Modello di Organizzazione Gestione e Controllo

ai sensi del D.lgs. 8 giugno 2001, n. 231

INDICE

Modello di Organizzazione Gestione e Controllo

Ai sensi del D.lgs. 8 giugno 2001, n. 231

PARTE GENERALE

1 IL DECRETO LEGISLATIVO N. 231/2001 E LA NORMATIVA RILEVANTE

1.1 LA RESPONSABILITÀ AMMINISTRATIVA A CARICO DELLE PERSONE GIURIDICHE

Il Decreto Legislativo n. 231 dell'8 giugno 2001, che introduce la *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"* (di seguito il "Decreto"), ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali precedentemente sottoscritte dallo Stato Italiano[1].

Il Decreto ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa (equiparabile sostanzialmente alla responsabilità penale) a carico degli enti (gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica; sono esclusi lo Stato, gli enti pubblici territoriali, gli enti pubblici non economici, e quelli che svolgono funzioni di rilievo costituzionale), che va ad aggiungersi alla responsabilità della persona fisica che ha realizzato materialmente alcune specifiche fattispecie di reato e che mira a coinvolgere, nella punizione degli stessi, gli Enti nel cui interesse o vantaggio tali reati siano stati compiuti.

L'art. 5 del Decreto stabilisce che le persone fisiche che commettendo uno specifico reato nell'interesse o a vantaggio dell'ente ne possono determinare la responsabilità, possono essere:

a) persone fisiche che rivestono posizione di vertice ("apicali") (rappresentanza, amministrazione o direzione dell'Ente o di altra unità organizzativa o persone che esercitano, di fatto, la gestione ed il controllo);
b) persone fisiche sottoposte alla direzione o vigilanza da parte di uno dei soggetti sopraindicati.

L'Ente non è ritenuto responsabile qualora i soggetti che rivestono posizione di vertice abbiano agito esclusivamente nell'interesse proprio o di terzi.

Inoltre, viene meno la responsabilità dell'Ente per i reati commessi dalle persone di cui sopra, quando lo stesso prova che:

[1] In particolare: la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea; la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione di funzionari pubblici sia della Comunità Europea che degli Stati membri; la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e gestione idonei a prevenire la commissione di reati della specie di quello verificatosi;
- l'Ente ha affidato il compito di vigilare sul funzionamento, l'osservanza e l'aggiornamento del modello di organizzazione e di gestione ad un organismo dotato di autonomi poteri di iniziativa e di controllo;
- l'autore dell'illecito ha commesso il reato eludendo in modo fraudolento i modelli di organizzazione e di gestione predisposti;
- l'Organismo di Vigilanza (di seguito "OdV") non ha omesso o adempiuto in modo parziale ai suoi doveri.

Non tutti i reati commessi dai soggetti sopracitati implicano una responsabilità amministrativa riconducibile all'Ente, atteso che sono individuate come rilevanti solo alcune specifiche tipologie di reato[2].

Si ritiene che le tipologie di reato ad oggi previste nel Decreto e che possono potenzialmente riguardare la società Justbit Società a Responsabilità limitata (di seguito "Justbit"), sono quelle di seguito indicate:

A- Reati di corruzione, anche tra privati [articolo 24 del Decreto come modificato dalla L. n. 190/2012 e dal D.lgs. 75/2020] e altri reati nei rapporti con la pubblica amministrazione e l'UE (Art. 24 del Decreto modificato dal D.lgs. 75/2020))

- Concussione (art. 317 c.p.) [modificato dalla L. n. 69/2015]
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [articolo modificato dalla L. n. 190/2012] [modificato dalla L. n. 69/2015]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [modificato dalla L. n. 69/2015]
- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.) [modificato dalla L. n. 69/2015]
- Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012] [modificato dalla L. n. 69/2015]
- Peculato (art. 318 c.p.) in offesa degli interessi finanziari dell'Unione Europea;

[2] L'elenco dei reati presupposto rilevanti ai sensi del Decreto è soggetto a continue variazioni.

- Peculato mediante profitto dell'errore altrui (art. 316 c.p.) in offesa degli interessi finanziari dell'Unione Europea;
- 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 dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) [articolo modificato dalla L. n. 190/2012]
- Abuso d'ufficio (art. 323 c.p.) in offesa degli interessi finanziari dell'Unione Europea
- Traffico influenze illecite (art 346 bis c.p.)
- Malversazione a danno dello Stato (art. 316-bis c.p.)
- Indebita percezione di erogazioni a danno dello Stato (art.316-ter c.p.)
- Truffa in danno dello Stato o di altro ente pubblico o dell'Unione Europea (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.)

B- Reati informatici e trattamento illecito dei dati, disciplinati dall'art. 24-bis, introdotto con la Legge 18 marzo 2008, n. 48 come modificato dalla Legge n. 133 del 18/11/2019 (Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica), ovvero

- Falsità in un documento informatico pubblico avente efficacia probatoria (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- 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.)
- False informazioni e dati relativi perimetro di sicurezza nazionale cibernetica (art. 1 comma 11 del Decreto Legge 21/09/2019, n. 105 come convertito e modificato dalla Legge n. 133 del 18/11/2019)[3]

C- Delitti di criminalità organizzata (Art. 24-ter, Decreto 231) [articolo aggiunto dalla L. n. 94/2009]

- Associazione per delinquere (art. 416 c.p.p.)[4]
- Associazione di tipo mafioso (art. 416-bis c.p.) [modificato dalla L. n. 69/2015][5]

D- Resti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, Decreto 231) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001] [modificato dalla L. n. 99/2009][6]

- 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.)

[3] La legge n. 133 del 18/11/2019 ha introdotto una nuova fattispecie di reato che punisce con la reclusione da uno a cinque anni chiunque, allo scopo di ostacolare o condizionare l'espletamento delle procedure di controllo o delle attività ispettive ivi previste, fornisce informazioni, dati o elementi di fatto rilevanti non rispondenti al vero, od omette tali comunicazioni nei termini prescritti. La definizione di tali procedure di controllo e l'individuazione dei soggetti interessati facenti parte del perimetro di sicurezza cybernetica (enti, pubbliche amministrazioni o operatori) è stata demandata a un decreto del DPCM da emanare entro 10 mesi dall'entrata in vigore della legge. Per tali motivi, sino all'emanazione del suddetto decreto, tale fattispecie non risulta applicabile

[4] Tale reato costituisce presupposto per la responsabilità amministrativa degli enti se commesso in modalità transnazionale

[5] Tale reato costituisce presupposto per la responsabilità amministrativa degli enti se commesso in modalità transnazionale

[6] Il D.Lgs. 21 giugno 2016 n. 125 ha apportato talune modifiche ai seguenti articoli del Codice penale: (453, 461).

- 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.)-

E- Delitti contro l'industria e il commercio (Art. 25-bis.1, Decreto 231) [articolo aggiunto dalla L. n. 99/2009]

- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.)

F- Reati societari (Art. 25-ter, Decreto 231) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. n. 69/2015 e dal D. Lgs. 15 marzo 2017, n. 38]

- False comunicazioni sociali (art. 2621 c.c.) [modificato dalla L. n. 69/2015]
- Fatti di lieve entità (art. 2621-bis c.c.) [aggiunto dalla L. n. 69/ 2015]
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Formazione fittizia del capitale (art. 2632 c.c.)
- Illecita influenza sull'assemblea (art. 2636 c.c.)

G- Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater, Decreto 231) [articolo aggiunto dalla L. n. 7/2003]

- 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.)
- 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.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289-bis c.p.)
- Istigazione a commettere alcuno dei delitti preveduti 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.)
- Impossessamento, dirottamento e distruzione di un aereo (art. 1, L. n. 342/1976)
- Danneggiamento delle installazioni a terra (art. 2, L. n. 342/1976)
- Sanzioni (art. 3, L. n. 422/1989)
- Pentimento operoso (art. 5, D.Lgs. n. 625/1979)
- Convenzione di New York del 9 dicembre 1999 (art. 2)
- finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.)
- sottrazione di beni o denaro sottoposti a sequestro (art. 270-quinquies.2 c.p.)
- atti di terrorismo nucleare (art. 280-ter c.p.)

Tali reati sono considerati a fini prudenziali quali fattispecie potenzialmente rilevanti - tenuto conto che l'art 25-quater del Decreto 231 opera un rinvio "aperto" alle ipotesi di reati terroristici ed eversivi –seppur la predetta Legge non abbia espressamente apportato modifiche al Decreto 231.

H- Delitti contro la personalità individuale (Art. 25-quinquies, Decreto 231) [articolo aggiunto dalla L. n. 228/2003, come da ultimo modificato dalla L. n. 199/2016], razzismo e xenofobia (Art. 25-terdecies, del Decreto 231) [articolo aggiunto dalla Legge n. 167/2017]

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Detenzione di materiale pornografico (art. 600-quater)
- Adescamento di minorenni (art. 609-undecies c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.)
- Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 604 bis c.p.).

I- Reati di abuso di mercato (Art. 25-sexies, Decreto 231) [articolo aggiunto dalla L. n. 62/2005]

- Abuso di informazioni privilegiate (art. 184, D.Lgs. n. 58/1998)

L- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, Decreto 231) [articolo aggiunto dalla L. n. 123/2007]

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

M- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 231/2007; modificato dalla L. n. 186/2014]

- 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.).

N- Delitti in materia di violazione del diritto d'autore (Art. 25-novies, Decreto 231) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, comma 1, lett. a-bis), L. n. 633/1941);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, comma 3, L. n. 633/1941);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis, comma 1, L. n. 633/1941);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis, comma 2, L. n. 633/1941);

- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter, L. n. 633/1941);

O- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, Decreto 231) [articolo aggiunto dalla L. n. 116/2009][7]

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

P- Reati ambientali (Art. 25-undecies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 121/2011] [modificato dalla L. n. 68/2015 con aggiunta del comma 1-bis]

- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (artt. 1 e 2, L. n. 150/1992)
- Attività di gestione di rifiuti non autorizzata (art. 256, D. Lgs n.152/2006)
- Traffico illecito di rifiuti (art. 259, D. Lgs. n.152/2006)
- Attività organizzate per il traffico illecito di rifiuti (art. 452 quaterdecies c.p.)

Q- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, Decreto 231) [articolo aggiunto dal D.Lgs. n. 109/2012, come da ultimo modificato dalla L. n. 161/2017]

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, D.Lgs. n. 286/1998)
- Disposizioni contro le immigrazioni clandestine (art. 12 del D.Lgs. n. 286/1998)[8].

[7] Tale reato costituisce presupposto per la responsabilità amministrativa degli enti se commesso in modalità transnazionale

[8] Tale reato costituisce presupposto per la responsabilità amministrativa degli enti se commesso in modalità transnazionale

R- Reati in materia di imposte sui redditi ("reati tributari) come disciplinato dall'art. 25 - quinquiesdecies introdotto dalla Legge 19 dicembre 2019, n. 157. Conversione in legge, con modificazioni, del decreto-legge 26 ottobre 2019, n. 124, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili e modificato dal D. Lgs 75/2020

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (articolo 2 del Dlgs n. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (articolo 3 del Dlgs n. 74/2000);
- dichiarazione infedele (articolo 4 del D.lgs. 74/2000) nell'ambito di sistemi transfrontalieri;
- omessa dichiarazione (articolo 5 del D.lgs. 74/2000) nell'ambito di sistemi transfrontalieri;
- emissione di fatture o altri documenti per operazioni inesistenti (articolo 8 del Dlgs n. 74/2000);
- occultamento o distruzione di documenti contabili (articolo 10 del Dlgs n. 74/2000);
- Indebita compensazione (art. 10 quater del D.lgs. 74/2000) nell'ambito di sistemi transfrontalieri;
- sottrazione fraudolenta al pagamento di imposte (articolo 11 del Dlgs n. 74/2000).

Ciò premesso, e al fine di prevenire la commissione dei reati sopraindicati, si ritiene altresì opportuno evidenziare che JustBit può essere chiamata a rispondere, ex art. 4 del D.lgs. 231/2001, anche quando il reato è stato realizzato all'estero. In tal caso, il processo sarà effettuato dinanzi l'Autorità giudiziaria italiana. I presupposti (previsti dalla norma ovvero desumibili dal complesso del D.lgs. 231/2001) su cui si fonda la responsabilità della JustBit per reati commessi all'estero sono così sintetizzabili:

i. il reato deve essere commesso all'estero da un soggetto funzionalmente legato alla società, ai sensi dell'art. 5, comma 1, del D.lgs. 231/2001;
ii. la società deve avere la propria sede principale nel territorio dello Stato italiano;
iii. la società può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p.;
iv. sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti della società non proceda lo Stato del luogo in cui è stato commesso il fatto.

Per completezza, deve infine ricordarsi che l'art. 23 del Decreto punisce l'inosservanza delle sanzioni interdittive, che si realizza qualora alla Società sia stata applicata, ai sensi del Decreto,

una sanzione o una misura cautelare interdittiva e, nonostante ciò, lo stesso trasgredisca agli obblighi o i divieti ad essi inerenti.

1.2 LE SANZIONI PREVISTE DAL DECRETO

Nell'ipotesi in cui la società commetta uno dei reati indicati al precedente paragrafo, lo stesso potrà subire l'irrogazione di sanzioni da parte delle Autorità competenti.

Come stabilito all'art. 9 del Decreto, le sanzioni amministrative previste dal legislatore si suddividono in:

- Sanzioni pecuniarie (artt. 10, 11, 12 del D.lgs. 231/2001)

  si applicano in tutti i casi in cui sia riconosciuta la responsabilità della Società. Vengono applicate per "quote", in numero non inferiore a 100 e non superiore a 1.000, mentre l'importo di ciascuna quota va da un minimo di 258,23 € ad un massimo di 1.549, 37 €. Il numero di quote viene stabilito dal Giudice sulla base degli indici individuati dal comma 1 dell'art. 11, mentre l'importo delle quote è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto.

- Sanzioni interdittive (art. 9, comma 2 del D.lgs. 231/2001)

  sono irrogabili nelle sole ipotesi tassativamente previste e solo per alcuni reati. Le sanzioni interdittive sono:
  - l'interdizione dall'esercizio dell'attività;
  - la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
  - l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
  - il divieto di pubblicizzare beni e servizi.

  Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice in sede penale, tenendo conto dei fattori meglio specificati dall'art. 14 del Decreto. In ogni caso, le sanzioni interdittive hanno una durata minima di tre mesi e massima di due anni.

Uno degli aspetti di maggiore interesse è che le sanzioni interdittive possono essere applicate all'Ente sia all'esito del giudizio e, quindi, accertata la colpevolezza dello stesso, sia in via cautelare, ovvero quando:

- sono presenti gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato;
- emergono fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede;
- l'Ente ha tratto un profitto di rilevante entità.

- Pubblicazione della sentenza (art. 18 del D.lgs. 231/2001)

La pubblicazione della sentenza è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva.

- Confisca (art. 19 del D.lgs. 231/2001)

La confisca del prezzo o del profitto del reato è una sanzione obbligatoria che consegue alla eventuale sentenza di condanna.

Per completezza, infine, deve osservarsi che l'Autorità Giudiziaria può, altresì, disporre:

- il sequestro preventivo delle cose di cui è consentita la confisca (art. 53);
- il sequestro conservativo dei beni mobili e immobili dell'Ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54).

1.3 L'ADOZIONE E L'ATTUAZIONE DI UN MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto, forme specifiche di esonero della responsabilità amministrativa della società.

In particolare, l'art. 6, comma 1, prescrive che, nell'ipotesi in cui i fatti di reato siano ascrivibili a soggetti in posizione apicale, l'Ente non è ritenuto responsabile se prova che:

a) ha adottato ed attuato, prima della commissione del fatto, un Modello di Gestione, Organizzazione e Controllo (di seguito, per brevità, anche solo 'Modello') idoneo a prevenire reati della specie di quello verificatosi;

b) ha nominato un organismo, indipendente e con poteri autonomi, che vigili sul funzionamento e sull'osservanza del Modello e che ne curi l'aggiornamento;
c) il reato è stato commesso eludendo fraudolentemente le misure previste nel Modello;
d) non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Il contenuto del Modello è individuato dallo stesso art. 6, il quale, al comma 2, prevede che la società debba:

a) individuare le attività nel cui ambito possono essere commessi i reati;
b) prevedere specifici protocolli/procedure/regolamenti volti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
c) individuare modalità di gestione delle risorse finanziarie idonee a prevenire i reati;
d) prevedere obblighi di informazione nei confronti dell'OdV;
e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello.

Nel caso dei soggetti in posizione subordinata, l'adozione e l'efficace attuazione del Modello comporta che la l'Ente sarà chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza (combinato di cui ai commi 1 e 2 dell'art. 7).

I successivi commi 3 e 4 introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità della Società per entrambe le ipotesi di reato di cui all'art. 5, lett. a) e b). Segnatamente, è previsto che:

- il Modello deve prevedere misure idonee sia a garantire lo svolgimento dell'attività nel rispetto della legge, sia a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione o cambiamenti normativi; assume rilevanza, altresì, l'esistenza di un idoneo sistema disciplinare (condizione, invero, già prevista dalla lett. e), *sub* art. 6, comma 2).

Sotto un profilo formale, pertanto, l'adozione ed efficace attuazione di un Modello non costituisce un obbligo, ma unicamente una facoltà per gli Enti, i quali potrebbero decidere di non conformarsi al disposto del Decreto senza incorrere, per questo motivo, in alcuna sanzione.

Tuttavia, l'adozione ed efficace attuazione di un Modello idoneo è, per gli Enti, un presupposto irrinunciabile per poter beneficiare dell'esimente prevista dal Legislatore.
È importante, inoltre, tenere in precipuo conto che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette alla Società di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze (ad es. carenze nel sistema di controllo interno) che, al momento della sua creazione, non era possibile individuare.

2 ELABORAZIONE DEL MODELLO

L'elaborazione del Modello può essere sintetizzata nei seguenti step operativi:

- **Mappatura delle aree aziendali a rischio di reato**

  Compimento di una analisi della realtà della società, con l'obiettivo di individuare le aree interessate dalle potenziali casistiche di reato previste dal Decreto.
  Nel dettaglio, sono state analizzata le fattispecie di reato considerate dal decreto ed individuate le aree, i soggetti e le forme di operatività in relazione ai quali ci può essere un rischio di commissione di quei reati.
  Alla luce dei risultati di tale indagine è stato possibile valutare l'idoneità dei presidi esistenti ed assunto le decisioni in ordine alla eventuale implementazione di ulteriori punti di controllo.
  L'output di fase è costituito dalla mappatura delle aree, dei processi aziendali a rischio di reato e delle attività sensibili descritta all'interno delle specifiche "parti speciali".

- **Analisi dei rischi potenziali**

  Tale attività ha riguardato le possibili modalità attuative dei reati nelle diverse aree della società individuate nella fase di mappatura ed ha condotto ad una rappresentazione esaustiva delle modalità con cui le fattispecie di reato possono essere attuate rispetto al contesto operativo interno ed esterno in cui opera la società.
  L'output di fase è costituito da una mappatura delle potenziali modalità attuative degli illeciti nelle aree a rischio individuate descritta all'interno delle specifiche "parti speciali".

- **Valutazione/costruzione/adeguamento del sistema di controlli preventivi**

  Tale processo ha riguardato una valutazione del sistema di controlli preventivi eventualmente esistente e, ove necessario, al suo adeguamento, ovvero, la sua costruzione quando assenti. Il sistema di controlli preventivi è tale da garantire che i rischi

di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile". Si tratta, in sostanza, di progettare quelli che il D. Lgs. n. 231/2001 definisce *"specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire"*.

L'output di fase è costituito dalla descrizione documentata del sistema dei controlli preventivi attivato, con dettaglio delle singole componenti del sistema, nonché delle azioni integrative eventualmente necessarie ("Documento di analisi iniziale e Assessment").

Le componenti più rilevanti del sistema di controllo preventivo definito nelle Linee Guida sono:

- codice Etico comportamentale;
- sistema organizzativo;
- procedure manuali ed informatiche;
- sistema di controllo e gestione;
- comunicazioni al personale e sua formazione.

Il sistema di controllo, inoltre, è stato uniformato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni/direzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e delle procedure previste dal Modello;
- individuazione di un OdV, deputato a vigilare sul funzionamento, l'efficacia e l'osservanza del Modello ed a curarne l'aggiornamento, dotato dei seguenti requisiti:
  - autonomia ed indipendenza,
  - professionalità,
  - continuità di azione.
- obbligo di informativa nei confronti dell'OdV da parte delle funzioni aziendali operanti in aree a rischio di reato.

Il Modello di Jusbit è stato elaborato secondo la struttura e le direttive presenti nel Modello organizzativo della società che detiene la maggioranza delle quote societarie, EPRComunicazione S.p.A SB, al fine di acquisirne i principi generali di gestione e i protocolli comportamentali, pur mantenendo una propria autonomia gestionale.

3 IL MODELLO DI ORGANIZZAZIONE E CONTROLLO ADOTTATO DA JUSTBIT

3.1 PROFILO SINTETICO DI JUSTBIT S.R.L.

Justbit è una società attiva nella realizzazione di soluzioni digitali nata nel 2011 grazie all'idea di un gruppo di giovani ingegneri vincitori di un progetto sperimentale e innovativo come l'Ericsson Application Awards.
Alle competenze tecnologiche si uniscono esperienze di business management, marketing e comunicazione.
La visione trasversale consente di poter seguire l'intero ciclo di vita di un progetto: dall'idea alla progettazione, dallo sviluppo e realizzazione, fino alla sua promozione.

3.2 ORGANIZZAZIONE SOCIETARIA

Justbit è una società capitali a responsabilità limitata costituita nel 2011 e con un'unica sede operativa in Roma, Via Benedetto Cairoli 2.
Justbit ha come socio maggioritario la società "Eprcomunicazione S.p.A. Società Benefit", che ne ha acquisito la maggioranza delle quote nell'anno 2023. La restante parte di quote è suddivisa in parti uguali tra gli altri quattro soci, di cui tre risultano soci fondatori.
Al fine di assicurare la massima coerenza tra strategia e comportamenti, Justbit adotta un modello di governance tradizionale caratterizzato da:

- Un Consiglio di amministrazione (CdA) nominato dall'assemblea dei soci, composto da cinque amministratori;
- Il Presidente del Consiglio di amministrazione;
- Un Amministratore Delegato, unico soggetto ad avere, oltre al Presidente, i poteri di rappresentanza legale dell'impresa; lo stesso amministratore ricopre anche il ruolo di CFO (Chief Financial Officer);
- Una struttura gerarchica complessa organizzata per Business Unit.

Nel corso del mese di Febbraio 2024 sono stati delegati dal CdA i poteri circa la gestione dei flussi bancari in uscita al Responsabile dell'Unità amministrativa, che detiene anche il ruolo di Consigliere nell'ambito del CdA, fino a un massimo di 100.000 €.
La macrostruttura organizzativa viene riportata nel seguente organigramma:

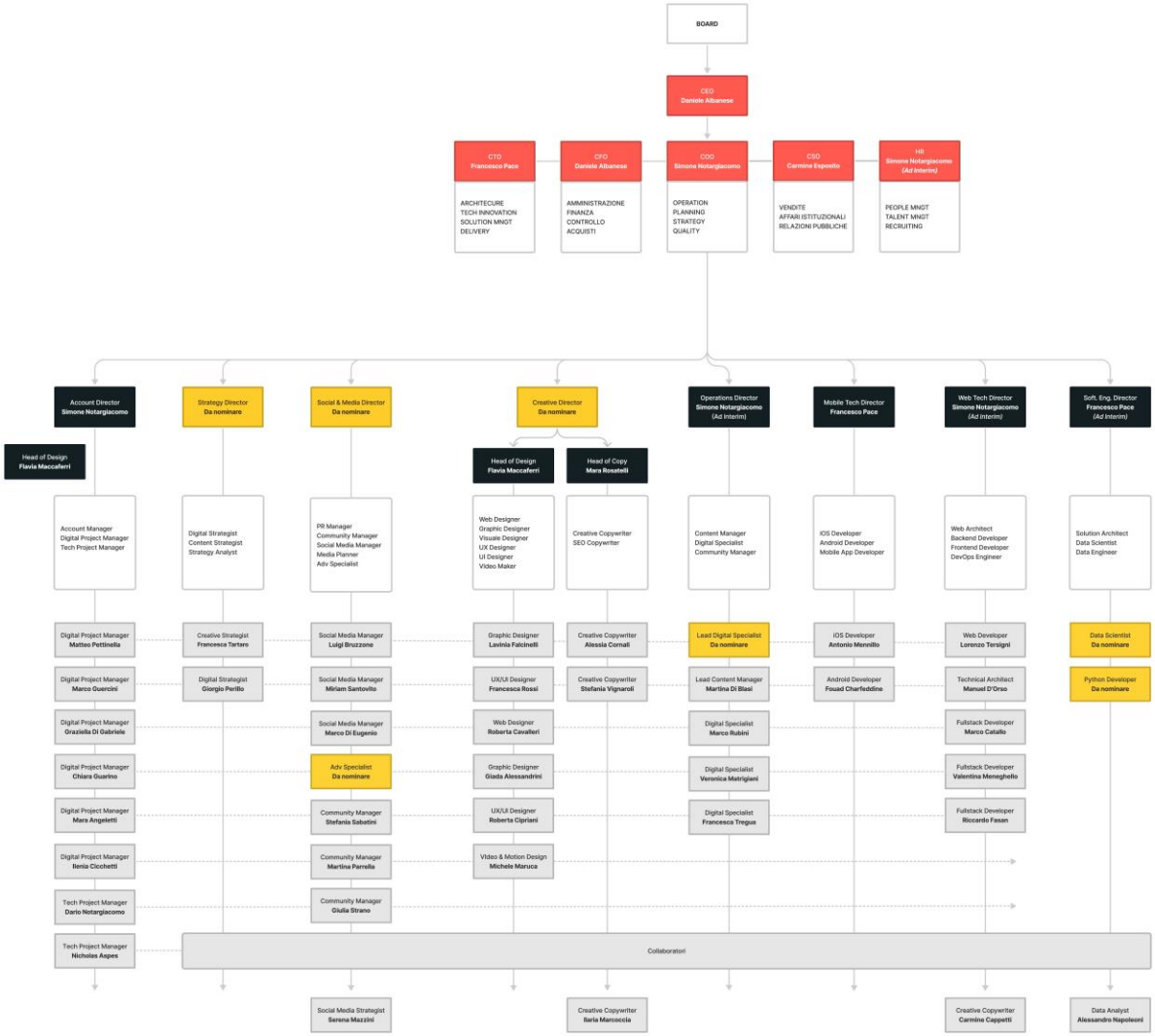

Figura 1- Organigramma aziendale

3.3 MOTIVAZIONI DELLA JUSTBIT NELL'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Justbit, al fine di assicurare condizioni di correttezza e di trasparenza nella conduzione delle proprie attività, ha ritenuto opportuno procedere all'adozione di un Modello di Organizzazione Gestione e Controllo in linea con le prescrizioni del Decreto 231/01.

