies c.p.); la tratta di persone (Art. 601 c.p.); l'acquisto e alienazione di schiavi (Art. 602 c.p.); l'intermediazione illecita e sfruttamento del lavoro (Art.603 bis c.p.); l'adescamento di minorenni (Art. 609-undecies c.p.).

### *3.6. Delitti in materia di strumenti di pagamento diversi dai contanti*

L'art. 3 del d.lgs.184/2021 ha esteso la responsabilità amministrativa degli enti ai delitti in materia di strumenti di pagamento diversi dai contanti, introducendo nel Decreto l'art. 25-octies 1, la cui numerazione vuole sottolineare lo stretto collegamento con i reati di riciclaggio previsti all'art. 25-octies. Il decreto appena menzionato costituisce infatti l'atto di recepimento della Direttiva 2019/713/UE del Parlamento europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, che rappresentano una minaccia alla sicurezza in quanto possono essere fonti di entrate per la criminalità organizzata e quindi rendono possibili altre attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani.

La definizione di strumenti di pagamento diversi dal contante è rinvenibile nell'art. 1 del d.lgs. 184/2021, il quale definisce come tale «un dispositivo, oggetto o record protetto immateriale o materiale, o una loro

combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali», chiarendo ulteriormente che:

i) per «dispositivo, oggetto o record protetto» si intende un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta (per esempio mediante disegno, codice o firma);

ii) la locuzione «mezzo di scambio digitale» indica «qualsiasi moneta elettronica definita all'art. 1, comma 2, lett. h ter), d.lgs. 385/1993, e la valuta virtuale», intendendosi quest'ultima come una «rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente»

Tali definizioni riprendono sostanzialmente quelle proposte nella Direttiva (UE) 2019/71.

In virtù del primo comma del art. 25-octies.1, la condanna dell'ente può discendere, oltre che dai delitti ex artt. 493-ter c.p. (indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti) e 493-quater c.p. (detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti), anche dalla commissione di frode informatica (art. 640-ter c.p.), nella nuova ipotesi aggravata quando il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale.

### *3.7. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*

Il reato di cui all'art. 25-decies, D. Lgs. 231/2001, si configura quando un soggetto avente facoltà di non rispondere è indotto, tramite violenza, minaccia, ovvero offerta o promessa di denaro o altre utilità, a non rendere dichiarazioni ovvero a rendere dichiarazioni mendaci davanti all'autorità giudiziaria (Giudice o P.M.). I destinatari di questa condotta sono, pertanto, gli indagati e gli imputati, anche in procedimenti connessi o in reati collegati, ai quali è riconosciuta dall'ordinamento la facoltà di non rispondere. Affinché si configuri il delitto in esame, è richiesta l'effettiva astensione della persona informata sui fatti dalle dichiarazioni oppure una sua falsa dichiarazione.

Tale fattispecie di reato può realizzarsi quando, ad esempio, il dirigente di un ente, con minaccia, induce la persona chiamata, davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, a rendere dichiarazioni mendaci (377-bis del c.p.).

*3.8. Reati Ambientali*

Il d.lgs. 7 luglio 2011, n. 121 - recante "Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente e della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni" – ha introdotto, nell'ambito dei reati presupposto di cui al d.lgs. 231/01, l'art. 25-undecies, che prevede la responsabilità degli enti per i reati ambientali.

Più recentemente, la Legge 22 maggio 2015 n. 68 recante "Disposizioni in materia di delitti contro l'ambiente" (G.U. Serie Generale n.122 del 28-5-2015), oltre ad aver modificato in maniera significativa il d.lgs.152/2006 in materia, *ha introdotto all'interno del codice penale un lungo elenco di reati ambientali* (collocati nel nuovo Titolo VI-bis intitolato "Dei delitti contro l'ambiente"), una buona parte dei quali è configurato dalla Legge stessa come reato-presupposto atto a far scattare la responsabilità amministrativa dell'impresa, con conseguente modificazione e integrazione dell'articolo 25-undecies del decreto legislativo 8 giugno 2001 n.231.

Trattasi, nello specifico di (i) delitto di inquinamento ambientale (art. 425-bis c.p.); (ii) delitto di disastro ambientale (art. 452-quater c.p.); (iii) delitti colposi contro l'ambiente (art.452-quinquies c.p.); (iv) delitti associativi aggravati ai sensi dell'articolo 452-octies; (v) delitto di traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.).

Tra i reati ambientali previsti dal D.Lgs. 231/2001 vi sono inoltre: 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.); 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 (art. 137 d.lgs. 152/2006); Attività di gestione di rifiuti non autorizzata (art. 256 d.lgs. 152/2006)[4]; Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 d.lgs. 152/2006)[5]; Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 d.lgs. 152/2006)[6]; Traffico illecito di rifiuti (art. 259 d.lgs. 152/2006)[7]; attività organizzate per il traffico illecito di rifiuti (commi 1 e 2) (art 452 quaterdecies c.p.); Sistema informatico di controllo della tracciabilità dei rifiuti (*260-bis* [8] d.lgs. 152/2006).