Tale iniziativa, unitamente all'adozione del Codice Etico comportamentale, è stata assunta nella convinzione che l'adozione del Modello - al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio - possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della società e di tutti gli altri soggetti alla

stessa cointeressati (Fornitori, Partners, Collaboratori a diverso titolo), affinché seguano nell'espletamento delle proprie attività comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.
Inoltre, le quote societarie di Justbit sono in maggioranza detenute da una società (EPRcomunicazione S.p.A. Società Benefit), che si è a sua volta dotata di un Modello conforme alle disposizioni del decreto. È convinzione sia dei soci sia degli organi sociali di Justbit, che l'adozione di un modello che sia fondato sui principi etici e comportamentali della suddetta società, e che ne ripercorra la struttura, possa essere la modalità più adeguata di armonizzazione e completa adesione agli stessi principi di legalità, trasparenza e correttezza a livello di gruppo.

Nell'ottica di tale armonizzazione, i principi etici e comportamentali alla base del Modello di Justbit sono da intendersi rivolti anche a soggetti terzi aventi qualsiasi rapporto commerciale e di altro tipo con la società maggioritaria.

3.4 DESTINATARI DEL MODELLO ORGANIZZATIVO

Il presente Modello si applica a tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella società, nonché a tutti i dipendenti di Justbit.

La società che detiene la maggioranza delle quote societarie è a sua volta dotata di un suo Modello, i cui principi etici e comportamentali e protocolli di controllo sono da intendersi internamente armonizzati con il presente Modello di Justbit, in quanto perseguenti le medesime finalità di cui al paragrafo 3.5.

Quanto sopra premesso, sono tenuti al rispetto del modello anche soggetti non legati a un rapporto di subordinazione con Justbit ma che:

- rivestono di fatto e di diritto un ruolo di coordinamento "direttivo" nell'ambito della struttura societaria;
- per delega occupino una posizione di coordinamento "direttivo" nell'ambito della società;

Per quanto riguarda, invece, agenti, professionisti, consulenti e fornitori in genere, trattandosi di soggetti esterni, non sono vincolati al rispetto dei protocolli nel Modello né a questi, in caso di violazione delle regole stesse, può essere applicata una sanzione disciplinare.

Per quanto riguarda, invece, agenti, professionisti, consulenti e fornitori in genere, gli stessi sono tenuti ad aderire a condividere i principi stabiliti nel Codice Etico comportamentale: la società provvederà a notificare o distribuire lo stesso Codice e lo stesso Modello prevedendo ove ritenuto

opportuno nei diversi contratti di collaborazione a titolo di sanzione, specifiche clausole risolutive in caso di violazione delle norme contenute nel citato Codice Etico comportamentale.

3.5 FINALITÀ DEL MODELLO

Il Modello predisposto dalla Justbit si basa su un sistema strutturato ed organico di processi nonché di attività di controllo che nella sostanza:

a) individuano le aree e le attività di possibile rischio nell'attività della società (vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati);

b) definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della Justbit in relazione ai rischi/reati da prevenire tramite:
   - un Codice Etico comportamentale, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività della società assunti dai componenti del CdA, dall'AD e ai soggetti apicali, dai dipendenti, da eventuale partner e collaboratori a vario titolo di Justbit;
   - la presenza di di deleghe e poteri di firma che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;

c) determinano una struttura organizzativa coerente, volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;

d) individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;

e) attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporne l'aggiornamento.

Pertanto, il Modello si propone come finalità quelle di:

- migliorare il sistema organizzativo interno;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività della Justbit, con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto della Justbit nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle

disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti, ma anche nei confronti della Justbit;

- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse della Justbit, che la violazione delle prescrizioni contenute nel Modello potrà comportare l'applicazione di apposite sanzioni, ovvero, nei casi più gravi, la risoluzione del rapporto contrattuale;
- ribadire che Justbit non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui Justbit stessa intende attenersi.
- introdurre un sistema di segnalazione che consenta a coloro che operino a qualsiasi titolo per conto della società di presentare, a tutela dell'integrità della società, segnalazioni circostanziate di condotte illecite, rilevanti e fondate su elementi di fatto precisi e concordanti, o di violazioni del presente modello di organizzazione e gestione, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- garantire inoltre misure idonee a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione, nei limiti in cui l'anonimato e la riservatezza siano opponibili per legge.

Tutte le finalità di cui sopra sono da intendersi come misure di prevenzione e controllo dei rischi di commissione dei reati presupposto previsti dal D. Lgs. 231/2001 non solo a vantaggio di Justbit stessa, ma anche di altre società del gruppo che detengono quote societarie e che detengono o possano detenere, in fatto o in diritto, qualsiasi forma di controllo.

3.6 MODIFICHE ED INTEGRAZIONI DEL MODELLO

Essendo il presente Modello un atto di emanazione dell'organo dirigente (come previsto dall'art. 6, comma 1, lettera a, del Decreto), la sua adozione, così come le sue eventuali successive modifiche ed integrazioni), sono rimesse alla competenza del Consiglio di Amministrazione ("CdA").

In particolare, è demandato dello stesso CdA, su proposta dell'Organismo di Vigilanza, di deliberare l'approvazione dell'integrazione del presente Modello, ovvero di deliberarne l'aggiornamento in conseguenza di introduzione di nuovi reati presupposto potenzialmente applicabili e intervenute modifiche significative nell'organizzazione aziendale o nelle attività svolte dalla società.

3.7 METODOLOGIA SEGUITA NELLA REDAZIONE DEL MODELLO ORGANIZZATIVO DELLA JUSTBIT

Justbit ha avviato all'inizio dell'anno 2024 il primo progetto di analisi e verifica del proprio sistema organizzativo finalizzato alla predisposizione del Modello Organizzativo in conformità alle indicazioni di cui al D.lgs. 231/01.

Il Progetto si è articolato nelle cinque fasi di seguito sinteticamente indicate:

Fasi	Attività
Fase 1	**Analisi preliminare della documentazione aziendale** La prima fase prevede, l'analisi della struttura organizzativa e delle attività gestite da **Justbit** tenendo conto anche della principale documentazione di base (organigramma, processi, ecc.).
Fase 2	**Rilevazione delle aree a rischio di reato** Mappatura delle attività a rischio di commissione di reato 231, ovvero di tutte quelle attività e processi aziendali che potrebbero potenzialmente generare la commissione degli illeciti previsti alla norma. La mappatura è stata realizzata attraverso un ciclo di interviste con i Responsabili delle Funzioni Aziendali, soci e collaboratori.
Fase 3	**Valutazione del sistema di controllo e risk assessment** Tutte le attività identificate come potenzialmente a rischio di reato 231 sono state oggetto di analisi al fine di valutare la presenza di opportuni controlli di processo in grado di mitigare i rischi rilevati.
Fase 4	**Gap Analisys** Analisi comparativa tra i controlli esistenti a presidio delle attività a rischio di reato e gli standard di controllo generali.
Fase 5	**Formalizzazione del Modello di organizzazione gestione e controllo** Definizione del Modello organizzativo ex D.lgs. 231/2001 articolato in tutte le sue componenti e regole di funzionamento, adattato alla realtà della Justbit.

3.8 ELEMENTI COSTITUTIVI DEL MODELLO DELLA JUSTBIT

Il presente Documento di Sintesi del Modello è costituito da una **Parte Generale** e da una **Parte Speciale**.

Nella Parte Generale, dopo aver effettuato una breve ma necessaria illustrazione della *ratio* e dei principi del Decreto, oltre ad una sintetica ricognizione delle previsioni di cui al documento "Disciplina e compiti dell'Organismo di Vigilanza", dedicato alla regolamentazione dell'OdV, pure ivi sinteticamente rappresentato, sono compendiati i principi di controlli sotto indicati, che compongono il Modello della Justbit:

- il sistema organizzativo;

- le deleghe conferite;
- i regolamenti aziendali;
- il Codice Etico comportamentale;
- il Sistema Disciplinare;
- la comunicazione ed il coinvolgimento del personale sul Modello, nonché la sua formazione ed addestramento.

La Parte Speciale è, a sua volta, suddivisa in sedici sezioni:

- Parte Speciale A, relativa ai c.d. reati reati di corruzione, anche tra privati, ed altri reati nei rapporti con la pubblica amministrazione e UE;
- Parte Speciale B, relativa ai c.d. reati informatici;
- Parte Speciale C, relativa ai c.d. reati di criminalità organizzata;
- Parte Speciale D, relativa ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- Parte Speciale E, relativa ai c.d. reati di industria e commercio;
- Parte Speciale F, relativa ai c.d. reati societari;
- Parte Speciale G, relativa ai c.d. reati con finalità di terrorismo e di eversione dell'ordine democratico;
- Parte Speciale H, relativa ai c.d. reati contro la persona individuale, razzismo e xenofobia;
- Parte speciale I, relativa ai c.d. reati in materia di abusi di mercato;
- Parte Speciale L, relativa ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- Parte Speciale M, relativa ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di illecita provenienza nonché autoriciclaggio e trasferimento fraudolento di valori;
- Parte Speciale N, relativa ai c.d. reati in materia di violazione dei diritti d'autore;
- Parte Speciale O, relativa ai c.d. reati di induzione a non rendere o a rendere dichiarazioni mendaci all'Autorità Giudiziaria.
- Parte Speciale P, relativa ai c.d. reati di natura Ambientale;
- Parte speciale Q, relativa al reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare o di favoreggiamento dell'immigrazione clandestina o permanenza di immigrati irregolari;
- Parte speciale R relativa ai reati c.d. tributari.

Nell'ambito delle Parti Speciali, si è provveduto ad indicare:

a) I reati applicabili;

b) le aree ritenute “a rischio reato” e le attività “sensibili’’;
c) i principi di comportamento da rispettare al fine di ridurre il rischio di commissione dei reati;
d) i principi di controllo in essere sulle singole aree a “rischio reato’’ e i richiami a eventuali procedure o prassi operative adottate dalla Justbit che regolamentano lo svolgimento di processi relativi alle suddette aree a rischio.

La presente Parte Generale e le sedici Parti Speciali, sono inoltre accompagnate dai documenti che, rappresentativi di alcuni Protocolli, completano e specificano il quadro della organizzazione, della gestione e del controllo della Justbit, quali il “**Codice Etico/comportamentale”**, il **“Sistema Disciplinare”, il documento “Disciplina e Compiti dell’Organismo di Vigilanza”** precedentemente citato**, le mappature dei rischi di livello 0 e livello 1, la “Matrice di rischio e controlli interni”** identificati come allegati al Modello stesso.

Tali documenti, unitariamente considerati, costituiscono il Modello da Justbit adottato ai sensi del Decreto.

3.9 ADOZIONE, ATTUAZIONE, AGGIORNAMENTO, DIFFUSIONE

Il sistema organizzativo e gestionale della Justbit è mirato a garantire lo svolgimento delle attività aziendali nel rispetto della normativa vigente e delle previsioni del Codice Etico/comportamentale.
Nell’ottica della pianificazione e gestione delle attività aziendali tese all’efficienza, alla correttezza, alla trasparenza ed alla qualità, la società ha adottato ed attua le misure organizzative, di gestione e di controllo descritte nel presente documento, di seguito indicato come Modello.
Per prevenire il rischio di commissione di reati dai quali possa derivare la responsabilità della Società ai sensi del D.lgs. n. 231/2001, il Modello prevede:

1. l’individuazione delle attività nel cui ambito possono essere commessi reati;
2. specifici principi comportamentali e operativi diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
3. l’individuazione di modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
4. obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e sull'osservanza del Modello;
5. l’introduzione un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.
6. Introduzione di un sistema atto a permettere la segnalazione di illeciti o violazioni dei principi dello stesso modello e la tutela assoluta del soggetto segnalatore, contrastando qualsiasi tipo di ritorsione o atto discriminatorio nei confronti dello stesso.

Il Modello è sottoposto a verifica periodica e viene modificato nel caso in cui siano scoperte significative violazioni delle prescrizioni o si verifichino mutamenti dell'organizzazione o delle attività della società, ovvero delle norme di riferimento.
Il Modello e i suoi aggiornamenti vengono approvati tramite delibera del CdA, che ne autorizza in tal modo l'adozione e la diffusione. La revisione di un allegato al Modello (es. il codice Etico comportamentale) o di una procedura, Regolamento o protocollo richiamato nel Modello stesso può essere approvata singolarmente, purché nella delibera di approvazione si confermi la valenza della versione del Modello vigente.
È fatto obbligo a chiunque operi nella società o collabori con essa a qualsiasi titolo di attenersi alle pertinenti prescrizioni del Modello, ed in specie di osservare gli obblighi informativi dettati per consentire il controllo della conformità dell'operato alle prescrizioni stesse.
Copia del Modello, dei documenti ad esso allegati e dei suoi aggiornamenti è presente presso una cartella condivisa della società ed è a disposizione di chiunque abbia titolo a consultarla.
Inoltre, sono pubblicati sul sito internet della società in area accessibile a tutti gli stakeholder il modello organizzativo (parte generale e parti speciali) e il codice etico/comportamentale.
La società provvede a notificare e informare ciascun soggetto interno tenuto a rispettare il Modello le pertinenti prescrizioni riferite alla specifica attività o funzione.

3.10 PROCESSI SENSIBILI RELATIVI ALLE AREE A RISCHIO

Sono individuati i seguenti processi e relative attività sensibili, comuni allo svolgimento delle attività della Justbit nelle aree o settori funzionali di cui al precedente paragrafo:

ID	Processo	Aree sensibili
P01	Processo commerciale	Scouting, gestione delle partnership, partecipazione alle gare, Elaborazione delle offerte a clienti pubblici e privati e preparazione della documentazione, riesame delle offerte, Costituzione di consorzi e ATI, stipula contratti, richiesta di finanziamenti

ID	Processo	Aree sensibili
P02	Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Predisposizione e trasmissione della documentazione inerente agli adempimenti/accertamenti/ispezioni di natura fiscale e contributiva da parte dell'Amministrazione Finanziaria. Predisposizione e trasmissione della documentazione inerente agli adempimenti/accertamenti/ispezioni in merito all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata. Rapporti con Autorità giudiziaria.
P03	Gestione dei contenziosi e recupero crediti	Gestione di contenziosi giudiziali ed extragiudiziali nei confronti di soggetti pubblici e privati, recupero crediti
P04	Gestione delle risorse umane	Selezione e assunzione del personale, gestione delle presenze, delle ferie e dei permessi, pagamento retribuzioni, gestione delle contestazioni disciplinari
P05	Gestione dei sistemi informativi	Gestione e protezione dei dati relativi a clienti pubblici e privati, partner, personale e fornitori, modalità di protezione fisica, gestione delle privacy, utilizzo dei sistemi informativi da parte del personale
P06	Gestione della Salute e Sicurezza sul lavoro (SSL) e dell'Ambiente	Valutazione e gestione dei rischi di SSL, ruoli e responsabilità in ambito di SSL e ambiente, coordinamento e cooperazione per la SSL in caso di affidamenti a persone fisiche e giuridiche, gestione infortuni e malattie professionali, gestione sorveglianza sanitaria, gestione dei rifiuti prodotti presso la sede.

ID	Processo	Aree sensibili
P07	Approvvigionamento	Qualifica e monitoraggio dei fornitori e consulenti, emissione degli ordini di acquisto, tipologia di contratti e incarichi conferiti, gestione delle contestazioni contrattuali
P08	Processo finanziario	Gestione dei flussi finanziari e relative autorizzazioni, gestione dei conti correnti bancari, accesso al credito e richiesta finanziamenti.
P09	Processo amministrativo	Ciclo passivo e contabilità, autorizzazione alla liquidazione delle fatture passive, redazione del bilancio, modalità di redazione e liquidazione delle relazioni fiscali periodiche (IVA e imposte sui redditi)
P10	Processo Societario	Gestione dei rapporti con i soci, Convocazione e verbalizzazione delle assemblee, Operazioni ordinarie e straordinarie
P11	Gestione delle commesse	Rapporti/incontri con i clienti pubblici e privati durante lo svolgimento delle attività, rendicontazione attività, approvazione interna ed esterna degli output di commessa, Emissione SAL attivi e Ordini di Vendita, gestione fatturazione e incassi.

3.11 PRINCIPI PER LA FORMAZIONE E L'ATTUAZIONE DELLE DECISIONI

In ragione della struttura organizzativa della Justbit, il sistema di deleghe di poteri e funzioni adottato, prevede che la totalità dei poteri decisionali sia concentrata nel vertice aziendale, rappresentato dal CdA, che ha delegato un soggetto apicale (Amministratore delegato, di seguito "AD") tutti i compiti amministrativi ad eccezione delle materie di cui all'art 2381 del Codice civile.
Con riferimento alle attività relative ai processi sensibili espressamente individuate, il Modello (Parti Speciali) prevede infatti specifici principi di controllo contenenti la descrizione formalizzata o i riferimenti:

1. dei processi interni per l'assunzione e l'attuazione delle decisioni di gestione (incluso il normale svolgimento delle relative attività), con l'indicazione delle modalità relative e dei soggetti titolari delle funzioni, competenze e responsabilità;
2. delle modalità di documentazione, e di conservazione, degli atti delle procedure, in modo da assicurare trasparenza e verificabilità delle stesse;
3. delle modalità di controllo della conformità tra i processi previsti e la loro attuazione e documentazione.

I principi di controllo assicurano la separazione e l'indipendenza gerarchica tra chi elabora la decisione, chi la attua e chi è tenuto a svolgere i controlli.

Sono stabiliti limiti all'autonomia decisionale per l'impiego delle risorse finanziarie, mediante definizione di più passaggi autorizzativi in coerenza con le competenze gestionali e le responsabilità organizzative affidate a singole persone.

Il superamento dei limiti quantitativi di cui al punto precedente può avere luogo nel rispetto delle procedure di autorizzazione e di rappresentanza stabilite, sempre assicurando separazione e indipendenza gerarchica tra coloro che autorizzano la spesa, coloro che la devono attuare e coloro ai quali sono affidati i controlli.

Deroghe ai principi di controllo previsti nel Modello sono ammesse in caso di assoluta emergenza o di impossibilità temporanea di attuazione delle stesse. La deroga, con l'espressa indicazione della sua ragione, è immediatamente comunicata all'Organismo di Vigilanza.

I principi di controllo ed eventuali protocolli/regolamenti/procedure di riferimento sono aggiornati anche su proposta o segnalazione dell'Organismo di Vigilanza.

3.12 MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE

Con riferimento alle attività relative ai processi sensibili espressamente individuate, il Modello (Parte Speciale) prevede specifiche modalità di gestione delle risorse finanziarie.

Le modalità di gestione assicurano la separazione e l'indipendenza tra i soggetti che concorrono a formare le decisioni di impiego delle risorse finanziarie, coloro che attuano tali decisioni e coloro ai quali sono affidati i controlli circa l'impiego delle risorse finanziarie.

Tutte le operazioni che comportano utilizzazione o impegno di risorse economiche o finanziarie devono avere adeguata causale ed essere documentate e registrate, con mezzi manuali o informatici, in conformità a principi di correttezza professionale e contabile; il relativo processo decisionale deve essere verificabile.

Tutte le operazioni inerenti ad attività o prestazioni atipiche o inusuali devono essere specificamente e chiaramente motivate e comunicate all'Organismo di Vigilanza.

Le modalità di gestione sono aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza.

3.13 MODALITÀ DI GESTIONE DELLE SCRITTURE CONTABILI E DELLE DICHIARAZIONI FISCALI PERIODICHE

Justbit ha previsto la redazione di una parte speciale del modello dove sono indicate le modalità gestionali poste in essere al fine di prevenire la commissione di irregolarità che possono comportare la commissione di reati di tipo tributario. Il controllo completamente informatizzato del processo di gestione delle scritture contabili attive e passive e le modalità di redazione delle relazioni fiscali periodiche e dei controlli ad esse afferenti, costituiscono gli elementi fondamentali dei protocolli/procedure contenuti o richiamati nella stessa parte speciale.

3.14 OBBLIGHI DI INFORMAZIONE

Il Modello prevede, per le attività relative ai processi sensibili espressamente individuate, specifici obblighi di informazione nei confronti dell'Organismo di Vigilanza.
In ogni caso l'OdV ha accesso a tutta la documentazione relativa ai processi sensibili indicati al punto 3.10 (Processi sensibili relativi alle aree a rischio).
È assicurata piena libertà a tutto il personale della Justbit di rivolgersi direttamente all'OdV o ad utilizzare i canali di predefiniti per segnalare violazioni del Modello o eventuali irregolarità.

4 ORGANISMO DI VIGILANZA

4.1 IDENTIFICAZIONE DELL'ORGANISMO DI VIGILANZA

Nel presente paragrafo 4.1 e nei successivi paragrafi 4.2, 4.3 e 4.4, viene effettuata una sintetica descrizione del c.d. Organismo di Vigilanza, individuandone la composizione, le funzioni principali, il reporting ed i flussi informativi ad esso destinati.

Per una più approfondita analisi e per una puntuale elencazione dei compiti dell'Organismo, si rimanda al documento "Disciplina e compiti dell'Organismo di Vigilanza", allegato ma parte integrante del Modello 231 di Justbit.

Ciò premesso, l'art. 6, comma 1 lett. b del Decreto, stabilisce come condizione per la concessione dell'esimente dalla responsabilità amministrativa, che sia affidato ad un Organismo dell'Ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei Modelli e di curare il loro aggiornamento.

Tale soggetto monocratico, per Justbit è composto da un soggetto esterno, nominato dal CdA, in possesso di adeguate competenze. La nomina dello stesso soggetto, che avviene attraverso delibera del CdA, è da considerare parte integrante del presente modello.

In fase di prima approvazione del Modello, l'OdV contestualmente incaricato è:

Avv. Massimiliano Rosai – Domicilio: Via Giorgio Morpurgo, 16, 00136 Roma RM.

Email: odv@justbit.it.

4.2 DURATA IN CARICA

La durata dell'incarico dell'OdV è fissata in anni tre, rinnovabili con delibera del CdA. Non è previsto un soggetto supplente. In caso di impossibilità di prosecuzione della collaborazione con il soggetto nominato si procederà direttamente a nuova nomina. L'OdV resta in carica fino alla nomina del nuovo OdV (prorogatio).

Il soggetto a cui è stato attribuito tale compito deve godere dei requisiti di:

- Autonomia e indipendenza
  Pur essendo rappresentato da un soggetto esterno, l'Organismo viene inserito come unità Staff in una posizione gerarchica la più elevata possibile, e prevedendo un'attività di reporting al vertice di Justbit, ovvero all'Organo con funzioni di supervisione strategica e di gestione.
  Tali requisiti sono fondamentali affinché l'Organismo non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo.
- Professionalità
  Il componente dell'Organismo prescelto è dotato delle conoscenze tecniche e giuridiche necessarie allo svolgimento del compito assegnato. Tali caratteristiche con l'indipendenza garantiscono l'obiettività di giudizio.
- Continuità d'azione
  La presenza dell'Organismo deve essere costante al fine di poter garantire un'efficace e continua applicazione del Modello.

Al fine di attuare quanto previsto dal Decreto, il CdA della Justbit ha individuato il soggetto più idoneo al quale attribuire detto compito e quindi a svolgere le funzioni dell'Organismo di Vigilanza.

In considerazione delle peculiarità delle proprie attribuzioni e dei contenuti professionali specifici da esse richiesti, l'Organismo di Vigilanza, nello svolgimento dei propri compiti, deve potersi

avvalere di altre funzioni della Justbit che, di volta in volta, si potranno rendere utili allo svolgimento delle attività da porre in essere.

4.3 FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA

All'Organismo è affidato sul piano generale il compito di vigilare:

a) sull'effettività del Modello, ossia sull'osservanza delle prescrizioni dello stesso da parte dei destinatari individuati in relazione alle diverse tipologie di reati contemplate dal Decreto;

b) sulla reale efficacia ed adeguatezza del Modello ossia sulla capacità, in relazione alla struttura della Justbit, di prevenire la commissione dei reati di cui al Decreto;

c) sul mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello;

d) sull'aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni di Justbit. Tale attività, di norma, si realizza in due momenti distinti ed integrati:
    a. presentazione di proposte di adeguamento del Modello verso gli organi/direzioni/funzioni di Justbit in grado di dare loro concreta attuazione. A seconda della tipologia e della portata degli interventi le proposte sono presentate alle funzioni interessate, e nei casi di particolare rilevanza, all'Organo con funzioni di supervisione strategica e di gestione;
    b. follow up, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

Sul piano più operativo sono affidati all'OdV i seguenti compiti:

- attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata alle Unità Operative e di Supporto;
- condurre ricognizioni dell'attività della Justbit ai fini della mappatura aggiornata delle aree di attività a rischio;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di attività a rischio;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso, contenente le istruzioni, chiarimenti o aggiornamenti;

- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere allo stesso Organismo obbligatoriamente trasmesse o tenute a sua disposizione;
- coordinarsi con le altre funzioni/unità di business di Justbit (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree a rischio. A tal fine l'Organismo viene tenuto costantemente informato sull'evoluzione delle attività delle suddette aree a rischio ed ha libero accesso a tutta la documentazione rilevante della Justbit. All'Organismo devono essere inoltre segnalate da parte delle varie Funzioni eventuali situazioni dell'attività che possono esporre Justbit al rischio di reato;
- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto per le diverse tipologie di reati. In particolare, all'Organismo devono essere segnalate le attività più significative e devono essere messi a sua disposizione i dati di aggiornamento della documentazione, al fine di consentire l'effettuazione dei controlli;
- coordinare le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del Modello eventualmente segnalate tramite i canali predisposti;
- verificare che gli elementi previsti per le diverse tipologie di reati (espletamento di procedure, adozione delle clausole standard ecc. siano adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, ad un aggiornamento degli elementi stessi;
- coordinarsi con i Responsabili delle varie unità organizzative per i diversi aspetti attinenti all'attuazione del Modello (definizione delle clausole standard dei contratti e delle lettere di assunzione, formazione del personale, provvedimenti disciplinari).

4.4 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

4.4.1 Segnalazioni da parte degli esponenti di Justbit e da parte di terzi

Nell'ambito dell'attività della Justbit deve essere portata a conoscenza dell'Organismo, oltre la documentazione prescritta dal Modello, ogni altra informazione di qualsiasi tipo proveniente anche da terzi e attinente all'attuazione del Modello nelle aree di attività a rischio ed all'osservanza di quanto previsto nel Codice Etico/comportamentale.

A tal proposito, sono raccolte eventuali segnalazioni relative alla commissione di reati previsti dal Decreto in relazione all'attività della Justbit o comunque comportamenti non in linea con le regole di condotta adottate da Justbit e/o previste dal Codice Etico comportamentale. Le segnalazioni vengono effettuate attraverso i canali istituiti internamente.

4.5 WHISTLEBOWLING

Il Legislatore ha approvato il D.lgs. 10 marzo 2023, n. 24 recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (c.d. “Decreto Whistleblowing”), il quale ha definito:

- gli illeciti oggetto di possibile segnalazione;
- i possibili soggetti segnalanti;
- gli obblighi degli Enti in termini di non discriminazione dei segnalanti e tutela della riservatezza degli stessi;
- i provvedimenti della società che possono essere inquadrati come atti ritorsivi;
- la necessità della presenza di uno o più canali interni (anche con modalità informatiche) che consentano ai soggetti segnalanti di presentare le segnalazioni garantendo la riservatezza dell’identità del segnalante;
- il divieto di atti di ritorsione o discriminatori nei confronti del segnalante per motivi collegati alla segnalazione;
- la necessità di prevedere nel sistema disciplinare sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.
- gli aspetti di tutela del dipendente che effettua una segnalazione;
- la possibilità di inoltrare segnalazioni esterne, in specifici casi.

Tra gli illeciti oggetto di possibile segnalazione rientrano le seguenti fattispecie:

- Illeciti che rientrano nell’ambito di applicazione degli atti dell’Unione europea o nazionali indicati nell’allegato al D. Lgs. 10 marzo 2023, n. 24 ovvero degli atti nazionali che costituiscono attuazione degli atti dell’Unione europea indicati nell’allegato alla direttiva (UE) 2019/1937, seppur non indicati nel suddetto allegato, relativi a settori specifici quali: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell’ambiente; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;

- atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
- atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati punti precedenti.
- azioni che possano essere penalmente rilevanti;
- azioni che possano rappresentare violazioni del codice etico comportamentale di Justbit;
- violazione di quanto prescritto dal Modello;
- azioni che possano arrecare un pregiudizio all'immagine di Justbit;
- azioni vessatorie, discriminatorie, di emarginazione, di molestia nei confronti di colleghi, dirigenti o altri soggetti operanti per conto di Justbit;
- comportamenti minacciosi o violenti;
- azioni di istigazione all'odio razziale o alla xenofobia;
- azioni capaci di arrecare un danno patrimoniale a Justbit;
- azioni che possano costituire un pericolo rilevante per la Salute e Sicurezza sul lavoro e per l'Ambiente.

A seguito dell'approvazione del Modello da parte del CdA, Justbit, contestualmente:

- istituisce un canale di segnalazione interna conforme alle disposizioni del decreto;
- nomina l'OdV quale soggetto esterno indipendentemente quale responsabile della gestione del canale;
- informa i possibili soggetti segnalanti delle modalità implementate per la gestione delle stesse segnalazioni.

Quanto sopra è stato regolamentato in una specifica procedura ("**Procedura per la gestione delle segnalazioni- "Whistlebowling")** approvata da Consiglio di Amministrazione e che è da considerare parte integrante del presente Modello.

4.4.2 Obblighi di informativa relativi ad atti ufficiali e alle dichiarazioni periodiche

È obbligo trasmettere all'Organismo le informative concernenti:

- i verbali delle riunioni assembleari dei soci e del CdA;
- i 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 i reati di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli organizzativi, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con la relativa motivazione;
- le segnalazioni pervenute su comportamenti illeciti e stato di attuazioni delle azioni disciplinari messe in atto.

Uleriori elementi dei flussi informativi periodici e ad evento sono riportati nel documento "Regolamento dell'OdV" allegato al presente Modello.

Periodicamente l'Organismo propone al CdA eventuali modifiche della lista sopra indicata.

4.6 REPORTING DELL'ORGANISMO DI VIGILANZA NEI CONFRONTI DEGLI ORGANI SOCIETARI

All'Organismo sono assegnate due linee di reporting:

- la prima su base continuativa direttamente con AD;
- la seconda, su base almeno annuale, nei confronti del CdA.

L'Organismo può essere convocato in qualsiasi momento dai suddetti organi o può, a sua volta, presentare richiesta in tal senso per riferire in merito al funzionamento del Modello o a situazioni specifiche.

5 IL MODELLO E IL CODICE ETICO COMPORTAMENTALE

5.1 GENERALITÀ

L'adozione di un Codice Etico comportamentale rilevante ai fini di prevenzione dei reati ex D.lgs. 231/2001 costituisce un elemento essenziale del sistema di controllo preventivo.

Le regole di comportamento contenute nel presente Modello, si integrano pertanto con quelle del Codice Etico comportamentale adottato da Justbit, allegato al presente documento e facente parte integrante dello stesso**.**

Il Codice Etico comportamentale è uno strumento adottato in via autonoma da Justbit come espressione dei principi di "deontologia societaria" che Justbit stessa riconosce come propri e sui quali richiama l'osservanza da parte di tutti gli organi sociali, dipendenti, delegati, partner, collaboratori e fornitori.

5.2 FINALITÀ, DESTINATARI E STRUTTURA DEL CODICE ETICO/COMPORTAMENTALE

Il Codice Etico comportamentale diJustbit indica i principi generali e le regole comportamentali che vengono considerati fattori fondamentali nella gestione d'impresa ed a cui devono aderire tutti i Destinatari.

Tali sono tutti i componenti del CdA, tra cui l'AD, ed i soggetti che operano per Justbit, i suoi dipendenti, gli altri soggetti apicali, i partner nonché tutti coloro che, pur esterni alla Justbit, operino, direttamente o indirettamente, per Justbit (collaboratori a qualsiasi titolo, consulenti, fornitori di seguito, indicati quali 'Terzi Destinatari').
I Destinatari sono tenuti ad osservare e, per quanto di propria competenza, a fare osservare i principi contenuti nel Modello e nel Codice Etico/comportamentale che ne è parte.

Il complesso delle regole contenute nel Codice Etico/comportamentale, peraltro, uniformando i comportamenti della Justbit a standard etici ed improntati alla massima correttezza e trasparenza, garantisce la possibilità di salvaguardare gli interessi degli *stakeholders*, nonché di preservare l'immagine e la reputazione della Justbit, assicurando nel contempo un approccio etico al mercato, con riguardo alle attività svolte nell'ambito del territorio italiano.

Il Codice Etico/comportamentale, in via del tutto sintetica, tratta i seguenti argomenti:

- individuazione dei principi etici e dei valori di riferimento;
- norme di comportamento nei rapporti interni a Justbit;
- norme di comportamento nei rapporti con i soggetti terzi;
- modalità di attuazione e controllo del rispetto del Codice Etico comportamentale.

6 FORMAZIONE DEL PERSONALE, DIFFUSIONE E CONDIVISIONE DEL MODELLO

6.1 FORMAZIONE DEL PERSONALE

Justbit promuove la conoscenza del Modello e dei suoi aggiornamenti tra tutti gli organi sociali, i dipendenti, partner e collaboratori che, pertanto, sono tenuti a conoscerne il contenuto, ad osservarlo ed a contribuire alla loro attuazione.

La formazione del personale ai fini dell'attuazione del Modello è articolata sui livelli di seguito indicati:

1. Amministratori, Responsabili e soggetti e con funzioni di o coordinamento di risorse della Justbit: informazione iniziale estesa di volta in volta a tutti i neo assunti; seminario di aggiornamento annuale; occasionali e-mail di aggiornamento; informativa nella lettera di assunzione per i neo assunti o clausola specifica nell'incarico, nei contratti o negli ordini di fornitori, consulenti e collaboratori;
2. Altro personale: nota informativa interna; informativa nella lettera di assunzione per i neo assunti; e-mail di aggiornamento.

Su proposta dell'OdV possono essere istituiti nell'ambito della Justbit, con decisione dell'AD, appositi sistemi di valutazione per la selezione di collaboratori esterni nonché di partner destinati a cooperare con Justbit nell'espletamento delle attività a rischio.

6.2 DICHIARAZIONI E CLAUSOLE CONTRATTUALI EX. D.LGS. 231/2001

6.2.1 Personale neoassunto

Le lettere di assunzione del personale dovranno contenere una dichiarazione con cui i neo assunti prendono atto delle previsioni del D. Lgs. 231/01 e dell'informativa data loro dalla Justbit. Un esempio di dichiarazione di questo tipo viene di seguito esposta:

"Il/La sottoscritto/a dichiara di conoscere e di aver preso atto delle previsioni di cui al D. Lgs. 231/01 e successive modifiche ed integrazioni. Il/La sottoscritto/a è consapevole che tale Decreto prevede la responsabilità diretta della società per i reati commessi, tra gli altri, dai suoi dipendenti, in aggiunta alla responsabilità della persona fisica che ha realizzato materialmente il fatto.

L'inosservanza da parte del dipendente di una qualsiasi delle previsioni della normativa così sommariamente esposta, ed in particolare la commissione da parte di questo di alcuno dei fatti criminosi previsti dalla normativa italiana come presupposto per la responsabilità diretta dell'ente, comporta le conseguenze previste nel Modello di Organizzazione, Gestione e Controllo adottato e

legittimerà la stessa a prendere le dovute misure sanzionatorie come specificato nel documento descrittivo del sistema sanzionatorio."

Il sottoscritto dichiara altresì di essere a conoscenza dell'implementazione da parte Justbit di procedura per la gestione delle segnalazioni "Whistlebowling" e dell'istituzione del canale interno presente in apposita sezione "Whistlebowling" del sito internet aziendale, secondo quanto previsto dal D. Lgs, 10 marzo 2023, n. 24.

Tutto ciò premesso, Il/La sottoscritto/a dichiara altresì di aver compreso il contenuto del Modello e relativi allegati e del Decreto e di impegnarsi a tenere un comportamento conforme alle prescrizioni in essi contenute."

6.2.2 Collaboratori esterni, partner, fornitori e potenziali clienti di servizi

Justbit promuove la conoscenza e l'osservanza del Modello anche tra i soggetti terzi con i quali potrebbe venire in contatto nell'espletamento della propria attività (ad es. professionisti, fornitori, consulenti, collaboratori a vario titolo, ecc.).

Pertanto, a questi verranno pertanto fornite apposite informative sui principi, sulle politiche e sulle procedure che Justbit ha adottato sulla base del presente Modello.

Qualunque contratto che crei una partnership o dia luogo ad operazioni simili con altre persone fisiche e giuridiche (Partner) o a contratti di consulenza, fornitura e altri contratti simili con società o persona fisica (Collaboratori Esterni), potrà contenere dichiarazioni e garanzie ad hoc ai fini del D.Lgs. 231/2001 che tutelino Justbit dai rischi e responsabilità connesse. Un esempio di clausola-base di questo tipo viene di seguito esposta, con la precisazione che la stessa potrà essere adattata adattata allo specifico rapporto contrattuale:

Collaboratori esterni

"Il sottoscritto dichiara di essere a conoscenza dell'adozione, da parte di Justibit S.r,l., di un modello di organizzazione, gestione e controllo ai sensi del D. Lgs.231/2001 e si impegna a tenere un comportamento conforme alle previsioni in esso contenute e nel codice Etico comportamentale ad esso allegato. L'inosservanza da parte del sottoscritto di una qualsiasi delle previsioni del predetto Decreto potrà costituire un inadempimento grave degli obblighi di cui al presente contratto e legittimerà Justbit S.r,l. a risolvere lo stesso con effetto immediato, ai sensi e per gli effetti di cui all'articolo 1456 c.c., fermo restando il risarcimento dei danni eventualmente causati a Justbit quali, a mero titolo esemplificativo e non tassativo, quelli derivanti dall'applicazione alla stessa delle sanzioni previste dal citato Decreto".

Il sottoscritto dichiara altresì di essere a conoscenza dell'implementazione da parte di Justbit di procedura per la gestione delle segnalazioni "Whistlebowling" e dell'istituzione del canale interno

presente in apposita sezione "Whistlebowling" del sito internet aziendale, secondo quanto previsto dal D.Lgs, D.lgs. 10 marzo 2023, n. 24".

Partner

"Le Parti dichiarano di conoscere il contenuto del D. Lgs.231/2001 adottato da Justbit S.r,l. e si impegnano reciprocamente ad improntare i rispettivi comportamenti, finalizzati all'attuazione dell'operazione in comune, a principi di trasparenza e correttezza e alla più stretta osservanza del Decreto, dichiarando altresì di non essere sino ad ora mai incorse nella commissione di uno dei reati nello stesso contemplati. L'inosservanza da parte del Partner di una qualsiasi delle previsioni del predetto Decreto comporterà un inadempimento grave degli obblighi di cui al presente contratto e legittimerà Justbit S.r,l. a risolvere lo stesso con effetto immediato, ai sensi e per gli effetti di cui all'articolo 1456 Cod. Civ., fermo restando il risarcimento dei danni eventualmente causati alla Justbit quali, a mero titolo esemplificativo e non tassativo, quelli derivanti dell'applicazione alla stessa delle sanzioni previste dal citato Decreto".

Le parti dichiarano di essere a conoscenza dell'implementazione da parte Justbit S.r,l. di procedura per la gestione delle segnalazioni "Whistlebowling" e dell'istituzione del canale interno presente in apposita sezione "Whistlebowling" del sito internet aziendale, secondo quanto previsto dal D.Lgs, D.lgs. 10 marzo 2023, n. 24.

6.2.3 Fornitori

In fase qualifica, preventiva all'emissione dell'OdA o di stipula del contratto, il fornitore deve esplicitamente accettare le seguenti clausole:

Il [Fornitore]:

a) *dichiara di essere a conoscenza che Justbit S,r,l. ha adottato un Modello di organizzazione gestione e controllo e un Codice Etico comportamentale concernenti l'applicazione del D.Lgs. n.231/2001 consultabili nella apposita sezione del Sito internet aziendale;*

b) *dichiara di essere a conoscenza dell'implementazione da parte Justbit di procedura per la gestione delle segnalazioni "Whistlebowling" e dell'istituzione del canale interno presente in apposita sezione "Segnalazioni" del sito internet aziendale, secondo quanto previsto dal D. Lgs, D.lgs. 10 marzo 2023, n. 24;*

c) *si impegna - anche per i propri eventuali lavoratori somministrati e collaboratori che vengano in contatto con Justbit nell'esecuzione degli incarichi ad esso conferiti - a conformarsi ai principi etici e comportamentali di cui al Modello, per quanto ad esso applicabili e ad informare tempestivamente l'Organismo di Vigilanza della Justbit con*

propria comunicazione di qualsiasi atto, fatto o comportamento di cui esso [Fornitore] venga a conoscenza nell'esecuzione degli incarichi conferiti, che possa integrare la fattispecie di uno degli illeciti penali inclusi nell'ambito di applicazione del D.lgs. n. 231/2001 e comportare la responsabilità amministrativa di Justbit;

d) *laddove esso [Fornitore] abbia adottato un modello di cui al D.lgs. n. 231/2001, dichiara di aver posto in essere i necessari adempimenti e cautele finalizzati alla prevenzione degli illeciti inclusi nell'ambito di applicazione del D.Lgs. n. 231/2001, avendo dotato la propria struttura aziendale di procedure interne e sistemi di organizzazione, gestione e controllo del tutto adeguati e conformi alle previsioni di legge in tema di responsabilità amministrativa degli enti;*

e) *dichiara di essere consapevole che la violazione dell'impegno di cui alla lettera (c) che precede ovvero la non veridicità delle dichiarazioni di cui alla lettera (d) che precede nonché la commissione e/o il concreto tentativo di commissione di uno degli illeciti penali inclusi nell'ambito di applicazione del D.Lgs. n. 231/2001, posto in essere da lavoratori subordinati, somministrati o collaboratori di esso [Fornitore] che vengano in contatto con Justbit S.r.l. ai fini dell'esecuzione degli incarichi di cui al presente Contratto, potrebbe costituire a tutti gli effetti grave inadempimento da parte di [Fornitore] ai sensi e per gli effetti dell'art. 1455 cod. civ.*

6.2.4 Offerte commerciali per la fornitura di servizi

In fase di proposta di servizi a clienti pubblici e privati, può essere inserita nei documenti di offerta la seguente informativa:

Informiamo la [nome azienda] che Justbit ha adottato ed attua un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire i reati previsti dal D.lgs. 231/01. Tale modello è comprensivo di un codice etico comportamentale che risponde all'esigenza di prevenire la commissione di particolari tipologie di reato e predispone principi etici e regole di comportamento. Il modello di organizzazione, gestione e controllo con il relativo codice etico comportamentale sono consultabili nella sezione dedicata del sito internet aziendale

Justbit ha istituito un organismo di vigilanza (OdV) avente il compito di vigilare sul funzionamento del modello ed al quale vanno segnalati eventuali comportamenti non coerenti con quanto indicato nel Modello e nel codice etico comportamentale. I contatti dell'OdV sono disponibili sul sito internet della Justbit

Justbit adotta inoltre specifica procedura per la gestione delle segnalazioni "Whistlebowling" e ha istituito il canale interno presente in apposita sezione "Whistlebowling" del sito internet aziendale, secondo quanto previsto dal D.Lgs, D.lgs. 10 marzo 2023, n. 24.

6.3 DIFFUSIONE DEL MODELLO

Justbit promuove la più ampia divulgazione, all'interno ed all'esterno della società, dei principi e delle previsioni contenute nel Modello e dei principi di controllo ad esso connessi.

Una copia cartacea del Modello viene conservata dall'Amministratore delegato. La delibera di approvazione da parte del CdA viene conservata dallo stesso.

Il Modello approvato è comunicato formalmente a tutti i soggetti apicali, ai partner, ai deegati e al personale della Justbit mediante messa a disposizione su cartella condivisa di copia integrale, su supporto informatico o in via telematica.

Della eseguita notifica della messa a disposizione di copia informatica del modello e dell'impegno da parte dei Destinatari al rispetto delle regole ivi previste, viene conservata traccia documentale da parte della società.

Il Modello e il Codice Etico comportamentale, una volta approvati, sono pubblicati sul sito internet della società, in area di libero accesso da parte di tutti gli stakeholder, in apposita sezione accessibile da tutte le pagine del sito.

7 VERIFICHE PERIODICHE

Il presente Modello è soggetto a due differenti tipologie di verifiche:

- **Verifiche sugli atti**: periodicamente si procede ad una verifica dei principali atti della Justbit nelle aree a rischio di reato; tali verifiche vengono effettuate principalmente dall'OdV, secondo la periodicità e le modalità dallo stesso definite e a sua completa discrezione;
- **Verifiche dell'applicazione delle regole comportamentali e dei principi di controllo:** periodicamente (di norma con periodicità annuale) si procede alla verifica dell'effettivo funzionamento del presente Modello con le modalità stabilite nelle parti speciali e nei corrispondenti principi di controllo ed eventuali regolamenti in essi richiamati (principalmente attraverso l'esecuzione di audit interni sulle aree a rischio reato).

  All'esito della verifica viene redatto un rapporto che evidenzi le possibili manchevolezze e che suggerisca le eventuali azioni da intraprendere. Tale rapporto viene sottoposto

all'attenzione dell'AD (che a sua volta lo porta all'attenzione del Cda alla prima riunione utile) e dell'OdV.

8 IL SISTEMA DISCIPLINARE DI JUSTBIT

Di seguito viene sintetizzato il Sistema Disciplinare di Justbit fermo restando che per la relativa completa disciplina si rimanda al documento nella sua interezza, allegato e parte integrante del Modello.

In ossequio alle disposizioni del Decreto, Justbit si è dotata di un Sistema Disciplinare che, oltre ad essere consegnato, anche per via telematica o su supporto informatico, ai soggetti in posizione apicale, ai dipendenti, ai partner e ai collaboratori è pubblicato in una cartella condivisa aziendale affinché ne sia garantita la piena conoscenza da parte di tutti i Destinatari.

Il Sistema Disciplinare della Justbit si articola in quattro sezioni.

Nella prima, sono indicati i soggetti passibili delle sanzioni previste, suddivisi in sei differenti categorie:

1. Gli Amministratori della società;
2. gli altri soggetti in posizione "apicale", indipendentemente dalla natura del rapporto lavorativo;
3. i dipendenti della Justbit;
4. gli altri soggetti tenuti al rispetto del Modello.

Nella seconda, dopo aver evidenziato che costituiscono violazioni del Modello tutte le condotte, commissive o omissive (anche colpose), che siano idonee a ledere l'efficacia dello stesso quale strumento di prevenzione del rischio di commissione dei reati rilevanti ai fini del Decreto, sono indicate le possibili violazioni, suddivise in due differenti categorie, graduate secondo un ordine crescente di gravità:

1. mancato rispetto del Modello, qualora si tratti di violazioni realizzate nell'ambito delle attività "sensibili" di cui alle aree "a rischio reato" identificate nelle Parti Speciali, e sempre che non ricorra una delle condizioni previste nel successivo n. 2;
2. mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto, o comunque sussista il pericolo concreto che sia contestata la responsabilità della Justbit ai sensi del Decreto.

Nella terza, sono indicate, con riguardo ad ognuna delle condotte rilevanti, le sanzioni astrattamente comminabili per ciascuna categoria di soggetti tenuti al rispetto del Modello. Con

precipuo riguardo ai Terzi Destinatari, sono previste apposite sanzioni di natura contrattuale per l'ipotesi di violazione del Modello o i principi di controllo ad esso connessi (ad es. diffida al rispetto del Modello, applicazione di una penale, risoluzione del contratto).

In ogni caso, ai fini dell'applicazione delle sanzioni si deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata, nonché delle seguenti circostanze:

a) la gravità della condotta o dell'evento che quest'ultima ha determinato;
b) la tipologia della violazione;
c) le circostanze nel cui ambito si è sviluppata la condotta;
d) le modalità della condotta.

Ai fini dell'eventuale aggravamento della sanzione, sono inoltre considerati i seguenti elementi:

- l'eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- l'eventuale concorso di più soggetti nella commissione della violazione;
- l'eventuale recidività del suo autore.

Nella quarta, è disciplinato il procedimento di irrogazione ed applicazione della sanzione con riguardo a ciascuna categoria di soggetti destinatari del Sistema Disciplinare, indicando, per ognuna:

- la fase della contestazione della violazione all'interessato;
- la fase di determinazione e di successiva applicazione della sanzione.

Le previsioni contenute nel Sistema Disciplinare non precludono la facoltà dei soggetti destinatari di esercitare tutti i diritti loro riconosciuti da norme di legge o di regolamento, nonché dalla contrattazione collettiva o dai regolamenti aziendali applicabili.

Modello di Organizzazione Gestione e Controllo

Ai sensi del D.lgs. 8 giugno 2001, n. 231

PARTI SPECIALI

PARTE SPECIALE A- REATI DI CORRUZIONE, ANCHE TRA PRIVATI, ED ALTRI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte Speciale "A", si provvede qui di seguito a fornire un elenco dei reati in essa contemplati, nonché una breve esposizione delle possibili modalità di attuazione dei reati indicati negli artt. 24, 25 e 25-ter del D.lgs. 231/01.

I reati contro la Pubblica Amministrazione e quelli in cui vengono lesi gli interessi finanziari dell'Unione Europea hanno come presupposto l'instaurazione di rapporti con soggetti pubblici e/o lo svolgimento di attività concretanti una pubblica funzione o un pubblico servizio.

Con riferimento al reato di corruzione tra privati, si evidenzia che tale reato, pur appartenendo alla categoria dei reati societari, è stato inserito all'interno della presente Parte Speciale al fine di garantire una maggiore uniformità nella trattazione dei fenomeni corruttivi che potrebbero manifestarsi nell'operativa aziendale.

Concussione (art. 317 c.p.)

Il reato si configura nel momento in cui un Pubblico Ufficiale, ovvero un Incaricato di Pubblico Servizio, abusando della relativa posizione, costringano o inducano taluno a dare o promettere indebitamente, anche in favore di un terzo, denaro o altre utilità non dovute.

Peculato (art. 314 comma 1 c.p.) in offesa degli interessi finanziari dell'Unione Europea [9]

L'ipotesi di reato di cui all'art. 314 comma 1 c.p. si configura nel caso un pubblico ufficiale o un incaricato di un pubblico servizio, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria. È escluso pertanto il cosiddetto "peculato d'uso", ossia il caso in cui lo stesso pubblico o ufficiale o incaricato si appropri temporaneamente della cosa e lo restituisca dopo l'utilizzo momentaneo e il caso in cui il fatto venga commesso in offesa di interessi che non siano specificatamente di tipo finanziario e dell'Unione Europea.

Peculato mediante profitto dell'errore altrui (art. 316 c.p.) in offesa degli interessi finanziari dell'Unione Europea[10]

[9] Reato introdotto nell'art. 25 dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

L'ipotesi di reato di cui all'art. 316 c.p. si configura nel caso in cui Il pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceva o ritenga indebitamente, per sé o per un terzo, denaro o altra utilità. È escluso il caso in cui il fatto venga commesso in offesa di interessi che non siano specificatamente di tipo finanziario e dell'Unione Europea.