[4] In particolare, nel D.Lgs 231/2001 viene fatto richiamo ai *Comma 1 (lettera a e b), 3 (primo e secondo periodo), 5, 6 (primo periodo) dell'art 256 d.lgs. 152/2006.*

[5] In particolare, nel D.Lgs 231/2001 viene fatto richiamo ai *Comma 1 e Comma 2, dell'art 257 del d.lgs. 152/2006.*

[6] In particolare, nel D.Lgs 231/2001 viene fatto richiamo ai *Comma 4 secondo periodo dell'art 258 del d.lgs. 152/2006.*

[7] In particolare, nel D.Lgs 231/2001 viene fatto richiamo ai *Comma 1 dell'art 259 del d.lgs. 152/2006.*

[8] In particolare, nel D.Lgs 231/2001 viene fatto richiamo ai Commi 6, 7 (secondo e terzo periodo), 8 (primo e secondo periodo) *Comma 1 dell'art 260-bis del d.lgs. 152/2006.*

*3.9. Impiego di cittadini di paesi terzi*

I reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare così come individuati nell'art. 25 duodecies del D.Lgs. n. 231 del 2001 si configurano qualora il soggetto che riveste la qualifica di datore di lavoro occupi alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o sia stato revocato o annullato, laddove ricorrano le specifiche circostanze aggravanti previste dall'art. 22 (art. 22, comma 12-bis, d.lgs. 25 luglio 1998, n. 286). L'art. 25duodecies è stato successivamente modificato dalla Legge n. 161 del 2017 (Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate), che ha introdotto l'ulteriore fattispecie di illecito, prevista dall'art. 12, comma 3, 3-bis, 3-ter e 5, del citato D. Lgs. 15 luglio 1998, n. 286 recante "Disposizioni contro le immigrazioni clandestine".

*3.10. Reati tributari*

Con l'entrata in vigore del provvedimento del 27/10/2019 Decreto Legge convertito con modificazioni dalla Legge del 19 dicembre 2019 n. 157 (in G.U. 24/12/2019, n. 301) la responsabilità amministrativa da reato delle società è stata estesa all'ambito penal-tributario, ricomprendendo nel novero dei reati presupposto di tale responsabilità anche:

- la dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2);
- la dichiarazione fraudolenta mediante altri artifici (art. 3);
- l'emissione di fatture o altri documenti per operazioni inesistenti;
- l'occultamento o distruzione di documenti contabili (art. 10);
- la sottrazione fraudolenta al pagamento di imposte (art. 11).

l) Inoltre, in data 14 luglio 2020, è stato pubblicato in Gazzetta Ufficiale il D.Lgs. 14 luglio 2020 n. 75[9], il quale è andato ad ampliare ulteriormente il novero dei reati tributari ex D. Lgs. 231, includendovi i seguenti reati, laddove presentassero elementi di transnazionalità e rilevanza (imposta IVA evasa superiore a 10 milioni di Euro):

- delitti di dichiarazione infedele;
- delitti di omessa dichiarazione;
- delitti di indebita compensazione.

[9] Decreto attuativo della Direttiva PIF Europea

### *3.11. Reati Transnazionali*

Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale: 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. 25 luglio 1998, n. 286); 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); induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.); favoreggiamento personale (art. 378 c.p.); associazione per delinquere (art. 416 c.p.); associazione di tipo mafioso (art. 416-bis c.p.)

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

La Legge 3 agosto 2007 n. 123 ha introdotto l'art. 25-septies del D.Lgs. 8 giugno 2001, n. 231, articolo in seguito sostituito dall'art. 300 del D.Lgs. 81/2008, che prevede la responsabilità degli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica per i reati di omicidio colposo (art. 589 c.p.) e lesioni personali colpose (art. 590 c.p.) gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

## 4. *AREE AZIENDALI SENSIBILI E SISTEMI DI CONTROLLO A PRESIDIO DEL RISCHIO*

Come più volte sottolineato il modello organizzativo consiste in un sistema strutturato e organico di procedure e attività di controllo costruito in funzione dei "processi sensibili" della società.

Per "processi sensibili" si intendono i processi critici che possono portare alla commissione dei reati previsti dalla legge con la conseguenza che l'individuazione delle aree a rischio risulta profilo indispensabile al fine di prevenire la commissione di tali reati.

L'individuazione delle aree nel cui ambito possono essere commesse le fattispecie di reato previste dalla legge non può che articolarsi facendo specifico riferimento alla diversa tipologia di delitti contenuti nel modello.

In particolare, vengono individuate le aree/i processi sensibili della società esposte al manifestarsi delle fattispecie di reato riportate nel capitolo 3 del presente documento.