Costituendo la concussione e il peculato reati propri di soggetti qualificati, la responsabilità di Justbit potrebbe essere contestata nel solo caso di concorso nel reato commesso da un Pubblico Ufficiale, ossia, a titolo esemplificativo nell'ipotesi in cui si compiano atti tali da favorire la realizzazione della condotta prevista e punita dalla legge.

Corruzione per l'esercizio della funzione (art. 318 c.p.)

Il reato si configura allorquando un Pubblico Ufficiale o un Incaricato di Pubblico Servizio ricevano per sé o per altri, in denaro o altra utilità, una retribuzione non dovuta per compiere, o per aver compiuto, un atto del proprio ufficio.

Ai fini della ricorrenza di tale reato è necessario che la promessa di denaro o di altra utilità siano accettate dal Pubblico Ufficiale, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 c.p.. Il delitto di corruzione si differenzia da quello di concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio.

Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)

Il reato si configura allorquando un Pubblico Ufficiale o un Incaricato di Pubblico Servizio ricevano per sé o per altri, in denaro o altra utilità, una retribuzione non dovuta per compiere, o per aver compiuto, un atto contrario ai doveri d'ufficio, ovvero per omettere o ritardare (o per avere omesso o ritardato) un atto del proprio ufficio.

E' necessario che la promessa di denaro o di altra utilità siano accettate dal Pubblico Ufficiale, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 c.p..

Circostanze aggravanti (art. 319-bis)

[10] Reato introdotto nell'art. 25 dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

La pena è aumentata se il fatto di cui all'articolo 319 c.p. ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene, nonché il pagamento o il rimborso di tributi.

Corruzione in atti giudiziari (art. 319-ter c.p.)

Il reato si configura nel caso in cui i fatti di corruzione di cui alle fattispecie che precedono siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

È opportuno evidenziare che nella nozione di Pubblico Ufficiale sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

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

Il reato si configura, salvo che il fatto costituisca più grave reato, nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Costituendo il reato di cui sopra un reato proprio di soggetti qualificati, la responsabilità di Justbit potrebbe essere contestata nel solo caso di concorso nel reato commesso da un Pubblico Ufficiale, ossia, a titolo esemplificativo nell'ipotesi in cui si compiano atti tali da favorire la realizzazione della condotta prevista e punita dalla legge.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)

Le disposizioni previste per il reato di corruzione per un atto contrario ai doveri di ufficio si applicano non solo al Pubblico Ufficiale bensì anche all'Incaricato di Pubblico Servizio. L'Incaricato di Pubblico Servizio, inoltre, soggiacerà alle norme in materia di corruzione per un atto d'ufficio qualora rivesta la qualità di pubblico impiegato.

Per quanto concerne le ipotetiche modalità di attuazione del reato, quindi, si rimanda ai reati di corruzione che hanno preceduto.

I reati di corruzione sopraindicati possono essere realizzati mediante l'erogazione di denaro o la promessa di erogazione di denaro al Pubblico Ufficiale/Incaricato di Pubblico Servizio, la cui provvista derivi:

- dalla creazione di fondi occulti tramite l'emissione di fatture relative ad operazioni inesistenti;

- da rimborsi spese fittizi o per ammontare diverso da quello delle spese effettivamente sostenute anche attraverso consulenti;
- dall'utilizzo delle deleghe di spesa attribuite.

Sotto un diverso profilo, i reati di corruzione possono essere realizzati mediante l'erogazione o la promessa di erogazione al Pubblico Ufficiale/Incaricato di Pubblico Servizio di una qualsiasi altra utilità o retribuzione, quali in via esemplificativa:

- omaggi e, in genere, regalie;
- dazione/conferimento di beni a condizioni più favorevoli rispetto a quelle di mercato;
- assunzione di personale indicato dal Pubblico Ufficiale o Incaricato di Pubblico Servizio;
- raggiungimento di accordi/sottoscrizione di lettere di incarico in favore di persone segnalate dal Pubblico Ufficiale o dall'Incaricato di Pubblico Servizio a condizioni ingiustamente vantaggiose;
- cancellazione immotivata (totale o parziale) di un debito residuo dell'Ente presso cui il Pubblico Ufficiale/Incaricato di Pubblico Servizio presta il suo servizio o di cui è rappresentante nei confronti della società, ecc.

A titolo esemplificativo, nei casi di corruzione per un atto d'ufficio, corruzione per un atto contrario ai doveri d'ufficio e corruzione di persone incaricate di un pubblico servizio, il reato potrebbe essere finalizzato ad ottenere:

- l'aggiudicazione di una gara pubblica;
- un provvedimento autorizzativo;
- ottenere una pronuncia favorevole alla società nell'ambito di un contenzioso.

Pene per il corruttore (art. 321 c.p.)

Le pene stabilite nel primo comma dell'art. 318, nell'art. 319, nell'art. 319-bis, nell'art. 319-ter e nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi da o promette al pubblico ufficiale o all'incaricato di un pubblico servizio denaro o altra utilità.

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

Il reato si configura nel caso in cui, nei confronti di un Pubblico Ufficiale o di un Incaricato di Pubblico Servizio, sia formulata la promessa o l'offerta di una somma di denaro o di un'altra utilità, qualora la promessa o l'offerta non siano accettate e riguardino, in via alternativa:

- il compimento di un atto d'ufficio;
- l'omissione o il ritardo di un atto d'ufficio;
- il compimento di un atto contrario ai doveri d'ufficio.

È, inoltre, penalmente sanzionata anche la condotta del Pubblico Ufficiale (o Incaricato di Pubblico Servizio) che sollecita una promessa o dazione di denaro o altra utilità da parte di un privato per le medesime finalità.

È necessario, inoltre, che la promessa di denaro o di altra utilità non siano accettate dal Pubblico Ufficiale, poiché, in caso contrario, deve ritenersi integrata una delle fattispecie di corruzione previste dagli artt. 318 e 319 c.p.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione, fermo restando che, ai fini della configurabilità della fattispecie in esame, è necessario che l'offerta o la promessa non siano accettate.

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, abuso di ufficio[11] (art. 322 bis c.p.)

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

- ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

[11] Reato introdotto da D. Lgs. n. 156 del 4 Ottobre 2022 Disposizioni correttive e integrative del decreto legislativo 14 luglio 2020, n. 75, di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale.

- a coloro che, nell'ambito di altri Stati membri dell'Unione Europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- 5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;
- 5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;
- 5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali.
- 5- quinquies) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione Europea, quando il fatto offende gli interessi finanziari dell'Unione.

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

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

1) *alle persone indicate nel primo comma del presente articolo;*
2) *a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.*

Abuso d'ufficio in offesa degli interessi finanziari dell'Unione Europea (art. 323 c.p.)[12]

L'ipotesi di reato di cui all'art. 323 c.p. si configura nel caso in cui un pubblico ufficiale o incaricato di pubblico servizio nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto. È escluso il caso in cui il fatto venga

[12] Reato introdotto nell'art. 25 dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

commesso in offesa di interessi che non siano specificatamente di tipo finanziario e dell'Unione Europea.

Costituendo il reato di cui sopra un reato proprio di soggetti qualificati, la responsabilità di Justbit potrebbe essere contestata nel solo caso di concorso nel reato commesso da un Pubblico Ufficiale o incaricato di pubblico servizio, ossia, a titolo esemplificativo nell'ipotesi in cui si compiano atti tali da favorire la realizzazione della condotta prevista e punita dalla legge.

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

Il reato si configura qualora, utilizzando artifici o raggiri ed in tal modo inducendo taluno in errore, si consegua un ingiusto profitto, in danno dello Stato, di altro Ente Pubblico o delle Comunità Europee.

Per 'artificio' o 'raggiro' si intende la simulazione o dissimulazione della realtà, atta ad indurre in errore una persona per effetto della percezione di una falsa apparenza. Il silenzio può integrare la condotta della truffa se attuata in presenza di un obbligo giuridico di comunicazione, anche di carattere extrapenale.

L'atto di disposizione del soggetto indotto in errore può comprendere ogni comportamento dotato di una efficacia in fatto; tale può essere considerata anche la semplice inerzia.

Il 'profitto' si ravvisa anche nella mancata diminuzione del patrimonio, per effetto, ad esempio, del godimento di un bene e, quindi, anche in assenza di un aumento effettivo di ricchezza; può anche non essere di natura patrimoniale, potendo consistere nel soddisfacimento di un interesse di natura morale.

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

Il reato si configura qualora la condotta di truffa sopra descritta sia posta in essere per conseguire indebitamente erogazioni pubbliche[13].

L'elemento qualificante rispetto al precedente reato è costituito dall'oggetto materiale della frode, in quanto per 'erogazione pubblica' si intende ogni attribuzione economica agevolata, erogata da parte dello Stato, di Enti Pubblici o delle Comunità europee.

13 Il D.L. 25 febbraio 2022 n. 13, pubblicato in GU n. 47 del 25 febbraio 2022"Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili" ha ampliato l'oggetto della condotta aggiungendo ai contributi, sovvenzioni e finanziamenti, i "mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate" e rendendo più generica la destinazione di tali erogazioni, non più necessariamente legata alla realizzazione di opere o allo svolgimento di attività di pubblico interesse.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si consegua un finanziamento o un contributo pubblico mediante il compimento di artifici e raggiri, come specificati nel punto precedente.

Malversazione di erogazioni pubbliche (art. 316-bis c.p.)

Il reato si configura nel caso in cui, dopo avere ricevuto sovvenzioni, finanziamenti o contributi[14] da parte dello Stato italiano, di altri enti pubblici o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi di pubblico interesse cui erano destinate. Tenuto conto che il momento di consumazione del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengano destinati alle finalità per cui erano stati erogati.

Frode nelle pubbliche forniture (art. 356 c.p.)[15]

Il reato si configura nel caso in cui, mettendo in atto un comportamento, da parte del privato fornitore, non conforme ai doveri di lealtà e moralità commerciale e di buona fede contrattuale, non si adempie fedelmente a quanto stabilito contrattualmente e si consegna una cosa o un'opera completamente diversa da quella pattuita, o una cosa od opera affetta da vizi o difetti.

Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)

Il reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, per sé o per altri e senza averne diritto, sovvenzioni, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione Europea. In questo caso, non rileva il corretto utilizzo delle erogazioni (come invece previsto dall'art. 316-bis), poiché il reato si concretizza nel momento stesso dell'ottenimento dei finanziamenti in modo indebito. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie dell'art. 640-bis c.p., con riferimenti a quei casi in cui la condotta non integri gli estremi più gravi della truffa ai danni dello Stato.

Frode informatica in danno dello Stato o di altro ente pubblico o dell'Unione Europea (art. 640-ter c.p.)[16]

14 Vedi nota precedente

15 Reato introdotto nell'art. 24 dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

16 Il D. Lgs. n. 150 del 10 Ottobre 2022 "Attuazione della legge 27 Settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari" ha modificato l'ultimo comma con l'esclusione del testo relativo all'Art.21 c.p. n.7 per cui è stata eliminata la previsione della procedibilità d'ufficio quando il danno patrimoniale cagionato è di rilevante gravità.

Il reato si configura nel caso in cui alterando, in qualsiasi modo, il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti o ad esso pertinenti, si ottenga un ingiusto profitto in danno dello Stato o di altro Ente Pubblico.

L'alterazione fraudolenta del sistema può essere la conseguenza di un intervento rivolto sia alla componente meccanica dell'elaboratore, sia al software.

Sono considerate pertinenti ad un sistema informatico, e quindi, rilevanti ai sensi della norma in questione, le informazioni contenute su supporti materiali, nonché i dati ed i programmi contenuti su supporti esterni all'elaboratore (come dischi e nastri magnetici o ottici), che siano destinati ad essere utilizzati in un sistema informatico.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si alteri il funzionamento di un sistema informatico o dei dati in esso contenuti al fine di conseguire di modificare i dati connessi al versamento dei contributi previdenziali.

Corruzione tra privati (art. 2635 c.c.) e istigazione alla corruzione tra privati (art. 2635 bis, comma 1 c.c.)[17]

La l. 6 novembre 2012 n. 190 ha introdotto nel nostro ordinamento una serie di novità finalizzate ad implementare la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione. Tra queste, ai fini del presente Modello, interessa la nuova formulazione dell'art. 2635 c.c., oggi intitolato "Corruzione tra privati".

La norma punisce la condotta degli amministratori, dei direttori generali, del dirigente preposto alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori che, a seguito della dazione o anche solo della promessa di denaro o di altra utilità, per sé o per altri, compiono o omettono atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando un danno alla società.

Sotto il profilo della responsabilità amministrativa degli enti, la l. 190/2012 ha aggiunto la lettera s-bis) all'art. 25 ter del Decreto, che a sua volta richiama il comma 3 del nuovo art. 2365 c.c. Tale disposizione fa riferimento alla sanzione prevista per il corruttore, ossia chi dà o promette denaro o altre utilità. In altre parole, l'unica ipotesi cui è stata estesa la responsabilità amministrativa degli enti è quella della società corruttrice, i cui amministratori, direttori generali, dirigente preposto alla redazione dei documenti contabili societari, sindaci, liquidatori, o soggetti sottoposti alla direzione o alla vigilanza di questi, pongono in essere atti corruttivi.

[17] Reato introdotto nell'art. 25-ter del Decreto 231 dal D.Lgs. 15 marzo 2017, n. 38

Traffico di influenze illecite (art. 346 bis c.p.)

Integra il reato di "traffico di influenze illecite", introdotto dalla Legge 190 del 2012 e riformato dal Decreto Anticorruzione, "chiunque, fuori dei casi di concorso nei reati di cui agli articoli 318, 319, 319-ter e nei reati di corruzione di cui all'articolo 322-bis, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altre utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri, è punito con la pena della reclusione da un anno a quattro anni e sei mesi".

La norma è tesa a punire le condotte di intermediazione di soggetti terzi nell'opera di corruzione tra il corrotto ed il corruttore.

Nel traffico di influenze illecite oneroso, la somma di denaro o il vantaggio patrimoniale vengono promessi o elargiti direttamente all'intermediario, come compenso per la propria attività di intermediazione illecita. Nel traffico di influenze illecite gratuito, invece, la somma di denaro o il vantaggio patrimoniale vengono promessi o corrisposti al mediatore nell'ottica di remunerare il pubblico funzionario. L'intermediario si presenta pertanto solo come un tramite materiale tra il privato e il pubblico funzionario, senza nulla pretendere per l'attività di intermediazione svolta.

Turbata libertà degli incanti (Art.353 c.p.)[18]

L'art. 352 del c.p. testualmente punisce chi, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di Pubbliche Amministrazioni, ovvero ne allontana gli offerenti. Reato che, come esplicitato al comma 3 e pur con un'attenuazione di pena, è integrato anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata.

Il turbamento di una gara si verifica quando la condotta fraudolenta o collusiva abbia anche soltanto potenzialmente influito sulla regolare procedura della gara, essendo irrilevante che si produca effettivamente un'alterazione dei risultati di essa.

Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.) [19]

[18] Reato introdotto dal D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023 "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia personale della magistratura e della pubblica amministrazione"

[19] Vedi nota precedente"

L'art. 352 del c.p. punisce chi, salvo che il fatto costituisca più grave reato, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione. Tale reato riguarda la fase di indizione della gara e, precisamente, quella di approvazione del bando, e punisce il comportamento di coloro che, con la collusione della stazione appaltante, cercano di far redigere bandi di gara che contengono requisiti talmente stringenti da predeterminare la platea dei potenziali concorrenti.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati transnazionali.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati previsti dalla presente parte speciale applicabili a Justbit, sono state individuate le seguenti aree di rischio ed i processi ad esse collegati:

Processi	Attività
P01- Commerciale	Valutazione delle opportunità a partecipare a gare pubbliche
P01- Commerciale	Valutazione delle opportunità a presentare offerta per clienti privati
P11- Gestione della commessa	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società Pubbliche
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Rapporti con le Autorità di controllo, altri organismi di diritto pubblico o enti pubblici nonché il rilascio di informazioni alla P.A

Processi	Attività
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Rapporti con pubblici ufficiali e incaricati di pubblico servizio relativamente sia agli adempimenti fiscali, tributari, previdenziali, ambientali e in materia di salute e sicurezza sui luoghi di lavoro che alle visite ispettive condotte dai funzionari pubblici in tali ambiti
P01- Commerciale	Negoziazione diretta con l'amministrazione pubblica, la stazione appaltante o ente aggiudicatore
P01- Commerciale	Predisposizione della documentazione (tecnica e amministrativa) e riesame dell'offerta
P01- Commerciale	Partecipazione a procedure per l'ottenimento di sovvenzioni, erogazioni, contributi o finanziamenti da parte di enti e organizzazioni pubblici italiani o comunitari e modalità di impiego dei finanziamenti erogati
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Richiesta di provvedimenti amministrativi occasionali, di autorizzazioni, licenze e concessioni per lo svolgimento di attività strumentali a quelle tipiche della Società
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità P03- Gestione di contenziosi giudiziali ed extragiudiziali	Gestione dei rapporti con l'Autorità Giudiziaria, i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale
P01- Commerciale	Gestione delle partnership nelle attività di partecipazione a gare e richiesta finanziamenti (es.: joint venture, anche in forma di ATI, RTI, consorzi, ecc.)
P01- Commerciale P07- Approvvigionamento	Assegnazione, ai fini della partecipazione alle procedure di cui alle attività commerciali di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo
P07- Approvvigionamento P11- Gestione della commessa	Nell'ambito dei contratti con i fornitori, - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento - gestione e segnalazione delle anomalie.
P09- Processo Amministrativo	Stipula ed esecuzione dei contratti, avendo riguardo anche agli aspetti inerenti all'applicazione di penali e le risoluzioni transattive in caso di contestazioni
P01- Commerciale P04- Gestione delle risorse umane	Gestione degli incentivi ai fini del pieno raggiungimento degli obiettivi commerciali
P08- Processo finanziario	Gestione dei conti correnti bancari

Con riferimento al reato di corruzione tra privati (art. 25-ter del D. Lgs. 231/2001), Al fine della valutazione delle possibili aree di rischio per la commissione del reato in esame, si deve anzitutto tenere presente che l'art. 2635 c.c., nonostante sia intitolato "Corruzione tra privati", trova applicazione solamente nei rapporti tra società. La norma infatti punisce le condotte corruttive che arrechino un danno al patrimonio sociale, e punisce pertanto la corruzione solamente nel caso in cui determini appunto un nocumento al patrimonio sociale, e non invece la corruzione in quanto tale.

Ne consegue che le potenziali aree a rischio per la commissione dei reati in questione sono quelle che riguardano i rapporti tra Justbit e le società terze con cui questa entra in contatto nello svolgimento della propria attività aziendale, quali a titolo esemplificativo gli agenti, i concessionari, i fornitori, i consulenti, ecc. Nell'ambito di tali rapporti si potrebbe infatti astrattamente ipotizzare, da parte dei Destinatari, la promessa di una qualche utilità in cambio di prestazioni o servizi a condizioni di maggior favore.

In via di principio, sono da considerarsi a rischio tutte quelle attività aziendali che comportano il relazionarsi, in nome e per conto della Società, e anche in via indiretta o mediata, con società terze nell'ambito di un rapporto di tipo commerciale.

Sono inoltre da considerarsi a rischio tutte quelle attività che, da un lato, potrebbero portare alla creazione dell'utilità che costituisce, in via di estrema semplificazione, il risultato ultimo nonché il fine dell'attività corruttiva. E si tratta quindi di tutte le attività inerenti al c.d. ciclo attivo, quali, a titolo esemplificativo, la definizione del prezzo di offerta di un bene o di un servizio, la definizione delle condizioni e dei termini di pagamento, della scontistica e della definizione di eventuali risoluzioni transattive in caso di contestazioni.

Sotto diverso profilo, sono allo stesso modo da considerarsi a rischio tutte quelle attività attraverso le quali sarebbe possibile costituire la provvista o i fondi necessari per le illecite dazioni o promesse di denaro. Si tratta quindi di tutte le attività relative al c.d. ciclo passivo quali, a titolo esemplificativo, gli acquisti di beni e servizi e l'affidamento di consulenze e altre prestazioni professionali.

Tenendo conto di quanto sopra, in occasione dell'attività di mappatura, sono state pertanto individuate nell'ambito della struttura organizzativa di Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati di corruzione tra privati.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della commissione del reato

di corruzione tra privati, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività
P01- Commerciale	Gestione delle richieste di offerta nell'ambito privatistico
P07- Approvvigionamento P11- Gestione della commessa	Nell'ambito dei contratti con i fornitori, - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento - gestione e segnalazione delle anomalie
P09- Processo Amministrativo	Stipula ed esecuzione dei contratti, avendo riguardo anche agli aspetti inerenti all'applicazione di penali e le risoluzioni transattive in caso di contestazioni
P09- Processo Amministrativo	Processi di ciclo passivo e contabilità
P01- Commerciale P04- Gestione delle risorse umane	Gestione degli incentivi ai fini del pieno raggiungimento degli obiettivi commerciali
P07- Approvvigionamento P11- Gestione della commessa	Richieste di acquisto e selezione del fornitore
P11- Gestione della commessa	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con privati
P11- Gestione della commessa	Gestione delle rendicontazioni delle commesse ai fini dei pagamenti
P07- Approvvigionamento	Valutazione e qualificazione dei fornitori
P07- Approvvigionamento	Pagamento e contabilizzazione

Sono state inoltre identificate altre aree di rischio a rischio che potrebbero assumere carattere strumentale e/o di supporto alla commissione dei reati contemplati dalla presente parte speciale:

Processi	Attività
P04- Gestione delle risorse umane	Ricerca e selezione del personale
P04- Gestione delle risorse umane	Gestione del sistema di incentivazione e sviluppo professionale del personale dipendente
P08- Processo finanziario	Gestione delle risorse finanziarie
P08- Processo finanziario	Recupero dei crediti, nonché le transazioni commerciali remissive a fronte di disservizi o contestazioni
P04- Gestione delle risorse umane	Amministrazione del personale e pagamento delle retribuzioni, gestione dei permessi e delle ferie
P04- Gestione delle risorse umane	Gestione dei rimborsi spese a dipendenti
P04- Gestione delle risorse umane	Gestione delle spese di rappresentanza
P08- Processo finanziario P11- Gestione della commessa	Eventuale conferimento di utilità a titolo gratuito (donazioni, regali, omaggi, ecc.) nei confronti di esponenti pubblici o di altre realtà organizzative private influenti
P10- Processo societario	Determinazioni in materia di compenso degli amministratori, destinazioni degli utili e delle riserve
P08- Processo finanziario	Gestione dei flussi finanziari in uscita
P03- Gestione di contenziosi giudiziali ed extragiudiziali	Gestione dei rapporti con l'Autorità Giudiziaria, i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

Obiettivo della presente Parte speciale è che tutti i Destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei reati previsti nel Decreto ed in particolare sono tenuti a osservare i seguenti principi generali:

- stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività di Justbit, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione;
- instaurazione e mantenimento di qualsiasi rapporto con la Pubblica Amministrazione, stazioni appaltanti e enti aggiudicatori sulla base di criteri di massima correttezza e trasparenza;
- instaurazione e mantenimento di qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari devono in generale conoscere e rispettare tutte le regole e i principi contenuti nel Codice Etico comportamentale ed in ogni altra documentazione relativa al sistema di controllo interno in essere nella società.

La presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nelle specifiche procedure e nei codici comportamentali adottati e condivisi), di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24 e 25 del D.lgs. 231/2001);
- violare i principi di controllo previsti nella presente Parte Speciale;

- attuare comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
- porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito dei suddetti comportamenti (sanciti anche dal Codice Etico comportamentale) è fatto divieto in particolare di:

1 distribuire omaggi al di fuori di quanto previsto dalla prassi aziendale (vale a dire, secondo quanto previsto dal Codice etico comportamentale, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per Justbit[20]. tale divieto è esteso anche nei confronti dei rappresentanti degli operatori economici che partecipano o abbiano espressa intenzione di partecipare a un pubblico incanto di interesse di Justbit, al fine di influenzare la partecipazione dello stesso soggetti e ottenerne un vantaggio nella eventuale procedura di aggiudicazione. Gli omaggi eventualmente consentiti e autorizzati a soggetti non ricoprenti il ruolo di pubblici ufficiali o funzionari si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte), o la brand image di Justbit;

2 accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione, di stazioni appaltanti o enti aggiudicatori che possano determinare le stesse conseguenze previste al precedente punto 1); tale divieto è esteso anche a rappresentanti di operatori economici che partecipino o per cui si sia venuti a conoscenza della volontà di partecipare a una gara pubblica di interesse di Justbit;

3 esercitare qualsiasi forma di coercizione, violenza o minaccia nei confronti di soggetti rappresentanti di soggetti candidati (anche solo potenzialmente) a pubblici incanti di

[20] Per linea di indirizzo aziendale, non sono ammessi conferimenti di regalie o altre utilità a qualsiasi soggetto con cui si sono intrapresi o è possibile che si intraprendano negozi giuridici, indipendentemente se facenti parte del settore pubblico o privato. Tale circostanza vale anche in occasione del periodo natalizio o altri periodi festivi. Eventuali eccezioni devono essere opportunamente motivate e espressamente autorizzate dall'amministratore delegato.

interesse di Justbit, al fine di evitarne la partecipazione, influenzarne l'intenzione di partecipazione o i contenuti delle relative offerte;

4 porre in essere qualsiasi azione finalizzata alla conclusione di accordi con operatori economici partecipanti o potenziali partecipanti a una procedura di pubblico incanto rientrante tra gli interessi commerciali di Justbit, ferme restando la possibilità di conclusione di accordi di partnership opportunamente formalizzati;

5 nel caso di venuta a conoscenza a qualsiasi titolo di un pubblico incanto di interesse economico di Justbit, per cui non è stato ancora portata a termine la fase di indizione e approvazione del relativo bando, contattare con alcun mezzo e stringere qualsiasi tipo di accordo con i rappresentanti dell'ente responsabile della procedura di gara, al fine di reaizzare attività dirette a influenzare a proprio vantaggio il contenuto del bando stesso;

6 effettuare prestazioni in favore dei parti terze che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con le stesse parti;

7 riconoscere compensi in favore dei Collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti;

8 presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

9 destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

10 alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;

11 coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'OdV eventuali situazioni di irregolarità.

12 effettuare le attività di cui ai punti precedenti, ricorrendo a terzi: a tale riguardo, si considerano infatti atti di corruzione non solo i conferimenti illeciti fatti direttamente a/da soggetti, o da loro dipendenti, ma anche i conferimenti illeciti fatti tramite persone che agiscono per conto di tali soggetti, sia in Italia che all'estero.

13 attuare, in generale, pratiche non consentite dalla legge, dagli usi commerciali o dai codici etici delle aziende e degli enti con cui si hanno rapporti.

I Destinatari hanno altresì l'obbligo in particolare di:

1 documentare in modo adeguato ogni regalia non di modico valore data e/o ricevuta e/o promessa, per consentire verifiche e autorizzazioni da parte dell'AD e, ove ritenuto opportuno, dell'OdV (Organismo di Vigilanza). Copia della documentazione rilevante (ad esempio, il documento di trasporto) deve essere conservata in appositi raccoglitori;

2 informare l'AD e l'OdV di richieste esplicite o implicite di benefici, da parte di un cliente o di qualsiasi soggetto terzo, fatto salvo il caso di omaggi di uso commerciale e di modesto valore, per l'adozione delle opportune iniziative;

3 informare l'AD e l'OdV, più in generale, di ogni operazione di acquisto e/o vendita che abbia caratteristiche "anomale", secondo l'esperienza del soggetto aziendale avente contatti con la parte terza.

In caso di contenzioso con la PA, stazioni appaltanti o enti aggiudicatori in tutte le fasi del processo è fatto divieto alle parti interessate e ai professionisti incaricati di tenere comportamenti che:

4 consentano, in sede di incontri formali e informali, anche a mezzo di Legali esterni e Periti di parte, di indurre Giudici o membri del Collegio Arbitrale (compresi gli ausiliari e i Periti d'ufficio), nonché - quando la Pubblica Amministrazione sia controparte del Contenzioso - i rappresentanti di questa, a favorire indebitamente gli interessi di Justbit;

5 consentano, nel corso delle fasi del procedimento (compreso il tentativo obbligatorio di conciliazione nelle cause di lavoro) anche a mezzo di legali esterni e periti di parte, di ottenere il superamento di vincoli o criticità ai fini della tutela degli interessi di Justbit;

6 consentano, in sede di ispezioni/controlli/verifiche da parte degli Organismi pubblici o periti d'ufficio, di influenzarne il giudizio/parere nell'interesse di Justbit;, anche a mezzo di Legali esterni e Periti di parte;

7 consentano, in sede di decisione del contenzioso/arbitrato, di influenzare indebitamente le decisioni dell'Organo giudicante, o le posizioni della Pubblica Amministrazione quando questa sia controparte del contenzioso, anche a mezzo di Legali esterni e di Periti di parte.

8 Tutti gli incontri tra le parti, formali e informali, devono tracciati documentalmente.

4 PRINCIPI DI CONTROLLO

Relativamente ai rapporti con la PA, con stazioni appaltanti o enti aggiudicatori (anche di natura commerciale), di seguito sono indicati i principi di controllo applicati e che i Destinatari sono tenuti a rispettare e che potranno, ove ritenuto opportuno, essere implementati in specifiche procedure aziendali:

1. Le opportunità di natura commerciale relative a gare pubbliche vengono di norma acquisite dai soci relativi all'area di riferimento attraverso segnalazioni da parte della società che detiene la maggioranza delle quote societarie Eprcomunicazione o da segnalazioni raccolte dai soci attraverso la loro rete di conoscenze acquisite. C'è da rilevare che tale tipologia di scouting commerciale non trova frequente applicazione nella società, in quanto le strategie interne propendono per una clientela di tipo privato;
2. I contratti vengono stipulati e sottoscritti unicamente dall'AD. Le attività vengono, ove previsto contrattualmente, rendicontate periodicamente tramite relazioni che attestano il regolare svolgimento delle attività (SAL). I rapporti con i referenti della stazione appaltante, sia in fase di richiesta di offerta che di rendicontazione, sono sempre tracciabili e motivati da richieste di chiarimento e in caso di necessità di rendicontare lo stato di avanzamento e vengono curate dagli Unit Director;
3. I rapporti commerciali con i potenziali committenti vengono gestite dai Project manager (PM) sotto la supervisione dello Unit Director aziendale di riferimento.
4. Relativamente alla partecipazione a procedure per l'ottenimento di sovvenzioni, erogazioni, contributi o finanziamenti da parte di enti e organizzazioni pubblici italiani o comunitari e modalità di impiego dei finanziamenti erogati, considerata anche la natura dei servizi forniti, l'attività ha rara applicazione. Ove effettuata, la gestione delle rendicontazioni dei finanziamenti viene attuata in modo sovrapponibile a quanto già fatto per i contratti pubblici di servizi e forniture. le procedure vengono svolte con le medesime modalità di partecipazione alle gare ad evidenza pubblica, valutando le opportunità sulla base unicamente di aspetti economici, produttivi e strategici. La gestione delle rendicontazioni dei finanziamenti viene attuata in modo sovrapponibile a quanto già fatto per i contratti pubblici di servizi e forniture;
5. Il ricorso ad eventuali partnership viene definito in fase di analisi dell'opportunità e preparazione delle offerte, sia per committenti pubblici che privati. Per linea aziendale, la

scelta delle partnership con soggetti esterni si basa unicamente sui seguenti criteri, in ordine di priorità:

- affidabilità,
- competenze,
- esperienza di collaborazione,
- costi.

6. Le negoziazioni dirette vengono gestite principalmente dai soci in modo da tenere traccia documentale di tutte le comunicazioni intercorse, secondo principi di trasparenza e di redditività della commessa;
7. Il personale non può dare seguito e deve immediatamente segnalare all'AD qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza: l'AD a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta all'OdV;
8. Nell'attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società Pubbliche, enti aggiudicatori o stazioni appaltanti, gli stessi contratti vengono stipulati e sottoscritti unicamente dall'AD. Le attività vengono, ove previsto contrattualmente, rendicontate periodicamente tramite relazioni che attestano il regolare svolgimento delle attività. Inoltre, il personale impegnato nell'operatività della commessa è tenuto a redigere attraverso modulo specifico del software "Alyante"® per ciascun giorno un elenco di attività svolte:
    - una libera descrizione;
    - un'ora di inizio e fine attività;
    - un numero ore impiegate in forma decimale;
    - un CDC di riferimento;
    - la classificazione dell'attività svolta (solo dopo aver compilato il campo CDL).
9. I rapporti con i referenti della stazione appaltante, sia in fase di gara che di rendicontazione, devono essere sempre tracciabili e motivati da richieste di chiarimento e in caso di necessità di rendicontare lo stato di avanzamento;
10. In caso di partecipazione a una gara/incanto pubblico, in caso di venuta a conoscenza a qualsiasi titolo della partecipazione o dell'intenzione di partecipazione di ulteriori

concorrenti, non vengono intrapresi contatti con tali soggetti se non per questioni estranee alla procedura di incanto cui Justbit partecipa o si intende partecipare;

11. anche nel caso si venga a conoscenza anticipatamente all'inizio della procedura di gara della tipologia del servizio futuro oggetto di incanto, non viene intrapreso alcun contatto con rappresentanti della pubblica amministrazione o stazione appaltante responsabile della procedura di gara prima della pubblicazione del bando.
12. I rapporti con le Autorità di controllo, altri organismi di diritto pubblico o enti pubblici nonché il rilascio di informazioni alla P.A vengono gestiti unicamente in base ai poteri di rappresentanza legale (Presidente del CdA o AD). Le eventuali ispezioni vengono presenziate dagli stessi soggetti. Le informazioni e tutte le comunicazioni sono tracciate attraverso mail o archiviazione delle richieste principalmente da parte dell'Unità amministrativa. Tutte le comunicazioni in uscita vengono sottoscritte secondo la rappresentanza legale e tutte le comunicazioni devono essere tracciate attraverso mail o archiviazione delle richieste.
13. In particolare, in occasione di ispezioni da parte dei soggetti indicati al punto 12, il soggetto che riceve l'ispezione avverte immediatamente il legale esterno, l'AD e l'Unità amministrativa (ove si tratti specificamente di materia tributaria/ fiscale). Alle Ispezioni devono presenziare almeno due soggetti, il soggetto ricevente, l'AD o uno dei Chief Officer, o soggetti da questi delegati. In occasione di ispezioni i soggetti interessati possono avvalersi, se opportuno, di professionisti esterni, sulla base della rilevanza e delle implicazioni giuridiche dell'ispezione, anche allo scopo di verificare la legittimità della stessa. Nel caso in cui, nell'ambito o a seguito dell'Ispezione, debbano essere effettuate comunicazioni (di qualsiasi genere e con qualsiasi mezzo) alla Pubblica Amministrazione, viene coinvolto il supporto legale esterno. Le comunicazioni predisposte devono essere sottoscritte unicamente dai soggetti aziendali muniti degli occorrenti poteri di rappresentanza legale (Presidente del CdA o AD). Le Funzioni interessate sono tenute a conservare un'evidenza documentale delle richieste ricevute, dei verbali predisposti dai Pubblici Ufficiali o dagli Incaricati di Pubblico Servizio in occasione delle Ispezioni nonché delle informazioni, dei dati e dei documenti consegnati, resi disponibili e/o comunicati. i verbali predisposti dai Pubblici Ufficiali o dagli Incaricati di Pubblico Servizio potranno essere firmati unicamente dai soggetti che per ruolo siano in possesso dei necessari poteri di rappresentanza. L'AD è tenuto ad inviare all'OdV. copia delle richieste di informazioni notificate o ricevute e dei verbali relativi e ad informare, alla prima riunione utile, il CdA.

14. In caso di richiesta di provvedimenti amministrativi occasionali, di autorizzazioni, licenze e concessioni per lo svolgimento di attività strumentali a quelle tipiche della società, tutte le attività vengono svolte secondo i poteri attribuiti secondo principi di segregazione dei compiti in base ai poteri autorizzativi conferiti, di tracciabilità e secondo le regole comportamentali applicate da Justbit. Le attività vengono continuamente monitorate durante lo svolgimento delle commesse dai Director di area e il personale impegnato nell'operatività della commessa è tenuto a rendicontare le attività svolte.

Relativamente alle aree di rischio in riferimento ai reati di corruzione tra privati, di seguito sono indicati i principi di controllo applicati e che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. Le opportunità di natura commerciale vengono intercettate dagli owner, dai PM e in generale dal Team di progetto in base ai fabbisogni espressi o impliciti dei clienti acquisiti o potenziali. I soggetti aziendali preposti propongono, unicamente su logiche di tipo commerciale, servizi aggiuntivi ai clienti, integrando eventualmente quanto già richiesto in fase di richiesta di offerta. La valutazione alla partecipazione e l'effettiva convenienza a presentare offerta è di competenza dei partner della società con approvazione finale dell'AD, sulla base unicamente di principi basati sulla redditività di commessa o sull'importanza strategica dell'acquisizione del progetto. I rapporti commerciali con clienti potenziali o acquisiti vengono gestiti dai PM sotto la supervisione del partner aziendale di riferimento.
2. I rapporti commerciali con i potenziali committenti vengono gestite dai PM sotto la supervisione dello Unit Director di area. La predisposizione dell'offerta viene principalmente redatta dal PM dell'unità di riferimento sotto il coordinamento e la supervisione di un singolo soggetto (di norma il Director di riferimento), tramite l'eventuale ausilio di soggetti interni specializzati nelle unità organizzative tecniche interne. In tale fase vengono anche definite necessità di eventuali partnership o consulenze specialistiche, su criteri basati sul pieno soddisfacimento dei requisiti del richiedente, della redditività di commessa e della trasparenza nei rapporti commerciali. Le offerte elaborate vengono sistematicamente validate dal socio di riferimento prima dell'inoltro ai clienti.
3. La preventivazione economica viene definita sul numero di giornate uomo necessarie per ogni funzione specialistica interna o esterna in base al livello di competenze e del ruolo delle singole risorse assegnate e alla conseguente quotazione economica, in base a criteri basati sulla massima trasparenza e effettivo impegno previsto per lo specifico progetto,

infatti il preventivo viene predisposto sulla base di un format indicante attività richieste, figure professionali coinvolte, numero di giornate necessarie e quotazione della singola giornata; qualsiasi variazione deve essere opportunamente autorizzata dallo Unit Director di riferimento;

4. Tutte le offerte vengono archiviate per cliente e conservate in formato elettronico su Google Drive.
5. In caso di richiesta di documentazione amministrativa propedeutica alla presentazione dell'offerta, viene coinvolta anche l'Unità amministrativa che provvede autonomamente alla preparazione della documentazione necessaria.
6. Lo stato dei preventivi (e relativa accettazione) viene tracciato all'interno del gestionale aziendale;
7. ai fini della partecipazione alle procedure di cui alle attività commerciali di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo, gli incarichi vengono assegnati previa qualifica e successiva selezione nell'ambito del processo di acquisti, interamente gestito dalla fase di richiesta a quella di rendicontazione/fatturazione con software gestionale "Alyante"®.
8. I fornitori vengono inseriti in apposito Albo previa compilazione di questionario (File "Censimento fornitore"), in cui lo stesso fornitore deve preventivamente dichiarare l'adesione al Codice Etico comportamentale e Modello 231 di Justbit;
9. La gestione del processo di acquisti è stata regolamentata da apposita procedura ("Procedura acquisti su sistema applicativo Teamsystem Alyante**)** da considerare parte integrante del presente modello. Tutti i fornitori vengono qualificati principalmente sulla stabilità finanziaria; le funzionalità del software sono riportate nel Manuale operativo, da considerare specifico protocollo di controllo per il presente Modello;
10. Nell'ambito dei contratti con i fornitori, relativamente alle attività di:

    - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento;
    - gestione e segnalazione delle anomalie,

    Il processo viene gestito interamente per via informatica attraverso specifico software gestionale (Alyante®) con cui vengono tracciate le attività sensibili, in particolare:

    - Richiesta di acquisto;

- Ordine di acquisto;
- Strategia di rilascio, comprendente:
  a. inserimento della RdA attraverso Alyante da parte del soggetto richiedente, facente parte del Team di Progetto;
  b. autorizzazione da parte dei responsabili di progetto (PM)
  c. generazione OdA ed invio del documento al fornitore da parte dei referenti di progetto, il quale condividerà lo stesso documento con il richiedente interessato.
  d. Approvazione del servizio/bene ricevuto per benestare ai pagamenti.

Relativamente al processo sono stati individuati Responsabili PM che gestiscono le fasi autorizzative della fornitura per il loro ambito di competenza. Il principio di concorrenza viene garantito attraverso la richiesta di quotazione ad almeno tre fornitori diversi, salvo urgenze.

Relativamente all'attribuzione di ruoli e responsabilità nell'ambito del processo di acquisti, il soggetto richiedente ha l'obbligo di curare le seguenti attività:

- raccogliere la proposta del cliente esterno o valutarne autonomamente le necessità sulla base del budget affidatogli;
- predisporre le specifiche tecniche della fornitura obbligatorie e desiderate ("nice to have");
- elaborare a sistema la richiesta d'acquisto corredata delle specifiche tecniche.

Il soggetto richiedente ha i seguenti compiti:

- proporre la rosa dei potenziali fornitori da consultare;
- inviare le richieste d'offerta corredate dalla specifica tecnica;
- analizzare e confrontare le offerte pervenute;
- valutare la parte tecnica delle offerte assieme ai PM di progetto;
- concludere la trattativa commerciale;
- sottoporre la proposta contrattuale all'approvazione dell'AD;
- emettere l'ordine.

In fase di erogazione del servizio o a ricevimento del bene, il soggetto richiedente ha la responsabilità di:

- curare la ricezione del bene o del servizio ed effettuare i relativi controlli; di congruità con quanto pattuito;
- effettuare il controllo qualitativo, se questo non è già certificato dal fornitore;
- comunicare all'Amministrazione la congruità e della qualità della fornitura e l'autorizzazione al pagamento;
- in caso di esito negativo dei controlli effettuati segnalare all'AD dei problemi riscontrati.

le funzionalità del software sono riportate nel Manuale di utilizzo, da considerare specifico protocollo di controllo per il presente Modello;

11. La messa in pagamento delle fatture passive avviene unicamente previa verifica da parte dell'Unità amministrativa (per forniture ricorrenti) o del Responsabile di progetto (in caso di servizi non continuativi) e in presenza di specifico ordine di vendita a sistema- L'unità amministrativa effettua prima della registrazione una verifica di correttezza formale del documento trasmesso in forma elettronica. Tutto il ciclo passivo viene gestito da applicativo gestionale.
12. In caso di necessità di recupero dei crediti, nonché le transazioni commerciali remissive a fronte di disservizi o contestazioni, le contestazioni relative a pagamenti non liquidati vengono per lo più risolte attraverso attività di mediazione di tipo stragiudiziale. Tali casi sono tutti opportunamente tracciabili e verificabili documentalmente.
13. Nei rari casi in cui si reputi necessario ricorrere a procedure esecutive di recupero del credito, le stesse vengono interamente gestite tramite il supporto di legale esterno esperto in materia, che ha aderito ai principi etico comportamentali di Justbit.

Relativamente alle aree di rischio a rischio che potrebbero assumere carattere strumentale e/o di supporto alla commissione dei reati contemplati dalla presente parte speciale, sono indicati i principi di controllo applicati e che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. Nelle attività di ricerca e selezione del personale e di eventuali partner e collaboratori, la necessità di acquisire nuove risorse deriva unicamente da:

- esigenze di rafforzamento organico in base alla complessità e ampiezza delle commesse acquisite;
- necessità di acquisizione di competenze altamente specialistiche comprovate da lunghi periodi di esperienza nel settore;
- necessità di ampliamento di determinate aree per scelte strategiche.

La selezione viene effettuata attraverso acquisizione dei curricula da candidature spontanee previo accesso in apposita area job del sito internet della società o attraverso indicazione dei soggetti che per competenza ed esperienza hanno maggior contezza dei fabbisogni afferenti alla propria area di esercizio. I colloqui vengono sempre effettuati da uno dei Director aziendali. I candidati non vengono mai valutati da un singolo soggetto ma effettuano sempre più colloqui con diverse figure aziendali, in base all'area/settore di riferimento della risorsa;

2. L'incentivazione è unicamente basata sul merito nella gestione delle commesse e sul raggiungimento degli obiettivi commerciali. Per politica direzionale, non vengono in alcun caso ammessi favoritismi o altre forme di avanzamento di carriera per i quali non sia dimostrabile con dati oggettivi la componente meritocratica;
3. Tutte le richieste di ferie, permessi, benefici di legge vengono richiesti in modo tracciabile e sono sottoposte all'accettazione da parte della Unità amministrativa; inoltre, la richiesta di disposizione di risorse finanziarie deve essere appositamente motivata.
4. I rimborsi spese vengono riconosciuti unicamente previa presentazione di tutti i giustificativi da parte del personale su applicativo. Normalmente non viene riconosciuto alcun anticipo sulle spese di trasferta. L'uso del contante viene in ogni caso ridotto al minimo e tutte le uscite sono adeguatamente tracciabili.
5. Sono state definite formalmente specifiche regole per i dipendenti, riportati nel Regolamento aziendale" da considerare specifico protocollo di controllo per il presente Modello e in cui vengono descritti:
   - Modalità di rilevazione presenze;
   - l'orario di lavoro;
   - le modalità di gestione delle ferie, permessi, malattia e straordinari
   - comunicazione in caso di infortunio;

- gestione dei beni e mezzi aziendali.

6. Le spese di rappresentanza sono riconosciute dalla Unità amministrativa unicamente se adeguatamente giustificate dalla natura dell'incarico o della commessa per cui si rendono necessarie. Le modalità di gestione di tali uscite sono ampiamente tracciabili e giustificabili.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE B- REATI INFORMATICI

1 TIPOLOGIA DI REATI APPLICABILI

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D. Lgs. 231/2001 è collegato il regime di responsabilità a carico di Justbit, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di organizzazione, gestione e controllo previsto dal decreto.

Ciò premesso, per quanto riguarda la presente Parte Speciale, si provvede di seguito a fornire l'elenco dei reati in essa contemplati e menzionati nell'art. 24-bis del Decreto

Falsità riguardanti un documento informatico (art. 491-bis c.p.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo, bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lett. p), D.Lgs. 82/2005).

Accesso abusivo a un sistema informatico o telematico (art. 615-ter cod. penale)

Il reato si configura nel momento in cui chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Costituiscono circostanze aggravanti 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti 4) qualora i fatti riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. penale)

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

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. penale)

Il reato si configura nel momento in cui chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. penale)

Il reato si configura nel momento in cui un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. penale)

Il reato si configura nel momento in cui un soggetto installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. penale)

Il reato si configura nel momento in cui un soggetto distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata e si procede d'ufficio.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-ter cod. penale)

Il reato si configura nel momento in cui un soggetto 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.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione, o la soppressione delle informazioni, dei dati o dei programmi informatici e/o il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata.

Danneggiamento di sistemi informatici e telematici (art. 635-quater cod. penale)

Il reato si configura nel momento in cui chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- quinquies cod. penale)

Il reato si configura quando il fatto di cui all'art. 635-quater (Danneggiamento di sistemi informatici o telematici) è diretto a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Destinatario cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero nel caso in cui l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati transnazionali.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di

commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati previsti dalla presente parte speciale applicabili a Justbit, sono state individuate le seguenti aree di rischio ed i processi ad esse collegati:

Processi	Attività
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Gestione della sicurezza logica dei sistemi, con particolare attenzione a: - controllo accessi a sistemi informativi e rete dati (rete aziendale, internet, extranet); - crittografia dei dati e/o del canale di comunicazione (ad esempio infrastrutture firewall, Reti private virtuali, ecc.)
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Sviluppo e attuazione di sistemi di monitoraggio e revisione per la prevenzione e individuazione di attività non autorizzate/illecite sulla rete, sistemi e banche dati aziendali
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Attività di amministrazione applicativa/sistemistica di: - applicazioni a supporto dei processi di business; - database/archivi elettronici; - sistemi operativi.
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Attività informatiche che potrebbero comportare la diffusione di software malevoli, esecuzione di attacchi informatici che potrebbero essere condotte attraverso strumenti/dispositivi/informazioni aziendali
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Gestione di caselle di posta e domini di rete
P05- Gestione dei sistemi informativi	Gestione di servizi online finalizzati alla dematerializzazione (es. Cedolino/CUD online, iter autorizzativo ferie/permessi/missioni).
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Utilizzo da parte del personale delle postazioni di lavoro fisse (es. desktop) e mobili (es. laptop, PDA); utilizzo della posta elettronica e di internet
P05- Gestione dei sistemi informativi P11- Gestione delle commesse	Utilizzo del sistema informatico per: - accesso in via telematica, o direttamente on site, a sistemi elettronici di clienti e fornitori; - acquisizione delle informazioni utili per la qualificazione dei fornitori;
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità P05- Gestione dei sistemi informativi	Creazione, trattamento, archiviazione di documenti elettronici con valore probatorio
P05- Gestione dei sistemi informativi	Gestione degli accessi fisici alle aree riservate

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica Justbit si pone sono i seguenti:

- Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- Integrità: garanzia che ogni dato della società e dei clienti sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;
- Disponibilità: garanzia di reperibilità di dati della società e dei clienti in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico dei Destinatari (limitatamente rispettivamente agli obblighi contemplati nei principi di controllo e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/2001);
- violare i principi di controllo previsti nella presente parte speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

1 alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

2 accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati, senza avere ottenuto preventivamente le necessarie autorizzazioni;

3 accedere abusivamente al proprio sistema informatico o telematico e a quelli di soggetti terzi al fine di alterare e/o cancellare dati e/o informazioni;

4 detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di clienti, soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

5 detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

6 svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

7 svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

8 istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati in modo abusivo e fraudolento;

9 svolgere abusivamente attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

10 svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

11 distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1 utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio o di regolare erogazione dei servizi richiesti dalla clientela, attenendosi alle autorizzazioni acquisite;

2 non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza avere precedentemente sottoscritto un patto di riservatezza e senza l'autorizzazione del Chief Information Security Officer ("CISO");

3 in caso di smarrimento o furto, informare tempestivamente il Chief Information Security Officer ("CISO") e presentare denuncia all'Autorità Giudiziaria preposta; In caso di detenzione di dati di soggetti terzi, avvisare tempestivamente anche il soggetto interessato;

4 evitare di introdurre e/o conservare nella società (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché applicazioni/software che non siano state preventivamente approvate dal CISO o la cui provenienza sia dubbia;

5 evitare di trasferire all'esterno della società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà di Justbit o di altra società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione dell'AD;

6 evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (familiari, amici, etc…);

7 evitare l'utilizzo di passwords di altri utenti della società, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione di AD; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia ai Sistemi Informativi;

8 evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

9 utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;

10 rispettare le procedure e gli standard previsti, segnalando senza ritardo al CISO eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

11 impiegare sulle apparecchiature della società solo prodotti ufficialmente acquisiti da Justbit;

12 astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

13 astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

14 osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della società;

15 osservare scrupolosamente quanto previsto dalle politiche di sicurezza della società per la protezione e il controllo dei sistemi informatici.