*4.1. Reati contro la Pubblica Amministrazione*

*Aree/soggetti e processi a rischio*

Con riferimento a tali reati, i principali processi sensibili ritenuti più specificatamente a rischio, in Blue Factor S.p.A., sono i seguenti:

- Gestione degli adempimenti, delle comunicazioni e delle richieste non connesse all'attività caratteristica, anche in occasione di verifiche ed ispezioni da parte delle Autorità di Vigilanza quali, ad esempio:

a) Gestione dei rapporti con le Autorità Pubbliche di Vigilanza (es. Banca Italia, Agenzia Entrate, Garante Privacy), delle comunicazioni e informazioni ad esse dirette e trasmissione della documentazione prevista per legge;
b) Gestione dei rapporti con la Guardia di finanza, Agenzia delle Entrate, Ispettorato del Lavoro ed altri Enti competenti in materia fiscale e tributaria in occasione di verifiche, ispezioni e accertamenti;
c) Gestione dei rapporti con i funzionari pubblici in occasioni di verifiche circa il rispetto dei presupposti e delle condizioni (ad es. piano informativo, durata ecc.) richieste dalla normativa vigente per le assunzioni agevolate e le assunzioni obbligatorie (categorie protette);
d) Gestione degli adempimenti in materia di assunzioni, cessazioni dal rapporto di lavoro, retribuzioni, ritenute fiscali, contributi previdenziali e assistenziali relativi a dipendenti e collaboratori;
e) Gestione dei rapporti con funzionari competenti (INPS INAIL ASL ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento, ad esempio in materia di predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro; autorizzazione per l'assunzione di personale appartenente a categorie protette; ottenimento della certificazione di ottemperanza in materia di collocamento obbligatorio; elenchi di personale attivo, assunto e cessato presso l'INAIL; controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente;

Il responsabile dell'Area Administration provvede a fornire al soggetto obbligato i vari adempimenti sopra descritti, il supporto informativo e logistico, nonché a predisporre i documenti necessari, per l'adempimento di tutti gli obblighi normativi e regolamentari. Tale funzione include la raccolta e trasmissione dei dati e delle informazioni:

- ✓ all'organo amministrativo per la redazione del bilancio annuale, la relazione degli amministratori, le dichiarazioni fiscali periodiche e quelle annuali;

- ✓ ai professionisti esterni per la compilazione e revisione degli atti e dichiarazioni sopra citate e/o l'inoltro degli stessi all'Autorità.

Inoltre, al responsabile dell'Area Administration competono la gestione di tutti i rapporti amministrativi con le società di recupero, incluso il pagamento delle competenze, il recupero delle somme indebitamente corrisposte, gli adempimenti fiscali, tributari e amministrativi in genere.

*Suddivisione di aree sensibili per specifici reati contro la PA*

Nel dettaglio, la fattispecie art. 316 ter c.p. di reato di cui all'art. può essere realizzata nell'area Amministrazione e Finanza a cui è demandata la direzione risorse umane. Le fattispecie di cui agli artt. 317, 318, 319, 322 ter c.p. possono essere realizzate nell'Area Amministrazione e Finanza e nell'Area Operations.

La fattispecie di reato "Truffa" prevista dall'art. 640, comma 2, n. 1 c.p., che rileva ai fini della responsabilità dell'ente solo nel caso in cui il reato di truffa sia commesso in danno dello Stato o di altro ente pubblico e, quindi, può essere realizzata nell'Area Amministrazione e Finanza.

*Controlli a presidio del rischio*

Il rischio di commissione del reato di istigazione alla corruzione (art. 322 ter c.p) che sussiste in quanto la Società può avere rapporti con pubblici ufficiali o incaricati di pubblico servizio[10] è presidiato dalle verifiche periodiche che Blue Factor S.p.A. effettua, supportate da consulente esterni, sul rispetto delle diverse normative pubbliche.

### *4.2. Reati informatici*

*Aree/soggetti e processi a rischio*

Come già ampiamente accennato e ricordato, i reati in questione previsti dall'art. 24 bis, così come le altre fattispecie contemplate nel modello di organizzazione e gestione, presuppongono l'esistenza dell'interesse o vantaggio per la Società.

La responsabilità della Società, dunque, potrebbe essere rilevata in caso di attacco ad un sistema informatico posto in essere per arrecare vantaggio alla stessa (si pensi ad esempio alle ipotesi di spionaggio o sabotaggio nelle gare per la cessione dei crediti).

Il rischio di commissione può interessare tutte le aree aziendali.

[10] Si pensi ai controlli delle ASL, all'Ispettorato del Lavoro, alle verifiche di conformità alla legge sulla privacy, alle verifiche fiscali, ai rapporti con uffici tecnici comunali, provinciali e regionali per nuove concessioni ecc.

Con riferimento ai reati elencati all'art. 24 bis sono ipotizzabili delle oggettive difficoltà nella individuazione del reo, col conseguente rischio di potersi configurare una responsabilità della società proprietaria del computer, senza che l'autore sia individuato o individuabile.
La gestione del database societario e del trattamento dei dati informatici fanno capo ai responsabili delle Aree Administration e Operation oltre che agli addetti al servizio IT, quando non siano riservati, per legge o per statuto, all'organo amministrativo nella persona del legale rappresentante.

*Suddivisione di aree sensibili per specifici reati informatici*

Il rischio di commissione di Reati di falsità in documenti informatici (art. 491 bis c.p.) può sussistere nell'Area Amministrazione e Finanza in quanto la Società deve effettuare comunicazioni e segnalazioni periodiche telematiche a Banca d'Italia inoltre può configurarsi nell'Area IT e Operation ove viene svolta l'attività di trasmissione e importazione files e documenti informatici nel programma gestionale.
L'accesso abusivo ad un sistema informatico o telematico (615 ter c.p.) può interessare l'Area Amministrazione e Finanza, l'Area Operations e l'Area IT in quanto la Società è autorizzata all'accesso a sistemi informatici e telematici ed archivi protetti.
Il rischio di commissione del reato previsto dall'art 617 quater c.p. può interessare l'Area IT in collaborazione con l'Area Operation a cui è demandata la funzione di trasmissione delle offerte per l'acquisto dei crediti in cessione.
Il reato di Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.) può essere commesso dall'Area IT in collaborazione con l'Area Operation in quanto i responsabili delle due aree potrebbero recarsi presso la Società cedente per svolgere attività di Due Diligence sulle pratiche oggetto di futura cessione.
Il rischio di commissione del reato di danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.) può interessare tutte le aree aziendali della società. l'Area Operation, l'Area Amministrazione e Finanza e l'Area IT. Il rischio può configurarsi solo quando la Società, in persona del Responsabile o addetto all'Area Operation e del Responsabile Area IT, si reca presso la Società cedente per svolgere attività di Due Diligence sulle pratiche oggetto di futura cessione.

*Controlli a presidio del rischio*

I responsabili delle Aree Amministrazione e Finanza e Operation e gli addetti al servizio IT provvedono a fornire all'organo amministrativo e a tutte le aree della società i flussi informativi necessari all'adempimento delle funzioni a ciascuno spettanti.
Per tutti gli altri dipendenti e collaboratori la possibilità di accesso al database societario e il trattamento dei dati informatici sono limitati ai soli settori di proprio interesse.

Inoltre, il Responsabile Area Amministrazione e Finanza si avvale di consulente esterni ed effettua controlli sull'importazione e trasmissione di files e documenti informatici.
Seppur, l'attività di Blue Factor non richieda l'accesso a sistemi informatici e telematici nell'ordinaria attività l'accesso abusivo ad un sistema informatico o telematico (615 ter c.p.) al Responsabile Area Operation è demandata la funzione di sicurezza e controllo.
Il Responsabile dell'Area IT si occupa invece della gestione e della supervisione dei sistemi informatici a presidio dei rischi di danneggiamento di dati sensibili favorendo posizioni pendente di Blue Factor.
Internamente la Società impedisce ai non addetti ai lavori l'accesso a dati o programmi informatici altrui se non in consultazione

### *4.3. Reati contro il patrimonio: ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita*

*Aree/soggetti e processi a rischio*

Per i reati di cui agli artt. 648, 648 bis, 648 ter il rischio di commissione di tale reato può interessare tutte le Aree aziendali a vari livelli organizzativi in quanto i core business della Società si sostanzia nella valorizzazione dei crediti acquistati da terzi e nella relativa attività di riscossione di flussi di denaro, provenienti, ancorché per il tramite di altri intermediari finanziari, dai debitori ceduti.

I reati previsti dall'art. 25 octies del D. Lgs. 231/2001, che sono reati funzionali al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo, come già sottolineato, possono concretizzarsi in tutte le Aree aziendali ed a vari livelli organizzativi.
A tal fine bisogna distinguere le tipologie di rapporti che intercorrono tra la società i debitori ceduti, i creditori cedenti, i clienti e fornitori e le società di recupero.
I rapporti con i debitori sono mantenuti in maniera concorrente dai responsabili delle Aree Administration e Operation. La ripartizione dei rapporti è effettuata secondo il seguente criterio:

- ✓ al responsabile dell'Area Operation compete, nell'ambito delle procedure vigenti e delle direttive dell'organo amministrativo, per i crediti classificati in fase di esazione la definizione degli accordi di pagamento e le transazioni, oltre che l'eventuale esazione diretta del credito;
- ✓ al responsabile dell'Area Administration competono la gestione di tutti i rapporti amministrativi con il debitore, inclusa la riscossione delle somme esatte, l'emissione dei documenti fiscali, gli adempimenti fiscali, tributari e amministrativi in genere, oltre che l'annotazione delle formalità nelle scritture contabili aziendali.

La gestione dei rapporti finanziari con i Clienti e i Fornitori fanno capo al responsabile dell'Area Administration quando non siano riservati, per legge o per statuto, all'organo amministrativo.

Il responsabile dell'Area Administration provvede, senza limite di importo, all'adempimento delle obbligazioni pecuniarie validamente contratte dalla società, annotandone la formalità nelle scritture contabili aziendali.

I rapporti con le società di recupero sono mantenuti in maniera concorrente dai responsabili delle Aree Administration e Operation. La ripartizione dei rapporti è effettuata secondo il seguente criterio:

- ✓ al responsabile dell'Area Operation compete, nell'ambito delle procedure vigenti e delle direttive dell'organo amministrativo, la selezione delle società, la verifica dei requisiti di professionalità, la definizione degli accordi di collaborazione, l'assegnazione, la revoca e/o la sospensione degli incarichi, la verifica del raggiungimento degli obiettivi e dei risultati;
- ✓ al responsabile dell'Area Administration competono la gestione di tutti i rapporti amministrativi con le società di recupero, incluso il pagamento delle competenze, il recupero delle somme indebitamente corrisposte, gli adempimenti fiscali, tributari e amministrativi in genere.

I rapporti con i creditori cedenti sono demandati in maniera concorrente al Responsabile dell'Area Operation ed Administration. La ripartizione dei rapporti avviene come segue:

- ✓ al responsabile Area Operation è demandata l'attività di analisi di trattativa, analisi e conclusione del contratto;
- ✓ al responsabile Area Administration è demandata l'attività di regolamento finanziario dell'operazione di cessione e i relativi adempenti contabili.