4 PRINCIPI DI CONTROLLO

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3 della presente sezione, oltre che dei principi generali contenuti nella parte generale del presente Modello, nel disciplinare la fattispecie di attività sensibile di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento:

1 Nomina di un Chief Information Security Officer ("CISO"), avente i seguenti compiti principali:

- identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità;
- definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati. A cura dei responsabili dovranno inoltre essere affissi i cartelli contenenti l'informativa, in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;
- assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni associative. Così, per i dati relativi ad attività di studio e di ricerca (art. 100), il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
- adempiere agli obblighi di sicurezza, quali:

- adottare, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);
- definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- definire una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

- far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
- comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare l'eventuale cessazione di trattamento
- in merito agli incaricati, il Responsabile deve:
  - individuare, in collaborazione con il Titolare del trattamento, designandoli per iscritto, gli incaricati del trattamento;
  - recepire eventuali istruzioni cui devono attenersi gli incaricati nel trattamento dei dati, da parte del Titolare del trattamento, assicurandosi che vengano materialmente consegnate agli stessi;
  - adoperarsi al fine di rendere effettive le suddette istruzioni cui devono attenersi gli incaricati del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza da parte degli incaricati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
  - stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.7;

- tenere aggiornato periodicamente, l'elenco nominativo degli Incaricati al trattamento con relativi profili autorizzativi per l'accesso alle banche dati di pertinenza;

- trasmettere le richieste degli interessati al Titolare del trattamento, ai fini dell'esercizio dei diritti dell'interessato, ai sensi degli artt.7, 8, 9 e 10, 12 del D. Lgs. n. 196/2003;
- collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi dell'art.10 del D. Lgs. n.196/2003 e delle istanze del Garante per la protezione dei dati personali;
- collaborare con il Titolare del trattamento, ai fini della nomina in qualità di Responsabili esterni al trattamento, se necessari;
- collaborare con il Titolare del trattamento provvedendo a fornire ogni informazione dal medesimo richiesta;
- Mcomunicare tempestivamente al Titolare del trattamento ogni notizia rilevante ai fini della tutela della riservatezza.

2 Nomina di un soggetto esterno qualificato avente il ruolo di Data Protection Officer ("DPO"), avente i compiti:

- Informare e consigliare la società ed i suoi dipendenti circa gli obblighi di protezione dei dati ai sensi del GDPR;
- Monitorare la conformità della società al Regolamento GPDR ed alle policy e procedure interne in materia di protezione dei dati. Questo compito include anche il monitoraggio dell'assegnazione delle responsabilità e della formazione del personale coinvolto nelle operazioni di trattamento dei dati;
- Fornire consulenza sulla necessità o meno di eseguire valutazioni d'impatto sulla protezione dei dati (DPIA), come eseguirle e quali risultati aspettarsi;
- Fungere da punto di contatto per l'autorità di controllo per tutte le questioni inerenti alla protezione dei dati, come la segnalazione di violazioni dei dati;
- Fungere da punto di contatto per gli interessati in materia di privacy dei dati, per esempio per le richieste di accesso dei dati personali.

3 Esistenza di regole per la gestione del rischio informatico che individui le seguenti fasi:

- identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con

riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;

- individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
- individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
- identificazione delle possibili contromisure;
- effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
- definizione di un piano di azioni preventive e correttive da porre in essere e da riesaminare periodicamente in relazione ai rischi che si intendono contrastare;
- documentazione e accettazione del rischio residuo.

4 Esistenza di regole per la gestione del rischio informatico al fine di tenere sotto controllo i seguenti aspetti:

- definizione del quadro normativo riferito a tutte le aree della società, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un ruolo interno alla società (CISO) che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche di utilizzo dei software;
- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale;

- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

5 Implementazione delle seguenti misure di sicurezza:

Sul piano organizzativo:

- Istituzione registro dei trattamenti;
- nomina del Responsabile Protezione dei dati personali (DPO);
- individuazione di una funzione interna referente per le incombenze ai fini privacy;
- assegnazione e formalizzazione del ruolo agli incaricati al trattamento;
- formalizzazione dei ruoli con gli incaricati esterni al trattamento e con i Responsabili del trattamento dei dati;
- aggiornamento periodico ambito trattamento;
- formazione periodica;
- adozione di una procedura per il processo di trattamento dei dati personali e i data breach;
- assistenza tecnica solo da soggetti qualificati;
- manutenzione periodica apparecchiature;
- monitoraggio continuo stato apparecchiature.

Sul piano della sicurezza fisica:

- adozione di piani di emergenza;
- ubicazione archivi in locali non esposti a rischio;
- certificazione impianti;
- installazione di gruppi di continuità/stabilizzatore;
- installazione di impianto di climatizzazione;
- verifica norme costruzione uffici;
- schermatura apparecchiature;

- registrazione e regolamentazione degli accessi ai locali;
- attivazione di sistemi di allarme;
- utilizzo di contenitori con chiave;
- identificazione degli utenti che accedono ai locali;
- protezione dei locali con serrature di sicurezza.

Sul piano della sicurezza informatica:

- attivazione e installazione di antivirus;
- attivazione e installazione di firewall;
- analisi periodica dei log file;
- backup periodico;
- utilizzo di sistemi di firma digitale ove possibile;
- criptazione dei dati ove possibile;
- procedure di autenticazione di utenti;
- disattivazione delle credenziali non utilizzate
- utilizzo di credenziali con password rafforzate;
- modifica periodica della password;
- protocollo di rete SSL;
- divieto di installazione di software non autorizzati.

6 Definizione e diffusione tramite il CISO di Linee guida per la disciplina del processo di trattamento dei dati personali e protezione delle persone fisiche con riguardo al trattamento dei dati personali (parte generale e parte Speciale);

7 Attuazione di una politica di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.

8 Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l’accesso a un sistema elaborativo o trasmissivo. L’identificazione e l’autenticazione devono essere effettuate prima di ulteriori interazioni

operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.

9 Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichi attraverso la verifica e la gestione dei diritti d'accesso.

10 Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici;

11 Definizione di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.

12 Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).

13 Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti;

14 Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking.

15 Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio della società oggetto di protezione (risorse tecnologiche e informazioni);

16 Predisposizione e attuazione di regole organizzative al fine di definire (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di principi di controllo idonei a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE C- REATI DI CRIMINALITÀ ORGANIZZATA

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte speciale “C”, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell’art. 24-ter del Decreto.

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

Si tratta di un delitto associativo contro l'ordine pubblico che si realizza mediante la condotta di tre o più persone che si associano al fine di commettere una serie non determinata di delitti.

È un delitto cd. plurisoggettivo, nel senso che affinché sia configurabile necessita della partecipazione di minimo tre persone.

La condotta rilevante consiste nel promuovere, costituire, organizzare l'associazione oppure anche solo nel partecipare alla stessa.

Dal punto di vista soggettivo, la condotta deve essere sorretta dalla coscienza e dalla volontà di far parte del sodalizio criminoso e di contribuire alla realizzazione del programma concernente la commissione di più delitti.

I requisiti essenziali delineati dalla giurisprudenza per configurare il reato associativo, (in modo da differenziarlo rispetto al mero concorso di persone nel reato) sono: i) un vincolo associativo tendenzialmente permanente; ii) la consapevolezza di ciascun associato di far parte del sodalizio e di partecipare al programma comune: iii) lo scopo di commettere più delitti volti ad attuare un indeterminato programma criminoso; iv) una struttura organizzativa, anche rudimentale, purché idonea a realizzare un indeterminato programma criminoso.

La dottrina ammette la configurabilità del 'concorso esterno' nel reato di associazione per delinquere (ex art. 110 c.p.) caratterizzato dal contributo esterno al mantenimento e rafforzamento dell'associazione. La giurisprudenza si è pronunciata in relazione al reato di cui all'art. 416 bis c.p.

Circostanze aggravanti speciali del reato sono: la scorreria in armi (art. 416, 4° comma c.p.); il numero di dieci o più degli associati (art. 416, 5° comma c.p.) associazione diretta alla riduzione in schiavitù, alla tratta di persone, all'acquisto di schiavi (art. 416, 6° comma).

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

Tale tipologia di reato si applica a chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone. Il trasgressore è punito con la reclusione da sette a dodici anni.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati transnazionali.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "C" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività
P01- Commerciale	Valutazione delle opportunità a partecipare a gare pubbliche
P01- Commerciale	Gestione delle partnership nelle attività di partecipazione a gare e richiesta finanziamenti (es.: joint venture, anche in forma di ATI, RTI, consorzi, ecc.)
P01- Commerciale P07- Approvvigionamento	Assegnazione, ai fini della partecipazione alle procedure di cui alle attività commerciali di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo

Processi	Attività
P08- Processo finanziario	Gestione dei conti correnti bancari
P07- Approvvigionamento P11- Gestione della commessa	Richieste di acquisto e selezione del fornitore
P04- Gestione delle risorse umane	Ricerca e selezione del personale
P09- Processo Amministrativo	Compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione
P09- Processo Amministrativo	Predisposizione delle dichiarazioni fiscali periodiche
P09- Processo Amministrativo	Liquidazione delle imposte

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- violare i principi di controllo di Justbit previsti nella presente parte speciale.
- formare associazioni in qualsiasi forma per perseguire finalità non consentite dalla legge;
- intrattenere rapporti, negoziare, stipulare, porre in esecuzione contratti o atti o assumere persone indicate nella black list o in organizzazioni ad esse collegate;

- verificare l'attendibilità commerciale e professionale dei prestatori di servizi e partner.

Di seguito sono indicati i principi procedurali che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1 rispettare i criteri di selezione di fornitori di beni/servizi e partner per la stipula di contratti e per la realizzazione di investimenti, nonché i criteri di valutazione delle offerte;

2 è vietato porre in essere qualsiasi transazione finanziaria a destinatari senza avere svolto le necessarie verifiche;

3 le operazioni la cui entità è definita significativa devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli e accertamenti o comunque ne sia certa l'onorabilità;

4 i dati raccolti relativamente ai rapporti con clienti, consulenti e partner devono essere completi e aggiornati, sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del loro profilo.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

4 PRINCIPI DI CONTROLLO

Di seguito sono indicati i principi di controllo che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1 rispettare i criteri di selezione di fornitori di beni/servizi e partner per la stipula di contratti e per la realizzazione di investimenti, nonché i criteri di valutazione delle offerte;

2 qualunque transazione finanziaria deve presupporre la conoscenza del beneficiario della relativa somma;

3 le operazioni la cui entità è definita significativa nell'ambito delle procedure vigenti devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli e accertamenti o comunque ne sia certa l'onorabilità;

4 i dati raccolti relativamente ai rapporti con clienti, consulenti e Partner devono essere completi e aggiornati, sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del loro profilo.

5 Rispetto degli obblighi relativi alle attività e i controlli svolti in adempimento agli obblighi di tracciabilità dei flussi finanziari in materia di appalti pubblici di lavori, servizi e forniture (Legge 13 agosto 2010, n. 136. art. 3).

Oltre ai principi comportamentali sopra individuati valgono, in via prioritaria, i principi di controllo già previsti da Justbit in relazione ad altre tipologie di reato 231 disciplinate nelle seguenti parti speciali del presente Modello Organizzativo:

- Reati di corruzione, anche tra privati, ed altri reati nei rapporti con la Pubblica Amministrazione;
- Reati Societari;
- Reati aventi finalità di terrorismo o di eversione dell'ordine democratico;
- Reati di Ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE D- REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

1 TIPOLOGIA DI REATI APPLICABILI

L'art. 6 del D.L. n. 350/2001 convertito, con modificazioni, dalla Legge 23 novembre 2001, n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro", ha inserito nel Decreto 231 l'art. 25-bis, il quale mira a punire il reato di falsità in monete, in carte di pubblico credito e in valori di bollo, a sua volta riformulato dalla Legge 23 luglio 2009, n. 99 recante "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia".

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)

Tale reato punisce chiunque, fuori dei casi previsti dagli artt. 453 e 454 introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione.

Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)

Tale reato punisce chiunque spende, o mette altrimenti in circolazione monete contraffatte o alterate, da lui ricevute in buona fede.

Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)

Tale reato punisce i) chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, ii) chiunque contraffà o altera brevetti, disegni o modelli industriali nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati.

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

Tale reato punisce chiunque, fuori dei casi di concorso nei reati previsti dall'art. 473 c.p., introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati.

Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello Stato, è punito chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati.

2 AREE DI RISCHIO

Con specifico riferimento ai delitti di falsità in monete, in carte di pubblico credito e in valori in bollo, non appare realisticamente concretizzabile la possibilità che i Destinatari di Justbit pongano in essere, autonomamente o in concorso con terzi, nell'interesse o a vantaggio della società stessa, fatti idonei a configurare tali tipologie di reato.

In occasione dell'attività di mappatura, sono state comunque individuate nell'ambito della struttura organizzativa ed aziendale di Justbit delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati transnazionali.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

Ciò premesso, in relazione ai reati previsti dall'art. 25-bis del D.Lgs. 231/2001 applicabili alla società, sono state individuate le seguenti attività sensibili ed i processi ad esse collegati:

Processi	Attività sensibile
P05- Gestione dei sistemi informativi P07- Approvvigionamento	Acquisto e gestione di software tutelati da brevetti (es. antivirus, applicativi)
P05- Gestione dei sistemi informativi	Gestione del sito internet aziendale

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. Alterare o copiare marchi o segni distintivi di prodotti industriali;
2. Intraprendere negoziazioni con clientela non compiutamente nota ovvero avente ad oggetto importi di rilevante entità e di dubbia provenienza;
3. Segnalare all'AD qualunque tentativo di messa in circolazione di banconote o valori sospetti di falsità da parte della clientela o di terzi del quale il personale risulti destinatario o semplicemente a conoscenza;
4. Non utilizzare, in assenza delle necessarie autorizzazioni, software tutelati da brevetti e/o un nuovo marchio che risulti precedentemente registrato.

4 PRINCIPI DI CONTROLLO

Di seguito sono indicati i principi procedurali che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. Modalità gestionali definite per il processo di selezione dei fornitori ed alla contrattualizzazione degli stessi;
2. Assenza di utilizzo del contante in qualsiasi negoziazione con soggetti terzi.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE E- REATI CONTRO L'INDUSTRIA E IL COMMERCIO

1 TIPOLOGIA DI REATI APPLICABILI

Con l'approvazione della legge L. 99/2009 è stato introdotto l'art. 25-bis.1 che amplia le tipologie di reati presupposti alle seguenti categorie:

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

Il reato si configura nel momento in cui un soggetto adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio. Il reato tutela il normale esercizio dell'attività industriale o commerciale svolta dai soggetti privati.

L'incriminazione ha natura sussidiaria perché è destinata a operare qualora il fatto non costituisca un fatto più gravemente sanzionato (ad es. incendio, oppure uno dei reati informatici previsti dall'art. 24-bis del Decreto).

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (Art. 517-ter c.p.)

Salva l'applicazione degli articoli 473 e 474 la norma punisce chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso.

Viene altresì in uguale misura punito chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i beni di cui al precedente periodo.

I suddetti delitti sono punibili sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati contro l'industria e il commercio.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di

commissione dei reati. I risultati complessivi di tale attività sono riportati nella “Matrice di rischio e controlli interni” in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale “E” del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P01- Commerciale	Valutazione delle opportunità a partecipare a gare pubbliche
P01- Commerciale	Valutazione delle opportunità a presentare offerta per clienti privati
P11- Gestione della commessa	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società Pubbliche
P11- Gestione della commessa	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con privati
P05- Gestione dei sistemi informativi	Gestione del sito internet aziendale
P10- Processo societario e rapporti con stakeholder	Definizione delle forme pubblicitarie

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall’AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti “Destinatari”).

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l’espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
2. violare i principi di controllo previsti nella presente parte speciale;
3. divulgare qualsiasi notizia o giudizio relativo a un competitor e alla qualità dei suoi servizi tale da determinarne il discredito;

4. porre in essere qualsiasi atto che possa essere finalizzato a una concorrenza non basata su principi di correttezza e trasparenza;
5. divulgare informazioni mendaci in danno di potenziali competitor;
6. mettere in atto qualsiasi atto intimidatorio o vessatorio nei confronti di potenziali competitor;
7. applicare principi di selezione dei fornitori che non si basino unicamente su criteri di massima oggettività e trasparenza;
8. nell'ambito delle proprie attività, utilizzare qualsiasi bene od oggetto che violi un titolo di proprietà industriale.

4 PRINCIPI DI CONTROLLO

Di seguito sono indicati i principi procedurali che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. qualunque transazione finanziaria deve presupporre la conoscenza del beneficiario della relativa somma;
2. le operazioni la cui entità è definita significativa nell'ambito delle procedure vigenti devono essere concluse con persone fisiche e giuridiche verso le quali siano state preventivamente svolte idonee verifiche, controlli e accertamenti;
3. i dati raccolti relativamente ai rapporti con clienti, consulenti e Partner devono essere completi e aggiornati, sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del loro profilo e sulla loro attendibilità;
4. definizione dei criteri per la gestione dei processi di acquisto, con particolare riferimento alla selezione dei fornitori;
5. diffusione di una politica aziendale improntata a principi di eticità e correttezza nei confronti dei concorrenti nella gestione delle comunicazioni esterne e in occasione della partecipazione a gare;
6. verifica preliminare da parte della Unità organizzativa competente di qualsiasi contenuto di natura promozionale o pubblicitaria da pubblicare al fine di prevenire i reati di violazione dei diritti di proprietà industriale.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE F- REATI SOCIETARI

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte Speciale "F", si provvede di seguito a fornire una elencazione dei reati in essa contemplati e indicati all'art. 25-ter del Decreto (di seguito i "Reati Societari"), raggruppandoli, per maggiore chiarezza, in tre tipologie differenti.

1.1 FALSITÀ IN COMUNICAZIONI E RELAZIONI

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

I reati si configurano allorquando si procede alla esposizione, all'interno dei bilanci, delle relazioni o delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero (ancorché oggetto di valutazione), ovvero alla mancata indicazione, nei medesimi documenti, di informazioni, la cui comunicazione è prescritta dalla legge, riguardanti la situazione economica, patrimoniale o finanziaria della società o del gruppo a cui appartiene, per trarne ingiusto profitto e in modo concretamente idoneo a trarre i destinatari in errore.

La legge n° 69 del 27/05/2015 ha introdotto la fattispecie prevista nel caso i fatti di cui all'art. 2621 c.c. siano di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta. In tal caso la pena pecuniaria è dimezzata.

Ai fini dell'integrazione degli elementi costitutivi delle fattispecie criminose all'esame, si precisa che:

- le informazioni false o omesse devono essere tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale appartiene;
- la responsabilità sussiste anche nel caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- la condotta deve essere realizzata con l'intenzione di ingannare i soci o il pubblico, nonché rivolta al fine di conseguire per sé o per altri un ingiusto profitto;
- la punibilità è esclusa se le falsità o le omissioni determinano una variazione del risultato economico d'esercizio, al lordo delle imposte, non superiore al 5% o una variazione del patrimonio netto non superiore all'1%. In ogni caso, il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10 % di quella corretta;

- con riferimento all'art. 2622 c.c., la Legge 28 dicembre 2005, n. 262, ha introdotto una circostanza aggravante per l'ipotesi in cui dalla falsità derivi un nocumento ad un numero rilevante di risparmiatori - pari allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT - indotti ad operare scelte di investimento sulla base delle informazioni riportate nelle scritture sociali, ovvero se sia consistito nella distruzione o riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo;
- l'ipotesi di reato prevista dall'art. 2622 c.c. è punita a querela di parte, salvo che il fatto sia commesso in danno dello Stato, di altri Enti Pubblici, delle Comunità europee o che si tratti di società quotate, nel qual caso il delitto è procedibile d'ufficio.

Trasformazioni, fusioni e scissioni transfrontaliere[21]

L'obiettivo della direttiva da cui trae orgine il decreto cha ha modificato l'art. 25- ter comma 1, è quello di facilitare le trasformazioni, le fusioni e le scissioni transfrontaliere delle società dell'UE, eliminando gli ostacoli ingiustificati alla libertà di stabilimento nel mercato unico ed armonizzando le discipline dei diversi Paesi, così da rendere compatibili i vari ordinamenti mediante la previsione di livelli minimi di garanzia per soci, creditori e lavoratori.

La nuova normativa si applica non solo alle operazioni straordinarie transfrontaliere poste in essere entro i confini dell'Unione europea, ma anche alle operazioni internazionali alle quali partecipino o da cui risultino una o più società regolate dalla legge italiana e almeno una società regolata dalla legge di uno Stato non appartenente all'Ue.

Rileva, nell'ambito dell'art. 55 del citato decreto, una modifica al D. Lgs. 231/2001 e, segnatamente, all'art 25-ter comma 1. Il decreto, con la lettera "s-ter", introduce il delitto di "false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva (UE) 2019/2121, del Parlamento europeo e del Consiglio, del 27 novembre 2019". Tale delitto è punito con la sanzione pecuniaria da centocinquanta a trecento quote.

1.2 TUTELA DEL CAPITALE SOCIALE

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

Il reato si configura allorquando si proceda, fuori dei casi previsti dalla legge, all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società o della controllante, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Si precisa che, se

[21] Reato introdotto dal D.lgs. 19 del 02/03/2023 recante "Attuazione della direttiva (UE) 2019/2121 del Parlamento europeo e del Consiglio, del 27 novembre 2019, che modifica la direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere

il capitale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio riferito all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto. Soggetti attivi del reato sono gli amministratori. È configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante siano da questi ultimi effettuate su istigazioni dei primi.

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

Il reato si configura allorquando si proceda, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli. Soggetti attivi del reato sono gli amministratori, ma i soci beneficiari della restituzione o della liberazione possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

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

Il reato si configura allorquando si proceda alla ripartizione di utili, o acconti sugli utili, non effettivamente conseguiti o destinati per legge a riserva, ovvero alla ripartizione di riserve, anche non costituite con utile, che per legge non possono essere distribuite. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato. Soggetti attivi del reato sono gli amministratori. I soci beneficiari della ripartizione degli utili o delle riserve possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

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

Il reato si configura allorquando siano realizzate riduzioni di capitale sociale, fusioni con altre società o scissioni attuate in violazione delle disposizioni di legge e che cagionino danno ai creditori. Il risarcimento del danno ai creditori prima del giudizio estingue il reato. Soggetti attivi del reato sono gli amministratori.

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

Il reato si configura allorquando si proceda alla formazione o all'aumento in modo fittizio del capitale sociale tramite:

- attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;

- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori e i soci conferenti.

1.3 TUTELA PENALE DEL REGOLARE FUNZIONAMENTO DELLA SOCIETÀ

Impedito controllo (art. 2625 c.c.)

Il reato si configura allorquando si ostacoli o si impedisca lo svolgimento delle attività di controllo e/o di revisione, legalmente attribuite ai soci, ad organi sociali o a società di revisione. La condotta può essere integrata mediante l'occultamento di documenti o l'utilizzo di altri idonei artifici. La pena è aumentata qualora sia cagionato un danno ai soci. Soggetti attivi del reato sono gli amministratori.

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

Il reato si configura allorquando con atti simulati o con frode si determina la maggioranza in assemblea, allo scopo di conseguire, per sé o per altri, un ingiusto profitto. Il reato può essere commesso da chiunque, anche da soggetti esterni alla società.

2 AREE DI RISCHIO

In occasione dell'implementazione dell'attività di mappatura delle attività a rischio, sono state individuate, per la famiglia di reati sopra indicati, le attività "a rischio di reato", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in esame.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "F" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P09- Processo Amministrativo	Stipula ed esecuzione dei contratti, avendo riguardo anche agli aspetti inerenti all'applicazione di penali e le risoluzioni transattive in caso di contestazioni
P09- Processo Amministrativo	Processi di ciclo passivo e contabilità

Processi	Attività sensibile
P10- Processo societario e rapporti con stakeholder	Operazioni societarie straordinarie (tra cui modifiche statuarie)
P09- Processo Amministrativo P10- Processo societario	Redazione del bilancio, del bilancio consolidato, e delle altre comunicazioni sociali
P10- Processo societario	Determinazioni in materia di compenso degli amministratori, destinazioni degli utili e delle riserve
P10- Processo societario	Tenuta dei libri sociali
P10- Processo societario	Convocazione e verbalizzazione delle assemblee dei soci e del CdA
P10- Processo societario	Comunicazione tra soci e società di revisione
P08- Processo finanziario P10- Processo societario	Operazioni societarie effettuate in danno ai creditori
P09- Processo Amministrativo P10- Processo societario	Redazione dei documenti e dei prospetti informativi concernenti la Società e le società appartenenti al Gruppo
P08- Processo finanziario P10- Processo societario	Gestione delle risorse finanziarie, i cui principi sono individuati nel sistema delle procure e deleghe aziendali
P10- Processo societario	Predisposizione e fornitura informazioni o documenti in genere a supporto delle verifiche dell'Organismo di vigilanza
P10- Processo societario	Operazioni sul capitale
P10- Processo societario	Acquisto e vendita di titoli societari
P08- Processo finanziario	Gestione dei flussi finanziari in uscita

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

È necessario che tutte le operazioni svolte nell'ambito delle attività "sensibili" ricevano debita evidenza.

Nell'esecuzione di tali operazioni, occorre che sia garantito il rispetto dei principi di comportamento di seguito indicati:

1. astenersi dal porre in essere condotte tali da integrare le fattispecie di reato illustrate nella presente Parte Speciale F;
2. garantire il rispetto delle regole comportamentali previste nel Codice Etico comportamentale di Justbit, con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua;
3. tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'esecuzione di tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire agli associati e ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;
4. tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e regolamentari vigenti, nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni necessarie per consentire di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della società;
5. garantire il rispetto dei principi di integrità, correttezza e trasparenza così da consentire ai destinatari di pervenire ad un fondato ed informato giudizio sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività;
6. osservare le prescrizioni imposte dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire nel rispetto dei principi etici della società che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;
7. assicurare il regolare funzionamento della società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale prevista dalla legge, nonché la libera formazione della volontà assembleare;
8. gestire con la massima correttezza e trasparenza il rapporto con le Pubbliche Autorità;
9. tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV potrà predisporre controlli dei quali dovrà essere fornita evidenza scritta.

4 PRINCIPI DI CONTROLLO

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi allegati (Sistema Disciplinare, Codice Etico comportamentale, ecc.), i soggetti coinvolti nella gestione delle aree a rischio individuate in relazione ai reati societari di cui all'art. 25 ter del D.lgs. 231/01 sono tenuti, al fine di prevenire e impedire il verificarsi dei reati, al rispetto di una serie di principi di controllo, basati sull'assunto che la trasparenza e la correttezza contabile si fonda sulla verità, accuratezza e completezza delle informazioni di base per le relative registrazioni contabili.