*Controlli a presidio del rischio*

L'Area Controlli presidia il rischio di riciclaggio di denaro contenendo significativamente il fenomeno. Pertanto, sono previste regole di comportamento capillarmente diffuse in tutte le aree aziendali, alimentate da controlli continui coordinati dalla responsabile nell'Area Controlli.

*Blue Factor ha inoltre, stilato il manuale delle procedure operative WhistleBlowing, al fine di consentire ai dipendenti o alle persone in posizione comparabile che operano nell'azienda, di inviare segnalazioni di illeciti delle quali sono venuti a conoscenza durante lo svolgimento del proprio lavoro in ottemperanza alle disposizioni normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.*

### *4.4. Reati societari*

*Aree/soggetti e processi a rischio*

Le potenziali aree a rischio reati che la società ha individuato nell'ambito dei reati societari sono quelle relative all':

- Area Amministrazione e Finanza con funzione di predisposizione dei bilanci, relazioni e altre comunicazioni sociali previste dalla legge; alle comunicazioni alle Autorità di Vigilanza e alla gestione

dei rapporti con gli stessi; alla gestione dei rapporti con il Collegio Sindacale, e gli altri organi societari. L'area Amministrazione e Finanza, potrebbe essere esposta nella predisposizione del bilancio di esercizio e delle altre relazioni infra-annuali ai reati di cui agli artt. 2621 c.c. (false comunicazioni); nei rapporti con il collegio sindacale, ai reati di cui all' articolo 2625 c.c. (nel caso di impedimento al controllo ad esempio nei casi di omissione di documentazione ovvero non corretta gestione dei libri contabili);e nei rapporti con Autorità di Vigilanza ai reati di falso di cui agli artt. 2621 c.c. e di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.) nell'assolvimento degli obblighi imposti dalla vigilanza informativa e ispettiva. Nei rapporti con le autorità di vigilanza potrebbero avvenire anche episodi di corruzione rilevanti ai sensi dell'art. 318 c.p. e seguenti (corruzione).

- C.d.A. nello svolgimento delle riunioni consiliari/Delibera di operazioni societarie è sensibile a tale reato. Il CdA nell'assunzione delle decisioni di sua competenza può incorrere nel rischio riferito ai reati di cui agli artt. 2626 c.c.(indebita restituzione dei conferimenti), all' art 2627 c.c. (illegale ripartizione degli utili e delle riserve), all'art 2628 c.c. (illecite operazioni sulle azioni o quote sociali della Capogruppo), 2629 c.c. (operazioni in pregiudizio dei creditori) e all'art. 2632 c.c. (formazione fittizia del capitale).

*Controlli a presidio del rischio*:

Al fine di presidiare tali rischi di reato Blue Factor è dotata di policy interne e controlli di compliance e governo del rischio dei reati sopra citati, e in particolare al rischio di diffusione di informazioni non corrette da parte delle diverse aree aziendali. I regolamenti interni a tal fine disciplinano le modalità operative, i tempi, le responsabilità per la redazione, la pubblicazione dei documenti e/o la trasmissione alle autorità competenti.

Blue Factor si è dotata di una policy in materia di conflitto di interessi e di una mappatura dei soggetti collegati e dei potenziali conflitti. Il MOGC intende presidiare il rischio dei reati di cui all'art 25 ter garantendo inoltre la tracciabilità delle attività sia a livello di sistema informatico sia in termini documentali.

L'esplicitazione delle responsabilità delle varie funzioni permette infine un maggior controllo.

### *4.5. Delitti contro la personalità individuale*

*Aree/soggetti e processi a rischio*

Sebbene non si possano escludere casi in cui la Società persegua finalità illecite connesse a reati lesivi della personalità individuale, si ritiene che profili di rischio maggiormente rilevanti con riferimento ai reati previsti dall'art. 25 quinquies del D. Lgs. 231 possano ravvisarsi soprattutto con riferimento ai casi in cui

l'esponente societario agisca in concorso con soggetti terzi. In particolare, oltre al gruppo di selezione del personale (i.e. CFO, Responsabile Area Operations, e Presidente del C.d.A.), i reati previsti all'art 25 quinquies potrebbero essere commessi dalle società a cui sono delegate le attività in outsourcing.

*Controlli a presidio del rischio*

In particolare, tale rischio viene presidiato nella fase in cui Blue Factor formalizza il mandato a svolgere la lavorazione stragiudiziale all'esterno in regime di outsourcing a soggetti muniti di autorizzazione all'attività di recupero crediti. Tale rischio è inoltre fronteggiato internamente attraverso la formalizzazione del piano ferie e dalla riduzione dell'orario lavorativo.

### *4.6. Delitti in materia di strumenti di pagamento diversi dai contanti*

*Aree/soggetti e processi a rischio*

Le aree e i processi organizzativi interessati da tale reato sono quelli che si occupano di gestire, controllare e monitorare i flussi patrimoniali e finanziari, in quanto la gestione illecita - diretta o indiretta - degli strumenti di pagamento (in entrata o in uscita) e dei movimenti monetari, potrebbe rappresentare fonti di entrate per la criminalità organizzata. In particolare, l'Area suscettibile di incorrere in tale reato è l'Area Amministrazione e Finance nella gestione pagamenti e dei flussi di cassa.

*Controlli a presidio del rischio*:

Potrebbe verificarsi una gestione impropria dei flussi di cassa - anche al fine di avvantaggiare la società o terzi - (i.e., il pagamento di importi maggiori o importi non dovuti rispetto al pattuito, ricezione di denaro proveniente da attività illecite, impiego di denaro in modo da far perdere le tracce di denaro di origine illecita e utilizzo di strumenti di pagamento non intestati alla Società). Inoltre, nella gestione e nello sviluppo dei sistemi informativi interni in grado di segnalare tempestivamente eventuali anomalie negli accessi ai sistemi informativi interni/gestiti dalla società. Inoltre, la società adotta procedure di controllo periodiche sulle disponibilità finanziarie dell'intermediario al fine di contrastare l'accesso illegittimo ai sistemi informativi aziendali con lo scopo di effettuare trasferimenti illeciti di denaro.

### *4.7. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*

*Aree/soggetti e processi a rischio:*

I reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, possono concretizzarsi nell'Area Legale e in particolare nei rapporti della stessa con il soggetto imputato dinnanzi all'autorità giudiziaria.

L'art. 25-decies prevede nello specifico il reato commesso da chi, con violenza o minaccia o con offerta o promessa di denaro o di altre utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci coloro che siano chiamati a rendere dichiarazioni davanti all'autorità giudiziaria, utilizzabili in un procedimento penale, ed abbiano la facoltà di non rispondere. Si precisa che tale reato può dar luogo alla responsabilità dell'ente anche se commesso senza le caratteristiche della transnazionalità, essendo richiamato, oltre che dalla L.146/2006, anche dall'art. 25 decies del Decreto.

*Controlli a presidio del rischio*

Dato l'attività di recupero crediti per il tramite del pignoramento (pratica legale) laddove non si arrivi ad un accordo stragiudiziale, Blue Factor potrebbe incorrere in tale reato. Tuttavia, le fasi di lavorazione del credito giudiziale sono separate dalla fase di sentenza del giudice sul pignoramento dello stipendio. La società non ha contatti con il debitore se la pratica passa a sentenza del giudice, per cui non avrebbe modo di indurre a false dichiarazioni l'accusa. Inoltre, la società si è dotata di un manuale delle procedure e dei comportamenti interni sulla base di requisiti di correttezza, professionalità e trasparenza.

### *4.8. Reati Ambientali*

*Aree/soggetti e processi a rischio*

I reati previsti dall'art. 25 undecies del D. Lgs. 231/2001, possono concretizzarsi in tutte le Aree aziendali ed a vari livelli organizzativi. Tuttavia, le attività che presentano un rischio potenziale più elevato sono le aree che si occupano della (i) selezione e gestione dei rapporti con i fornitori per lo smaltimento dei toner e degli hardware; e della (ii) selezione e gestione dei rapporti con i fornitori del servizio di raccolta e smaltimento rifiuti.

*Controlli a presidio del rischio*

Trattandosi di fattispecie di danno e di pericolo concreto, la società sta introducendo da inizio 2023, anche a seguito delle comunicazioni ricevute da Banca di Italia, nuovi e comunque più penetranti strumenti di verifica e controllo sui processi operativi e sulle attività aziendali relative alla gestione ambientale. A tal proposito verrà individuata una struttura ad hoc che avrà nil compito di presidiare il rischio di accadimento delle fattispecie di reato legate all'ambiente e al clima.

*4.9. Impiego di cittadini di paesi terzi*

*Aree/soggetti e processi a rischio*

Blue Factor tutela, rispetta e promuove la diversità in termine di genere, di etnia, di religione, di orientamento sessuale, di disabilità, di età e di estrazione sociale. In tal senso l'intermediario potrebbe incorrere nel reato di favoreggiamento all'immigrazione irregolare in termini di assunzioni alle proprie dipendenze di lavoratori stranieri privi del permesso di soggiorno e nella stipula di contratti con le società di outsourcing che potrebbero commettere tale reato (in particolare, con riferimento alle società di recupero crediti dislocate in varie parti di Italia).

*Controlli a presidio del rischio*:

La Società nella formalizzazione del mandato a svolgere la lavorazione stragiudiziale all'esterno, in regime di outsourcing, controlla che i soggetti individuati abbiano l'autorizzazione all'attività di recupero crediti oltre ai presidi per evitare di incorrere in rischio di favoreggiamento all'impiego di cittadini di paesi terzi.

*4.10. Reati tributari*

Aree/soggetti e processi a rischio

In forza della struttura delle fattispecie incriminatrici è possibile individuare l'Area esposta a rischio-reato "diretto", ossia quelle aree che includono attività di natura fiscale, come la predisposizione e la presentazione delle dichiarazioni fiscali, la liquidazione e il versamento dei tributi e la tenuta e la custodia della documentazione obbligatoria. All'interno dell'intermediario tale area è riconducibile all'Area Amministrazione e Finanza che si occupa sia di attività sensibili in materia di gestione fiscale/tributaria sia di attività sensibili in materia di gestione amministrativo – contabile.