Segnatamente per ogni operazione contabile viene conservata agli atti sociali una adeguata documentazione di supporto dell'attività svolta, in modo da consentire:

- l'agevole registrazione contabile;
- l'individuazione dei diversi livelli di responsabilità;
- Messa a disposizione della adeguata documentazione a supporto per le relazioni finanziarie.

In ogni caso, dovrà tenersi conto, in relazione alle ulteriori specifiche fattispecie di reato di seguito indicate, delle seguenti previsioni.

Le false comunicazioni sociali

Per la prevenzione dei reati relativi alla predisposizione delle comunicazioni indirizzate agli associati e al pubblico in generale, nonché ai fini della formazione del bilancio i processi implementati da Justbit garantiscono:

1. il rispetto dei principi di compilazione dei documenti contabili di cui agli artt. 2423, 2423 bis, 2423 ter c.c.;
2. il rispetto del principio di completezza del bilancio, mediante l'indicazione di tutti i dati prescritti dalla normativa vigente (cfr., artt. 2424 e ss.c.c.);
3. l'elencazione dei dati e delle notizie che ciascuna funzione/direzione interessata deve fornire; l'indicazione delle altre funzioni/direzioni a cui i dati devono essere trasmessi; i criteri per la loro elaborazione; la tempistica di consegna;

4. la trasmissione dei dati alla funzione/direzione responsabile per via informatica, affinché resti traccia dei vari passaggi e siano identificabili i soggetti che hanno operato;
5. la tempestiva trasmissione da parte dell'Unità amministrativa al CdA, della bozza di bilancio, garantendo l'idonea registrazione di tale trasmissione;
6. la giustificazione di ogni eventuale variazione dei criteri di valutazione adottati per la redazione dei documenti contabili sopra richiamati e delle relative modalità di applicazione. Tali situazioni devono, in ogni caso, essere tempestivamente comunicate all'OdV;
7. la preventiva approvazione, da parte dell'assemblea dei soci, delle operazioni della società potenzialmente rilevanti ai fini del Decreto, qualora siano caratterizzate da una discrezionalità di valutazione che possa comportare significativi impatti sotto il profilo patrimoniale o fiscale; per linee e principi etici societari tutte le eventuali operazioni societarie vengono effettuate unicamente sulla base delle strategie di carattere finanziario ed economico finalizzate alla crescita dell'azienda nel mantenimento dei principi di legalità e trasparenza escludendo qualsiasi danni a terzi.
8. La tracciabilità delle operazioni che comportino il trasferimento e/o il deferimento di posizioni creditorie;
9. La tracciabilità di tutti gli scambi documentali tra gli organi societari, al fine di favorire le attività di verifica.
10. La raccolta, verifica e tracciabilità della documentazione fornita alla Società di Revisione;
11. La trascrizione, pubblicazione e archiviazione dei verbali di assemblea e del Consiglio di Amministrazione.

La tutela del capitale sociale

Per la prevenzione dei reati relativi alla gestione delle operazioni concernenti accantonamenti a riserva legale o altre riserve, sottoscrizione ed acquisto di quote sociali, operazioni sul patrimonio, il processo gestito dalla società prevede:

1. l'approvazione, da parte del Consiglio di Amministrazione, della proposta di distribuzione degli utili e delle riserve;
2. l'esplicita approvazione, da parte dell'Assemblea dei soci, di ogni attività relativa, all'acquisizione o alienazione di partecipazioni societarie, nonché in merito alla effettuazione all'accantonamento a riserva legale o altre riserve, a operazioni sul patrimonio della società;

3. per policy aziendale che tutte le operazioni finanziarie sul capitale e sugli utili siano poste in essere unicamente ai fini dello sviluppo societario nel mantenimento dei principi di legalità e trasparenza.

PARTE SPECIALE G- REATI AVENTI FINALITÀ DI TERRORISMO E DI EVERSIONE DELL'ORDINE DEMOCRATICO

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte Speciale "G", l'art. 25-quater del Decreto non elenca specificamente i reati per i quali è prevista la responsabilità dell'ente, limitandosi a richiamare, al primo comma, i delitti previsti dal codice penale e dalle leggi speciali e, al terzo comma, i delitti diversi da quelli disciplinati al comma 1 ma posti in essere in violazione di quanto stabilito dall'art. 2 della Convenzione di New York.

Quanto ai reati richiamati dal primo comma dell'art. 25-quater si riportano, tra gli altri:

Associazioni con finalità di terrorismo e di eversione dell'ordine democratico (art. 270-bis c.p)

I reati di cui al terzo comma dell'art. 25-quater, rientranti nell'ambito di applicazione della Convenzione di New York, sono invece quelli diretti a fornire, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo. In particolare, la Convenzione rinvia ai reati previsti da altre convenzioni internazionali, tra i quali: il dirottamento di aeromobili, gli attentati contro personale diplomatico, il sequestro di ostaggi, l'illecita realizzazione di ordigni nucleari, i dirottamenti di navi, l'esplosione di ordigni, ecc.

In questi casi chi (persona fisica o ente fornito o meno di personalità giuridica) fornisce i fondi o comunque collabora nel loro reperimento deve essere a conoscenza dell'utilizzo che di essi verrà successivamente fatto.

2 AREE DI RISCHIO

C'è innanzitutto da rilevare che appare difficilmente ravvisabile, considerate le finalità di Justbit, in maniera oggettiva, la commissione, nell'interesse della società o comunque a suo vantaggio, dei reati di cui all'art. 25-quater del Decreto,

Tuttavia, in relazione a tale tipologia di illeciti, tenuto conto della numerosità dei rapporti che la società intrattiene quotidianamente con la propria clientela, e, soprattutto delle prescrizioni normative che individuano nel conseguimento di un interesse o vantaggio anche indiretto per la società, una possibile fonte d'imputabilità ai sensi del Decreto 231/2001, sono state individuate le seguenti attività sensibili ed i processi ad esse collegati:

Processi	Attività sensibile
P07- Approvvigionamento P11- Gestione delle commesse	Richieste di acquisto e selezione del fornitore
P04- Gestione delle risorse umane	Ricerca e selezione del personale
P05- Gestione dei sistemi informativi	Gestione degli accessi fisici alle aree riservate
P07- Approvvigionamento	Valutazione e qualificazione dei fornitori

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da ulteriori altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. Effettuare qualsiasi sovvenzione in denaro o altra utilità o in qualsiasi altra, forma di finanziamento a favore di enti o soggetti nazionali o esteri che possano ragionevolmente essere considerati a rischio o sospetti di svolgere attività con finalità di terrorismo;
2. Concludere o intraprendere qualsiasi attività negoziale, di partnership e in generale accordi, con enti e soggetti nazionali o stranieri che possano ragionevolmente essere considerati a rischio o sospetti di svolgere attività con finalità di terrorismo;
3. Concludere o intraprendere qualsiasi attività negoziale, di partnership e in generale accordi, con enti e soggetti nazionali o stranieri inseriti in liste pubbliche segnalati quali soggetti collegati ad attività di terrorismo;
4. Assumere personale segnalato in liste di riferimento come collegato ad attività di terrorismo.

4 PRINCIPI DI CONTROLLO

I processi implementati dalla Justbit garantiscono:

1. la tracciabilità di tutte le attività negoziali e gli accordi di partnership;
2. la tracciabilità totalmente informatica dell'intero processo di approvvigionamento attraverso applicativo dedicato;
3. la selezione dei soggetti con cui vengono intraprese attività negoziali e accordi di partnership, in base a criteri di rettitudine morale, storia personale e competenze professionali;
4. la selezione dei fornitori a fronte di criteri oggettivi di affidabilità, convenienza, adesione a principi di legalità e trasparenza;
5. criteri di selezione e gestione del personale ispirati a imparzialità, merito competenze e professionalità.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE H- REATI CONTRO LA PERSONALITÀ INDIVIDUALE, RAZZISMO E XENOFOBIA

1 TIPOLOGIA DI REATI APPLICABILI

L'art. 5 della legge n. 228/2003, in tema di misure contro la tratta delle persone, aggiunge al decreto 231/01 l'articolo 25-quinquies che prevede l'applicazione di sanzioni amministrative alle persone giuridiche, società e associazioni per la commissione di delitti contro la personalità individuale.

L'art. 25-quinquies è stato successivamente integrato ad opera dell'art. 10, legge n. 38 del 6 febbraio 2006, contenente "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", che modifica l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600-ter e 600-quater c.p.), includendo anche le ipotesi in cui tali illeciti siano commessi mediante l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori degli anni diciotto o parti di esse (c.d. "pedopornografia virtuale", ai sensi del rinvio al nuovo art. 600-quater.1, c.p.).

La citata legge n. 38/2006 è intervenuta anche a modificare le disposizioni di cui agli articoli 600-bis, 600-ter e 600-quater, relativi ai delitti di prostituzione minorile, pornografia minorile e detenzione di materiale pornografico, per i quali era già prevista la responsabilità amministrativa degli Enti.

I delitti potenzialmente applicabili sono:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 cp);
- Pornografia minorile - Offerta o cessione di materiale pedopornografico, anche per via telematica (art. 600-ter c.p.);
- Adescamento di minorenni (art. 609-undecies c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.).

Inoltre, in attuazione della Decisione Quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia, la Legge Europea 2017 ha disposto l'aggiunta al corpo normativo del Decreto Legislativo 8 giugno 2001, n. 231 dell'art. 25, in materia di lotta al razzismo e alla xenofobia.

I reati-presupposto sono quelli previsti dall'articolo 3, comma 3, della legge 13 ottobre 1975, n. 654, così come modificato dalla stessa Legge Europea, ai sensi del quale: "si applica la pena della

reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia, della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello Statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232".

Il primo comma dell'articolo 25 prevede che, in caso di commissione dei reati di cui sopra, all'ente sia irrogata una sanzione per quote per un controvalore da 51.600 euro a 1.239.200 euro. Alla sanzione pecuniaria, si possono poi aggiungere le sanzioni interdittive.

All'ultimo comma, la disposizione normativa prevede, come ipotesi aggravata, che se l'ente o la sua organizzazione sono stabilmente utilizzati allo scopo, unico o prevalente, di consentire o agevolare la commissione dei delitti di cui sopra si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa di Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi della società rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati contro la personalità individuale.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

Applicando nei confronti dei lavoratori le previsioni e le tutele specificatamente previste dal Contratto Collettivo Nazionale di Lavoro, relativamente allo specifico reato di "Intermediazione illecita e sfruttamento del lavoro", la commissione di un atto illecito da parte di Justbit appare del tutto remota. Appare altresì remota la possibilità di commissione a proprio vantaggio del reato di Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa", in considerazione delle relative modalità di realizzazione previste dalla norma.

Comunque, in relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "H" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P07- Approvvigionamento P11- Gestione della commessa	Richieste di acquisto e selezione del fornitore
P04- Gestione delle risorse umane	Ricerca e selezione del personale
P05- Gestione dei sistemi informativi	Gestione del sito internet aziendale
P07- Approvvigionamento	Valutazione e qualificazione dei fornitori

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari devono in generale conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- il Codice Etico comportamentale;
- ogni altra documentazione relativa al sistema di controllo interno in essere nella Justbit;

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25-quinques del D.lgs. 231/2001);
2. violare i principi presenti in società in materia di utilizzo delle risorse elaborative, dei computer e della rete Interne, in difformità all'uso lecito inerente alla semplice attività lavorativa;

3. organizzazione o partecipazione a qualsiasi iniziativa quale associazione, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi che in qualche modo utilizzi il nome di Justbit per promuovere o propagandare il razzismo o la xenofobia o in qualsiasi modo preveda la negazione della Shoah o dei crimini contro l'umanità;
4. utilizzare locali della sede di Justbit al fine di qualsiasi iniziativa associazionistica o propagandistica di istigazione al razzismo, alla xenofobia, alla negazione della Shoah e dei crimini di guerra e contro l'umanità;
5. esporre presso la propria postazione di lavoro stemmi, disegni, vessilli, bandiere, vignette satiriche o epigrafi che in qualche modo possano costituire esaltazione del nazismo, del fascismo o possano promuovere o incitare al razzismo o alla xenofobia;
6. porre in essere qualsiasi episodio di discriminazione nei confronti di colleghi o collaboratori per motivi di razza, religione, provenienza etnica, colore della pelle, credo politico, orientamenti sessuali, caratteristiche fisiche;
7. distribuire a colleghi o collaboratori volantini, scritti, disegni o porre in essere l'esercizio di qualsiasi forma di propaganda di iniziative o organizzazioni volte al razzismo, alla xenofobia o al negazionismo o alla mera banalizzazione della Shoah o dei crimini di guerra e contro l'Umanità.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli Organi Sociali della società (e i Dipendenti ed i Soggetti terzi nella misura necessaria alle funzioni dagli stessi svolte), devono in generale conoscere e rispettare le norme inerenti alla prevenzione dei reati di pornografia minorile e detenzione di materiale pornografico.

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

8. tenere un comportamento corretto nell'uso sia dei computer, sia del software concessi in uso alla Justbit, nonché degli accessi Internet, che devono essere finalizzati unicamente all'attività lavorativa;
9. non accedere in nessun caso a siti pornografici;
10. non cliccare su banner presenti su altri siti che reindirizzano a siti pornografici.

4 PRINCIPI DI CONTROLLO

I processi implementati dalla Justbit garantiscono il rispetto dei seguenti principi:

1. In fase di selezione del personale, qualsiasi condanna per reati di istigazione all'odio razziale o alla violenza o alla negazione dei crimini di guerra e contro l'umanità deve costituire elemento di immediata esclusione dalla candidatura;
2. qualsiasi episodio che dimostri inequivocabilmente atteggiamenti o tendenze razziste, xenofobe o negazioniste o discriminazione nei confronti di clienti, colleghi, collaboratori deve essere oggetto di segnalazione all'OdV e all'AD, costituendo violazione del Codice etico comportamentale adottato dalla Justbit e pertanto condotta sanzionabile;
3. in caso si richieda la disponibilità di locali di Justbit a scopo associazionistico o ricreativo, il richiedente deve motivare la richiesta a AD e sottoporre la stessa ad approvazione;
4. la selezione dei soggetti con cui vengono intraprese attività negoziali e accordi di partnership, avviene in base a criteri di rettitudine morale, storia personale e competenze professionali;
5. la selezione dei fornitori avviene a fronte di criteri oggettivi di affidabilità, convenienza, adesione a principi di legalità e trasparenza;
6. applicazione di criteri di selezione e gestione del personale ispirati unicamente a imparzialità, merito, competenze e professionalità.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE I- REATI IN MATERIA DI ABUSI DI MERCATO

1 TIPOLOGIA DI REATI APPLICABILI

I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Abuso di informazioni privilegiate (art. 184 del Testo unico della finanza)

Il reato si configura nel momento in cui un soggetto, essendo entrato (direttamente) in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dello stesso, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime – c.d. trading;

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio cui è preposto (a prescindere dalla circostanza che i terzi destinatari utilizzino effettivamente l'informazione "comunicata") - c.d. tipping;

c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a) - c.d. tuyuatage.

In aggiunta a tali soggetti l'art. 184 T.U.F. estende i divieti di trading, tipping e tuyuatage a chiunque sia entrato in possesso di informazioni privilegiate a motivo della preparazione o esecuzione di attività delittuose - c.d. criminal insider.

Manipolazione del mercato (art. 185 del Testo unico della finanza.)

Tale ipotesi di reato si configura a carico di chiunque diffonda notizie false o ponga in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, ed è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.

Non è punibile chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del regolamento (UE) n. 596/20141054. Il giudice può aumentare la multa fino al triplo o fino al maggiore importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati transnazionali.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati previsti dalla presente parte speciale applicabili a Justbit, sono state individuate le seguenti aree di rischio ed i processi ad esse collegati:

Processi	Attività sensibile
P10- Processo finanziario	Tutte le attività

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Destinatari devono in generale conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- il Codice Etico comportamentale;
- ogni altra documentazione relativa al sistema di controllo interno in essere nella Justbit.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. comunicare dati alterati e comunque non veritieri sulla situazione economica e patrimoniale di Justbit stessa e di società quotate che detengono quote societarie, per l'elaborazione e la predisposizione di bilanci, relazioni, prospetti o altre comunicazioni sociali;
2. diffondere qualsiasi informazione non veritiera allo scopo di causare una sensibile alterazione del prezzo di strumenti finanziari, in proprio vantaggio o in vantaggio di altre società che detengono quote societarie;
3. porre in essere qualsiasi tipo di operazione simulata per gli scopi di cui sopra;
4. diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso internet, o tramite qualsiasi altro mezzo, per acquisire un vantaggio proprio o per altre società che detengono quote societarie;
5. effettuare qualsiasi operazione fuori dalle regole del mercato;
6. rivelare a terze parti informazioni privilegiate relative alla società e a società quotate che detengono quote societarie, ferme restando eventuali richieste da parte di Autorità o il caso in cui la comunicazione di tali informazioni siano regolamentate da appositi accordi in cui le parti si impegnino all'utilizzo delle stesse informazioni ai soli fini contrattualizzati e alla totale riservatezza;
7. divulgare informazioni privilegiate in qualsiasi modo acquisite, anche con riferimento ad altre società che detengono quote societarie.

4 PRINCIPI DI CONTROLLO

Per la prevenzione dei reati relativi all'abuso di informazioni privilegiate e al così detto "market abuse" i processi implementati da Justbit garantiscono:

1. controlli di secondo livello espletati dalle competenti funzioni aziendali sulle operazioni finanziarie effettuate da società quotate aventi quote societarie, anche per il tramite di outsourcer esterni;
2. identificazione di potenziali comportamenti manipolativi messi in atto dalla clientela.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE L- REATI COMMESSI IN VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte Speciale "L", si provvede di seguito a fornire l'elenco dei reati in essa contemplati, indicati nell'art. 25-septies del Decreto:

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

Tali reati sono originati da comportamenti di natura colposa oltre che dolosa e l'attività a rischio di reato è rappresentata dal "non adempimento" ai dettami richiesti dalla normativa relativa alla sicurezza sul lavoro.

L'applicabilità di tali reati a Justbit è stabilita direttamente dalla legge come specificato negli articoli 3 e 30 del D.lgs. 81/2008 (Testo Unico sulla Sicurezza sul Lavoro):

Si precisa che l'elemento essenziale ed unificante delle varie e possibili forme di responsabilità del datore di lavoro ai fini dell'applicabilità dell'art. 25-septies del D.lgs. 231/2001, è uno solo ed è rappresentato dalla 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.

Il novero degli obblighi in materia antinfortunistica si accresce ulteriormente ove si consideri che l'obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza nei termini sopra esposti (forme di protezione oggettiva) ma deve intendersi anche in maniera dinamica implicando l'obbligo di informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

2 AREE DI RISCHIO

Con precipuo riferimento ai reati oggetto della presente Parte Speciale l, si evidenza innanzitutto, con riguardo alla identificazione degli ambiti aziendali, che non è possibile escludere aprioristicamente alcun ambito di attività, poiché tali reati potrebbero interessare la totalità delle componenti aziendali. Ne consegue che tutte le aree di Justbit sono potenzialmente a rischio di inadempimento.

Per quanto attiene l'individuazione e l'analisi dei rischi potenziali, la quale dovrebbe considerare le possibili modalità attuative dei reati in seno alla società, si rileva altresì che l'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dalla società sulla scorta della legislazione prevenzionistica vigente, ed in particolare dagli artt. 28 e ss. Del D.Lgs. 81/2008 e s.m.i..

In altri termini, i reati oggetto della presente Parte Speciale L potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno a Justbit, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

C'è in ultima istanza da evidenziare che in generale, considerate le attività facenti parte dell'oggetto sociale di Justbit, le stesse sono da considerare, per natura e modalità di svolgimento, a rischio basso relativamente all'accadimento di eventi infortunistici.

Di seguito un prospetto riepilogativo delle aree ritenute a rischio dei reati societari, nel cui ambito sono indicate le funzioni/direzioni coinvolte e le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati di violazione della normativa antinfortunistica nonché, i principali controlli previsti con riferimento alle attività che sono poste in essere nelle aree "a rischio reato". I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

Processi	Attività sensibile
P06- Gestione della Sicurezza e Ambiente	Pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro;
P06- Gestione della Sicurezza e Ambiente	Sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro
P06- Gestione della Sicurezza e Ambiente	Individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro; tra questi anche quelli derivanti dall'insorgenza di fattori esterni straordinari (emergenza sanitaria)
P06- Gestione della Sicurezza e Ambiente P04- Gestione delle risorse umane	Attività di formazione e informazione in tema di salute, sicurezza e igiene sul lavoro
P07- Approvvigionamento P06- Gestione della SSL e Ambiente	Rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro
P06- Gestione della Sicurezza e Ambiente	Controllo operativo delle attività

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

Justbit si impegna, come previsto dalla normativa vigente, a garantire il rispetto della normativa in tema di tutela della salute e sicurezza sul lavoro, nonché ad assicurare, in generale, un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività lavorativa, anche attraverso:

1. la valutazione dei rischi per la salute e la sicurezza;
2. la programmazione della prevenzione, mirando ad un complesso che, nell'attività di prevenzione, integri in modo coerente le condizioni tecniche, produttive della società, nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;
3. l'eliminazione dei rischi ovvero, ove ciò non sia possibile, la loro riduzione al minimo – e, quindi, la loro gestione - in relazione alle conoscenze acquisite in base al progresso tecnico;
4. il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature informatiche e nella definizione dei metodi di lavoro anche al fine di attenuare il lavoro monotono e quello ripetitivo;
5. la riduzione dei rischi alla fonte;
6. la sostituzione di ciò che è pericoloso con ciò che non lo è o è meno pericoloso;
7. la limitazione al minimo del numero di Lavoratori che sono, o che possono essere, esposti a rischi;
8. il controllo sanitario dei Lavoratori in funzione dei rischi specifici;
9. l'allontanamento di un Lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e, ove possibile, l'adibizione ad altra mansione;
10. la comunicazione ed il coinvolgimento adeguati dei Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla salute ed alla sicurezza sul lavoro; in quest'ottica, particolare rilevanza è riconosciuta alla consultazione preventiva dei soggetti interessati in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
11. la formazione e l'addestramento adeguati dei Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, rispetto alle questioni connesse alla salute ed alla sicurezza sul lavoro, al fine di assicurare la consapevolezza della importanza della conformità delle azioni rispetto al Modello e delle possibili conseguenze dovute a comportamenti che si

discostino dalle regole dettate dallo stesso; in quest'ottica, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti che possono incidere sulla salute e la sicurezza sul lavoro;

12. la definizione di adeguate misure igieniche, nonché di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei Lavoratori e di pericolo grave e immediato;
13. l'uso di segnali di avvertimento a sicurezza;
14. la regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

4 PRINCIPI DI CONTROLLO

Justbit ha deciso di implementare un apposito sistema di controllo dei rischi per la salute e la sicurezza sul lavoro.

Tale sistema è integrato con la gestione complessiva dei processi della società.

In particolare, in seno alla Justbit è prevista la predisposizione e l'implementazione di apposite norme di comportamento in materia di salute e sicurezza sul lavoro, redatte sulla scorta della normativa prevenzionistica vigente.

Ai fini della predisposizione di tali principi di controllo, la società ha rivolto particolare attenzione all'esigenza di garantire il rispetto dei seguenti principi:

1. formale e documentata identificazione, attraverso nomine specifiche rilasciate da parte dell'AD, in qualità di Datore di lavoro, delle responsabilità in materia di salute e sicurezza sul lavoro (ad es. Medico competente, ecc.);
2. assunzione da parte del Datore di Lavoro del Ruolo di Responsabile del servizio prevenzione e protezione (RSPP);
3. formale nomina del Medico Competente, il quale ha espressamente accettato l'incarico con conseguente attivazione di appositi ed adeguati flussi informativi verso il Medico Competente in relazione ai processi ed ai rischi connessi alle attività svolte;
4. identificazione e valutazione di tutti i rischi per la sicurezza e per la salute dei Lavoratori applicabili alle attività svolte, ivi compresi quelli riguardanti i Lavoratori esposti a rischi particolari, tenendo in adeguata considerazione la struttura della società, la natura dell'attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, le

attrezzature informatiche impiegate nelle attività. La valutazione dei rischi è documentata attraverso l'elaborazione, ai sensi della normativa prevenzionistica vigente, di un DVR; nell'ipotesi in cui siano rilevati rischi da interferenza, viene predisposto e sottoscritto, previa valutazione dei rischi stessi, il DUVRI. La relativa documentazione viene conservata ed archiviata.

5. adozione di adeguate misure ai fini della prevenzione degli incendi e dell'evacuazione dei Lavoratori dalla sede di Justbit;
6. organizzazione delle misure per la gestione delle emergenze e primo soccorso presso la sede;
7. predisposizione e aggiornamento, a cura del Medico Competente, del protocollo sanitario della società volto sia ad assicurare l'implementazione delle misure necessarie a garantire la tutela della salute e dell'integrità psico-fisica dei Lavoratori, sia a fornire una valutazione della situazione sanitaria esistente presso la società, sia a programmare l'effettuazione delle visite mediche;
8. definizione delle modalità ed i termini per l'acquisizione e la trasmissione dei dati informativi relativi agli infortuni sul lavoro, incluso per ciò che attiene la necessaria informazione dell'OdV;
9. definizione, documentazione, implementazione, monitoraggio e periodico aggiornamento di un programma di informazione e coinvolgimento dei Destinatari - con particolare riguardo ai Lavoratori neo-assunti, - in materia di salute e sicurezza sul lavoro, che preveda una puntuale informazione dei Lavoratori;
10. definizione di un sistema di flussi informativi che consenta la circolazione delle informazioni all'interno della società, al fine sia di favorire il coinvolgimento e la consapevolezza di tutti i Destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, sia di assicurare la tempestiva ed adeguata evidenza di eventuali carenze o violazioni del Modello, ovvero degli interventi necessari al suo aggiornamento;
11. definizione, documentazione, implementazione, monitoraggio e periodico aggiornamento di un programma di formazione ed addestramento periodici dei Destinatari - con particolare riguardo ai Lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione - in materia di salute e sicurezza sul lavoro, anche con riferimento ai differenti profili di rischio (ad esempio, squadra antincendio, pronto soccorso, ecc.).