Controlli a presidio del rischio

Sono presenti gli sistemi di controllo in senso stretto che fanno riferimento a processi di pianificazione e controllo tramite riconciliazioni periodiche dei dati/documenti/informazioni. Vengono inoltre effettuati controlli manuali su base campionaria per assicurare che i dati siano corretti e accurati. Tutti gli scostamenti non attesi sono identificati, investigati e risolti.

*4.11. Reati Transnazionali*

*Aree/soggetti e processi a rischio*

Le aree potenzialmente a rischio di commissione di tale reato sono l'area Operations nella gestione degli accordi con l'estero, e l'area Controlli nel verificare la provenienza e l'utilizzo dei fondi al fine di presidiare

il rischio di coinvolgimento diretto di Blue Factor in attività punibili secondo quanto previsto dalla legge Legge n. 146/2006.

*Controlli a presidio del rischio*

Il controllo sul rischio di coinvolgimento in attività di associazione a delinquere o associazione di stampo mafioso viene effettuato in prima istanza dall'Area Operations, successivamente dall'Area controlli interni. Tutte le controparti con cui la società entra in contatto vengono valutate attentamente attraverso anche controlli reputazionali con l'obiettivo di fare in modo che tali parti terze (anche estere), attengano nella loro operatività a regole di condotta non punibile secondo i reati previsti dalla normativa vigente.

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

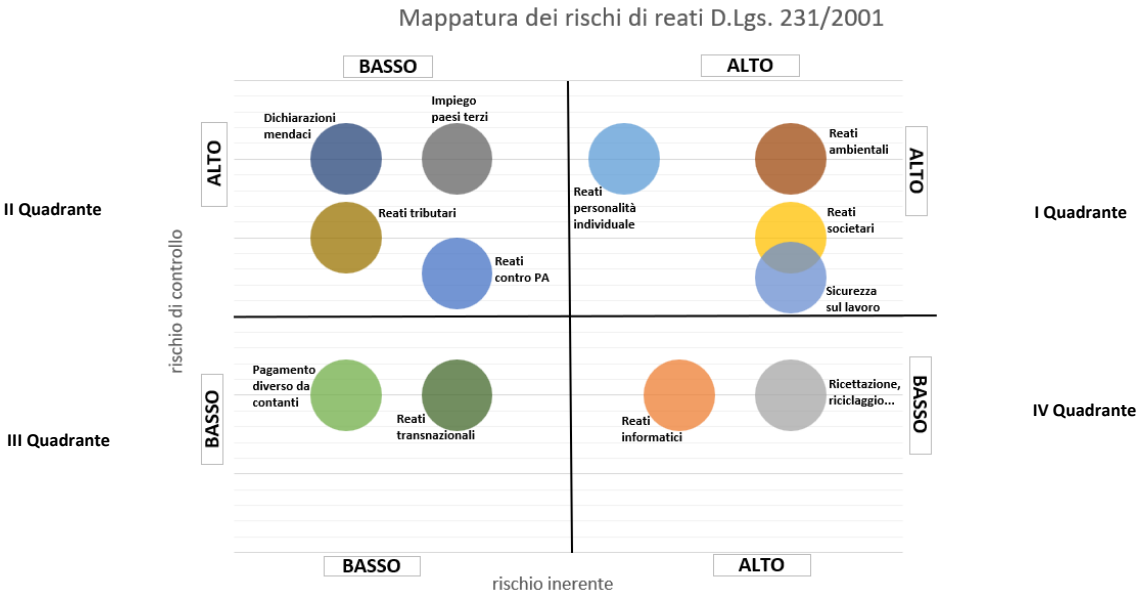
*Aree/soggetti e processi a rischio*

Tutte le aree aziendali sono esposte a tale rischio: dirigenti, quadri, soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché i medesimi dipendenti.
Tali reati potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro. L'elemento essenziale ed unificante delle varie e possibili forme di responsabilità del datore di lavoro è la mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili, alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche. In proposito la Corte Cost. ha precisato (sent. n. 312/1996) che l'obbligo generale di massima sicurezza possibile si riferisce alle misure che nei diversi settori corrispondono ad applicazioni tecnologiche generalmente praticate, sicché penalmente censurata è solo la deviazione del datore di lavoro dagli standard di sicurezza propri, in concreto ed al momento, delle singole diverse attività produttive.

*Controlli a presidio del rischio*

Blue Factor presta la massima attenzione alla salvaguardia della sicurezza e della salute dei propri dipendenti, impegnandosi a identificare ed eliminare le eventuali situazioni di rischio che si possono presentare e a migliorare le condizioni di lavoro. In altri termini, non sottovaluta l'importanza di un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività. Inoltre, alcune aree aziendali individuate come maggiormente rischiose per la sicurezza dei dipendenti, sono accessibili solo al personale autorizzato.

## 5. MAPPATURA DEI RISCHI DI REATO D.Lgs. 231/2001




La matrice riporta tutte le fattispecie di rischio potenziale evidenziate nel capitolo 3 a cui Blue Factor è esposta e come di seguito descritte:

I Quadrante

Si evidenziano le fattispecie di rischio a caratterizzate da un elevato coinvolgimento delle diverse aree aziendali e da un basso presidio in termini di controllo. Sono reati che sono di recente identificazione e per tali ragioni la società sta programmando la predisposizione di adeguati sistemi di controllo (e.g. reati ambientali; reati societari, sicurezza sul lavoro e reati contro la personalità individuali). In linea con le nuove disposizioni dell'Autorità di Vigilanza la società sta infatti integrando le logiche Environmental, Social e Governance (ESG) nell'operatività aziendale.

II Quadrante

Si evidenziano i rischi che impattano meno sull'operatività di Blue Factor e verso quali, per tale ragione, ad oggi non vi è una rete di controlli sufficientemente organizzata (e.g. reati contro PA, reati tributari, induzione a dichiarazioni mendaci, e impiego di cittadini di paesi terzi).

III Quadrante

Si evidenziano i rischi che coinvolgono in solo in parte le aree aziendali di Blue Factor e per i quali sono presenti adeguati presidi a supporto (e.g., reati transnazionali e reati legati a strumenti di pagamento diversi dai contanti).

IV Quadrante

Si evidenziano i rischi che impattano in maniera rilevante sull'operatività di Blue Factor per i quali è presente una struttura di controlli adeguata al loro presidio (e.g. reati informatici e reati legati al riciclaggio).

## 6. SISTEMA DI CONTROLLI ESISTENTE E PROGETTAZIONE NUOVI CONTROLLI FINALIZZATI ALLA DIMINUZIONE DEI RISCHI DA REATO. *RISK MANAGEMENT*

Il Consiglio di Amministrazione di Blue Factor ha attribuito nel gennaio 2016 il ruolo di Organismo di Controllo al Collegio Sindacale.

Secondo quanto stabilito dalla Parte Generale del Modello, tale organismo svolge sia l'attività di controllo sull'effettività del modello sia l'attività di vigilanza sull'adeguatezza dello stesso.

Al fine di poter assolvere in modo esaustivo ai propri compiti, l'Organismo di Vigilanza è dotato di poteri di acquisizione e di richiesta di informazioni da e verso ogni livello e settore operativo e amministrativo della Società.

Come sottolineato nel Manuale delle Procedure Interne, il titolare dei rapporti con l'Autorità Vigilante è il legale rappresentante della Società, il quale è tenuto ad informare senza indugio il Presidente del Collegio Sindacale di ogni atto o fatto comunque inerente lo svolgimento della attività soggetta a vigilanza nonché l'adempimento degli obblighi di informativa e comunicazione all'Autorità Vigilante.

Il Presidente del Collegio Sindacale è tenuto, invero, ad informare, altresì, l'organo amministrativo e, ove necessario, l'assemblea, dell'eventuale inadempimento degli obblighi imposti dalla legge, dai regolamenti o dall'Autorità Vigilante inerenti lo svolgimento dell'attività vigilata, mentre i titolari del rapporto sono coadiuvati dal Responsabile Amministrativo nell'adempimento degli obblighi inerenti lo svolgimento della attività vigilata.

Inoltre, dalla "Relazione sulle Attività di Verifica" compilata nel 2020 emerge che l'Organismo di Vigilanza ha organizzato singoli incontri con i Responsabili di Aree ed Uffici al fine di verificare in concreto il grado di comprensione del Modello e del Codice Etico e di completare la ridefinizione del sistema in base ai cambiamenti organizzativi verificatisi; l'Organismo di Vigilanza si è occupato, poi, di verificare il rispetto delle disposizioni contenute nel Modello, avvalendosi della collaborazione del Responsabile *Internal Auditing* che ha proceduto alla consegna dei verbali degli atti e delle operazioni poste in essere durante le fasi di lavorazione e chiusura delle pratiche, da lui redatti con il supporto dei Responsabili di Area.

Sulla base delle verifiche effettuate è emerso che il personale di Blue Factor S.p.A. ha letto, compreso e messo in atto il Modello di Organizzazione ed il Codice Etico e che la Società ha svolto puntualmente l'attività di diffusione ed implementazione del Modello sia all'interno che all'esterno della struttura societaria; non sono, invece, emerse attività relative alla possibile commissione dei reati da parte del

personale di Blue Factor S.p.A. il quale, viceversa, applica correttamente le procedure in essere e i protocolli esistenti.

L'attività svolta dal personale dipendente della Società è, inoltre, sottoposta ad un controllo di primo livello effettuato dai preposti all'area di riferimento ed in particolare dal Responsabile Area Administration, Responsabile Area IT e Responsabile Area Administration, mentre al Responsabile Risk Management, al Responsabile Compliance ed al Responsabile Antiriciclaggio è demandato il controllo di secondo livello sull'operato dei Responsabili Area.

L'attività di controllo di terzo livello è deputata, da ultimo, alla funzione di Internal Auditing.

A fronte del *Risk Mapping* sopra effettuato, considerato che le attività svolte da tutti gli uffici della Società sono potenzialmente esposte al rischio riciclaggio, al fine di assolvere agli obblighi previsti dalla normativa di riferimento ed in particolare dal Decreto Legislativo del 21 novembre 2007, n. 231 e successive modificazioni, si rende necessaria la predisposizione di un Regolamento Operativo Antiriciclaggio.

ALLEGATO A: Regolamento Antiriciclaggio