12. monitoraggio e documentazione del regolare svolgimento e la partecipazione ai corsi di in materia di salute, igiene e sicurezza sul lavoro
13. collaborazione con il RLS affinché lo stesso possa verificare, o ve lo ritenga opportuno, anche attraverso il libero accesso alle informazioni e alla documentazione di SSL, il rispetto dell'applicazione delle misure di sicurezza e delle misure di protezione;
14. con cadenza annuale, svolgimento, a cura del Datore di Lavoro e con la partecipazione del Medico competente, di apposite riunioni con i RLS, volte ad approfondire le questioni connesse alla prevenzione ed alla protezione dai rischi. Le riunioni devono essere adeguatamente formalizzate mediante la redazione di apposito verbale, il quale dovrà essere inviato all'OdV;
15. formalizzazione pubblicizzazione del divieto di fumare in tutti gli ambienti di lavoro, con realizzazione di apposite attività di vigilanza;
16. richiesta ai Lavoratori, salvo eccezioni debitamente motivate, di non riprendere la loro attività in situazioni di lavoro in cui persistono pericoli gravi e immediati;
17. svolgimento delle attività lavorative nel rispetto delle prescrizioni indicate nella cartellonistica e della segnaletica di sicurezza;
18. nei trasferimenti interni ed esterni, sia con mezzi propri che noleggiati a nome della società, devono essere osservate tutte le necessarie ed opportune precauzioni in materia di salute e sicurezza sul lavoro (ad esempio, rispetto della segnaletica stradale e del codice della strada.);
19. manutenzione ordinaria e straordinaria dei dispositivi di sicurezza presso la sede (ad esempio, lampade di emergenza, estintori, ecc.).
20. l'assegnazione, la verifica e la gestione degli affidamenti, viene effettuata e monitorata sulla base e nel rispetto di specifiche regole interne formalizzate.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE M- REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI E UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO E TRASFERIMENTO FRAUDOLENTO DI VALORI

1 TIPOLOGIA DI REATI APPLICABILI

L'art. 63, comma 3, D.lgs. 231/2007 introduce nel decreto n. 231/2001 l'art. 25-octies, che estende la responsabilità amministrativa degli Enti ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.

In particolare, si citano i seguenti articoli:

- 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)

Si riporta di seguito una sintetica descrizione dei reati richiamati all'art. 25-octies del D.lgs. n. 231/2001, nonché una esemplificazione delle possibili modalità di attuazione dei reati, fermo restando che, ai sensi dell'art. 26 del Decreto, Justbit, potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

Il D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023 "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia personale della magistratura e della pubblica amministrazione" ha inoltre introdotto nell' Art.25-octies.1 D.Lgs231/01 (Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori) il delitto di

- trasferimento fraudolento di valori (art. 512-bis c.p.).

Ricettazione (art. 648 c.p.)

Il bene giuridico tutelato dalla norma è il patrimonio (secondo alcuni l'interesse tutelato è anche quello della amministrazione della giustizia).

Il delitto di ricettazione può essere integrato da chiunque - senza che sia configurabile concorso nel reato presupposto - acquista, riceve od occulta denaro o cose provenienti da un qualsiasi

delitto o, comunque, si intromette per farle acquistare, ricevere od occultare, al fine di ottenere per sé o per altri un profitto.

Le pene previste sono quelle della reclusione da 2 a 8 anni e la multa da 516 a 10.329 euro. Qualora il fatto sia giudicato di particolare tenuità, le pene previste sono la reclusione fino a 6 anni e la multa sino 516 euro.

Per la ricorrenza della fattispecie in questione è necessario che il denaro o le cose provengano dalla commissione di un precedente delitto (ad es., furto, rapina, ecc.) che costituisce il presupposto della ricettazione. È, altresì, necessario che l'autore del reato abbia come finalità quella di perseguire - per sé o per terzi - un profitto, che può anche non essere di carattere patrimoniale.

Le nozioni di acquisto e ricezione fanno riferimento a tutti gli atti mediante i quali il soggetto agente entra nella disponibilità materiale del denaro o delle cose provenienti da delitto.

L'occultamento implica il nascondimento del denaro o delle cose.

Sotto il profilo oggettivo, è pure rilevante l'intromissione nell'acquisto, nella ricezione o nell'occultamento dei beni, per la cui integrazione è sufficiente che il mediatore metta in contatto, anche in modo indiretto, le parti.

Perché l'autore dei fatti sia punibile per il delitto di ricettazione è necessario che agisca con dolo – anche nella forma eventuale - ossia che sia a conoscenza della provenienza illecita del denaro o delle cose e le voglia acquistare, ricevere, occultare o, dolosamente, voglia intromettersi nel favorire queste condotte.

Un ulteriore elemento della fattispecie è la necessaria ricorrenza del dolo specifico, ovvero l'autore del fatto deve essere consapevole di raggiungere – o di far raggiungere a terzi – un profitto dal reato.

L'assenza del dolo tipico della ricettazione potrebbe portare, comunque, ad una incriminazione per incauto acquisto (art. 712 c.p.).

Riciclaggio (art. 648 bis c.p.)

Il delitto di riciclaggio è un c.d. reato plurioffensivo, in quanto i beni tutelati dalla norma possono essere diversi, ossia l'amministrazione della giustizia, il patrimonio e, a seconda delle fattispecie, anche l'ordine pubblico ed economico.

Il delitto di riciclaggio punisce chiunque, senza che sia configurabile concorso nel reato presupposto, 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 la identificazione della loro provenienza delittuosa.

Le pene sono quelle della reclusione da 4 a 12 anni e della multa da 1.032 a 15.493 euro. La pena è aumentata qualora il reato venga commesso nell'esercizio di una attività professionale, mentre è diminuita se il denaro, i beni o le altre utilità provengono da delitto non colposo per il quale è stabilita la pena della reclusione inferiore nel massimo a 5 anni.

Come per il delitto di ricettazione, anche per le ipotesi di riciclaggio, è necessario che il denaro, i beni o le altre utilità (rientrano nella previsione della norma anche le aziende, i titoli, i diritti di credito) provengano dalla commissione di un precedente delitto non colposo (ad es., reati tributari, reati contro il patrimonio, ecc.) che ne costituisce il presupposto.

La condotta della sostituzione del denaro, dei beni o di altre utilità di provenienza delittuosa, consiste nell''occultamento'' della illegittima provenienza del denaro, dei beni, delle utilità mediante il rimpiazzo degli stessi".

Il trasferimento implica il passaggio del denaro, dei beni o delle altre utilità da un soggetto ad un altro soggetto in modo che si disperdano le tracce della illegittima provenienza.

L'ulteriore condotta che punisce qualsivoglia operazione che sia tale da ostacolare la identificazione del denaro, dei beni o delle altre utilità è idonea a sanzionare qualsiasi attività diretta a riciclare il denaro, i beni o le altre utilità.

Sotto il profilo dell'elemento soggettivo, è richiesta la ricorrenza del dolo generico, inteso quale consapevolezza della provenienza delittuosa del bene e volontà della realizzazione delle condotte sopra indicate (sostituzione, trasferimento, compimento di altre operazioni al fine di ostacolare l'identificazione di denaro, dei beni o delle utilità).

A titolo esemplificativo, il delitto di riciclaggio potrebbe essere integrato nei casi in cui, a seguito della ricezione di beni e/o finanziamenti in denaro che costituiscono proventi di reato e sui quali sono stati omessi o effettuati parzialmente i controlli previsti, i dipendenti dell'Ente compiano operazioni quali: a) nel caso dei beni, l'impiego degli stessi presso l'Ente (si pensi, ad es., alla ricezione di computer oggetto di furto che poi vengono utilizzati o trasferiti presso un'altra società); b) nel caso del denaro, l'acquisto di beni o servizi in favore dell'Ente (si pensi, ad es., all'utilizzo di somme provenienti da un precedente reato tributario per acquistare una partita di nuove attrezzature nell'interesse dell'Ente).

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

Con riferimento al reato in questione gli interessi tutelati sono il patrimonio e ,in generale, l'ordine economico.

Salvo che la condotta sia riconducibile alle ipotesi di cui all'art 648 (ricettazione) o all'art. 648 bis (riciclaggio), è punibile chiunque impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, sempre che l'autore non abbia concorso alla realizzazione del reato presupposto (ad es., furto, reati tributari, reati di falso, ecc.).

Le pene sono quelle della reclusione da 4 a 12 anni e della multa da 1.032 a 15.493 euro. La pena è aumentata qualora il reato venga commesso nell'esercizio di una attività professionale, mentre è diminuita se il fatto sia qualificato come di particolare tenuità.

La nozione di "impiego" può riferirsi ad ogni forma di utilizzazione di capitali illeciti e, quindi, non si riferisce al semplice investimento.

Il riferimento alle attività economiche e finanziarie è riconducibile ad un qualsivoglia settore idoneo a far conseguire profitti (ad es., attività di intermediazione, ecc.).

Sotto il profilo dell'elemento soggettivo, è richiesta la ricorrenza del dolo generico, inteso quale consapevolezza della provenienza delittuosa del bene e volontà della realizzazione della condotta tipica sopra descritta.

In via astratta, il reato potrebbe verificarsi nel momento in cui i dipendenti dell'Ente a ciò deputati, pur consapevoli di aver ricevuto denaro, beni, o utilità provenienti da delitto - in quanto, per esempio, all'esito della attività di controllo prevista dalle procedure dell'Ente è emerso che il denaro è transitato su un conto intestato ad una società o a persone fisiche segnalate dalle liste c.d. antiterrorismo - utilizzino le somme in questione per effettuare investimenti, anche a mezzo di società di intermediazione.

Autoriciclaggio (art. 648 ter-comma 1 c.p.)

Con la Legge 186 del 15 dicembre 2014, "Disposizioni in materia di emissione e rientro di capitali all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio" è stata finalmente introdotta nel Codice Penale Italiano l'autonoma figura dell'Autoriciclaggio.

Il nuovo reato previsto dall'art. 648-ter, sanziona la condotta di chi, dopo aver commesso il reato presupposto, provvede a sostituire, trasferire od occultare i proventi del reato stesso - denaro, beni o altre utilità - per investirli o immetterli in attività economiche, finanziarie, imprenditoriali o speculative.

La punibilità è subordinata alla condizione che la condotta di trasferimento o sostituzione sia concretamente idonea a ostacolare la provenienza delittuosa del provento del reato. Di contro, uno specifico esimente è previsto nei casi in cui il denaro, i beni o le utilità vengano destinati alla mera utilizzazione o godimento personale del reo.

La nuova disposizione elenca tassativamente le condotte passibili di incriminazione ovvero l'impiego, la sostituzione ed il trasferimento. Autorevole dottrina sostiene che con il termine impiego il legislatore abbia inteso colpire l'utilizzazione del denaro, dei beni o delle altre utilità economiche, provenienti dal reato presupposto, per un determinato e specifico fine. La condotta di sostituzione ricomprenderebbe invece tutte quelle operazioni volte a rimpiazzare il denaro, i beni o le altre utilità con altri e diversi beni mentre il trasferimento atterrebbe allo spostamento dei proventi del reato nel patrimonio altrui.

Il delitto in esame previsto dall'art. 648-ter comma.1 del Codice Penale, viene punito con la reclusione da 2 a 8 anni e la multa da € 5.000 a € 25.000, salvo prevedere, al secondo comma, una pena dimezzata qualora il delitto presupposto dell'autoriciclaggio sia punito con la reclusione inferiore nel massimo a 5 anni.

Si ritiene che i principi di controllo adottati da Justbit per l'abbattimento del rischio di incorrere in "responsabilità amministrativa" per la commissione dei reati ex artt. 648 bis e 648 ter c.p. possono risultare efficaci anche per il contrasto del reato di autoriciclaggio.

Trasferimento fraudolento di valori (art. 512 bis c.p.)[22]

L'articolo punisce chi, salvo che il fatto costituisca più grave reato, attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di ricettazione, riciclaggio e impiego di denaro o beni di provenienza illecita.

2 AREE DI RISCHIO

In occasione dell'implementazione dell'attività di mappatura delle attività a rischio, sono state individuate, per ciascuno dei reati sopra indicati, le attività considerate "a rischio", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in esame.

[22] Reato introdotto dal D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023 "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia personale della magistratura e della pubblica amministrazione"

Di seguito un prospetto riepilogativo delle aree ritenute a rischio dei reati di cui alla presente sezione, nel cui ambito sono indicate le funzioni/direzioni coinvolte e le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati di ricetttazione, riciclaggio e autoriciclaggio nonché, i principali controlli previsti con riferimento alle attività che sono poste in essere nelle aree "a rischio reato". I risultati complessivi di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "M" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P07- Approvvigionamento P11- Gestione delle commesse	Nell'ambito dei contratti con i fornitori, - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento - gestione e segnalazione delle anomalie
P10- Processo societario	Operazioni societarie straordinarie
P08- Processo finanziario	Gestione dei conti correnti bancari
P09- Processo Amministrativo	Compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione
P09- Processo Amministrativo	Predisposizione delle dichiarazioni fiscali periodiche
P09- Processo Amministrativo	Liquidazione delle imposte
P08- Processo finanziario	Gestione dei flussi finanziari in entrata, con particolare riguardo alla gestione dei crediti
P08- Processo finanziario	Gestione dei flussi finanziari in uscita

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, da ulteriori altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nelle specifiche procedure e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- violare i principi di controllo di Justbit previsti nella presente parte speciale.

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra:

1. occorre garantire il rispetto delle previsioni contenute nel Codice Etico comportamentale;
2. nell'ambito dei rapporti con i consulenti, i fornitori, i partner commerciali e, in genere, con le controparti contrattuali, deve essere garantito il rispetto dei principi di correttezza, trasparenza e buona fede;
3. divieto di ricevere o accettare la promessa di pagamento in contanti, in alcun modo, in alcuna circostanza;
4. divieto di compiere operazioni che presentino il rischio di essere implicati in vicende relative a riciclaggio di denaro proveniente da attività criminali;
5. divieto di effettuare qualunque tipo di pagamento nell'interesse di Justbit o di altre società che detengono quote societarie in mancanza di adeguata documentazione di supporto;
6. salvo l'impiego per anticipazione spese da sostenere nell'ambito dell'operatività delle commesse e per viaggi e trasferte, comunque opportunamente tracciabili, soggette a giustificazione e autorizzazione preventiva da parte dell'Unità amministrativa attraverso modulistica specifica, sempre per importi limitati e comunque rientranti nei limiti di legge, divieto di utilizzo del contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie, nonché il divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia;
7. con riferimento alla attendibilità commerciale/professionale dei fornitori e dei partner devono essere richieste tutte le informazioni necessarie, utilizzando all'uopo anche gli strumenti messi a disposizione da consulenti esterni;

8. gli incarichi conferiti ad eventuali aziende di servizi e/o persone fisiche che curino gli interessi economico/finanziari di Justbit devono essere anch'essi redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;
9. è necessario che le funzioni competenti assicurino il controllo della avvenuta regolarità dei pagamenti nei confronti di tutti le controparti; in particolare, dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
10. il controllo sia formale che sostanziale (verifica della sede legale della società controparte, verifica degli istituti di credito utilizzati, verifica relativamente all'utilizzo di società fiduciarie) deve essere garantito con riferimento ai flussi finanziari di Justbit e ai pagamenti verso terzi;
11. devono essere rispettati scrupolosamente i requisiti minimi fissati ai fini della selezione dei soggetti offerenti i beni e/o servizi che Justbit intende acquisire e fissati i criteri di valutazione delle offerte in caso di conclusione di accordi/joint venture finalizzati alla realizzazione di investimenti. In via generale deve essere garantita la massima trasparenza;
12. deve essere assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dai principi di controllo interni, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività ''sensibili'' nelle aree classificate ''a rischio reato'';
13. rispettare i termini e le modalità previsti dalla normativa applicabile per la predisposizione delle dichiarazioni annuali e per i conseguenti versamenti relativi alle imposte sui redditi e sul valore aggiunto.
14. coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all''OdV eventuali situazioni di irregolarità.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'OdV avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

4 PRINCIPI DI CONTROLLO

Il sistema dei controlli di Justbit è volto a garantire:

1. La gestione informatica dell'intero ciclo attivo e ciclo passivo gestiti attraverso software dedicati e con accesso limitato per garantire la tracciabilità e la corrispondenza di tutti i flussi in entrata e in uscita con effettive prestazioni rese/ricevute;
2. La possibilità di fatturazione da parte del fornitore unicamente con indicazione nel documento contabile del numero di ordine di acquisto univocamente assegnato dall'applicativo ad accettazione del preventivo inviato;
3. la verifica sulla corrispondenza quantitativa e qualitativa tra gli items risultanti dal documento contabile dei servizi e beni acquistati e quelli risultanti dall'ordine di acquisto, al fine di identificare eventuali elementi attivi per un ammontare superiore/inferiore a quello effettivo o elementi passivi fittizi utilizzando una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
4. il controllo formale e sostanziale per tutti i beni e servizi acquisiti;
5. la verifica di corrispondenza tra la transazione finanziaria disposta e la relativa documentazione di supporto disponibile;
6. la verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nella transazione;
7. la predisposizione di controlli di riconciliazione contabile tra le somme pagate e i servizi e i beni ricevuti;
8. la qualificazione e valutazione qualitativa del fornitore attraverso applicativo Alyante ® secondo criteri basati sulla effettiva qualità del bene o servizio fornito;
9. transazioni finanziarie, attraverso operatori dotati di presidi manuali e informatici e/o telematici atti a prevenire fenomeni di riciclaggio;
10. evidenza documentale e tracciabile del processo di selezione e valutazione dei fornitori attraverso applicativo Alyante®;
11. la richiesta di almeno tre preventivi di acquisto al fine di garantire la necessaria competitività e valutazione circa la congruità dei prezzi offerti rispetto ai valori medi di mercato, salvo casi di estrema urgenza o necessità di forniture in settori altamente specializzati per cui è prevalente il criterio di assicurazione di qualità del bene/servizio richiesto;
12. Adempimento degli obblighi di tracciabilità dei flussi finanziari in caso di appalti pubblici di lavori, servizi e forniture (rif. Legge 13 agosto 2010, n. 136, art. 3).

Inoltre, di seguito sono indicati altri principi di controllo applicati e che i Destinatari sono tenuti a rispettare e che potranno, ove ritenuto opportuno, essere implementati in specifiche procedure aziendali:

13. Tutte le operazioni straordinarie societarie vengono sempre sottoposte ad approvazione nell'ambito della assemblea dei soci e opportunamente deliberate e verbalizzate. Eventuali proposte provenienti dai soci vengono valutate unicamente in base a criteri di sviluppo aziendale e valore strategico;
14. Tutta la documentazione contabile è gestita tramite software gestionale e l'accesso è oggetto di profilazione per gli addetti della unità ammimnistrativa. Qualsiasi modifica alle scritture contabili è bloccata o limitata in funzione del soggetto utilizzatore e secondo i criteri di progettazione del software in coerenza con quanto stabilito dalla legislazione vigente;
15. Tutti i rapporti con gli istituti bancari vengono gestiti dal soggetto avente poteri di rappresentanza legale. L'AD ha in tutte le operazioni possibilità di accesso al fine di esercitare il suo potere di sorveglianza. I poteri al Responsabile dell'unità amministrativa relativamente ai flussi di pagamento sono stati delegati in ambito di CdA;
16. Con riferimento alla gestione dei flussi finanziari in entrata, con particolare riguardo alla gestione dei crediti, gli stessi sono caratterizzati da adeguata tracciabilità e gestiti dalle funzioni interne competenti;
17. Tutte le richieste anticipazioni spese vengono richiesti attraverso richiesta documentata e sono sottoposte ad accettazione tracciabile; inoltre, la richiesta di disposizione di risorse finanziarie deve essere appositamente motivata.
18. Tutte le spese sostenute nell'ambito dello svolgimento dell'incarico sono opportunamente rendicontate attraverso dettagliata nota spese e classificate per centro di costo. I rimborsi spese vengono riconosciuti unicamente previa presentazione di tutti i giustificativi da parte del personale. Può essere riconosciuto un anticipo sulle spese di trasferta che viene consegnato direttamente alla risorsa da parte della amministrazione. L'uso del contante viene in ogni caso ridotto al minimo e nei limiti di legge e tutte le uscite sono adeguatamente tracciabili;
19. Sono state definite formalmente specifiche regole per i dipendenti, riportati nel "Regolamento aziendale".

20. Le spese di rappresentanza sono riconosciute e autorizzate unicamente se adeguatamente giustificate dalla natura dell'incarico o della commessa per cui si rendono necessarie. Le modalità di gestione di tali uscite sono ampiamente tracciabili e giustificabili;

A tali principi si aggiungono anche quelli previsti per i reati di corruzione tra privati (parte speciale A).

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE N- REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte speciale “L”, si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell’art. 25-novies del Decreto.

Divulgazione tramite reti telematiche di un'opera dell'ingegno protetta (art. 171, comma 1, lett. a-bis e comma 3. Legge sul Diritto d'Autore)

Il delitto di cui all'art. 171 primo comma, lettera a-bis, punisce la messa a disposizione del pubblico, attraverso l’immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un’opera di ingegno protetta o di parte di essa.

L'inserimento della previsione nel Decreto mira a responsabilizzare tutte quelle aziende che gestiscono server attraverso cui si mettono a disposizione del pubblico opere protette da diritto d’autore.

La norma tutela l’interesse patrimoniale dell’autore dell’opera, che potrebbe vedere frustrate le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete.

Dal punto di vista soggettivo, basta a configurare il reato il dolo generico, ovvero la coscienza e la volontà di porre in essere la condotta descritta dalla norma.

Il delitto di cui al comma 3 dell'art. 171 è configurabile qualora sia integrata alternativamente una delle condotte menzionate dall'art. 171 (quindi sia l'ipotesi prevista dall'art. 171 lett. a bis, sopra descritta, sia le altre ipotesi indicate dalla norma, ovvero riproduzione, trascrizione, diffusione, messa in vendita, di un 'opera altrui o rivelazione del contenuto, prima che sia reso pubblico; o anche rappresentazione o diffusione di un'opera altrui) ove commesse su un’opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell’opera, o con deformazione, mutilazione o altra modificazione dell’opera medesima, qualora ne risulti offesa all’onore od alla reputazione dell’autore.

Il bene giuridico protetto dalla norma di cui al terzo comma consiste nella protezione dei diritti personali del titolare dell'opera, ovvero il suo onore e la sua reputazione, a differenza della ipotesi criminosa precedente che mira a tutelare l’aspettativa di guadagno del titolare dell’opera.

Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non

contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di un programma per elaboratori (art. 171-bis, Legge 633/1941)

Il primo comma dell'art. 171-bis è volto a tutelare penalmente il c.d. software, punendo l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; ma anche l'importazione, la distribuzione, la vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; è altresì punita la predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

La condotta può consistere anzitutto nella abusiva duplicazione, essendo prevista la rilevanza penale di ogni condotta di duplicazione di software che avvenga ai fini di lucro.

Il riferimento all'abusività della riproduzione indica che, sul piano soggettivo, il dolo dell'agente debba ricomprendere anche la conoscenza delle norme extrapenali che regolano la materia.

La seconda parte del comma indica le altre condotte che possono integrare il reato de quo: importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale e locazione di programmi "piratati". Si tratta di condotte caratterizzate dall'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale.

Infine, nell'ultima parte del comma, il legislatore ha inteso inserire una norma volta ad anticipare la tutela penale del software, punendo condotte aventi ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Sul piano soggettivo, tutte le condotte sono caratterizzate dal dolo specifico di profitto.

Il comma 2 dell'art. 171-bis mira alla protezione delle banche dati; la condotta, invero, si concretizza nella riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; nell'estrazione o reimpiego della banca dati; nella distribuzione, vendita o concessione in locazione di banche di dati.

Per banche dati si intendono le raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo, con esclusione dei contenuti e dei diritti sugli stessi esistenti.

Art. 171-ter L. 633/41[23]

La norma punisce l'abusiva messa a disposizione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti o servizi analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; la riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

L'articolo punisce altresì chiunque abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85 -bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

Perché sia integrato il reato de quo, oltre alla realizzazione di una delle condotte descritte dalla norma, devono ricorrere due requisiti: il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, che costituisce il fine ulteriore che l'agente deve avere di mira perché sia integrato il fatto tipico previsto dalla norma.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale della Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra indicati.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di

[23] Articolo modificato dalla legge 14 luglio 2023, n. 93 (in G.U. 24 luglio 2023, n. 171), recante "Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica"

commissione dei reati. I risultati di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "N" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P05- Gestione dei sistemi informativi P07- Approvvigionamento	Acquisto e gestione di software tutelati da brevetti (es. antivirus, applicativi)
P05- Gestione dei sistemi informativi	Gestione del sito internet aziendale
P11- Gestione della commessa	Gestione della proprietà intellettuale del cliente
P11- Gestione della commessa	Gestione del materiale coperto da copyright nell'ambito di gestione delle commesse
P05- Gestione dei sistemi informativi	Gestione delle banche dati e degli archivi elettronici

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

La presente parte speciale, prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. Assicurare il rispetto delle norme interne, comunitarie e internazionali poste a tutela della proprietà intellettuale;
2. Utilizzare software privi delle necessarie licenze nell'ambito dei sistemi informativi aziendali;
3. Fare alcun uso illecito di materiale tutelato dal diritto d'autore;
4. Duplicare e/o diffondere in qualsiasi forma programmi e file se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati e nei termini (vincoli d'uso) delle licenze ottenute;

5. Riprodurre o diffondere, in qualunque forma e senza diritto, l'opera intellettuale altrui, in mancanza di accordi contrattuali formalizzati per iscritto con i relativi titolari per lo sfruttamento economico o in violazione dei termini e delle condizioni previste in detti accordi;
6. Installare e utilizzare qualsiasi sistema di file sharing;
7. Utilizzare file multimediali sul proprio computer ottenuti in violazione della normativa sul diritto d'autore;
8. Con particolare riguardo alla gestione dei siti internet, divieto di diffondere immagini, documenti o altro materiale tutelati dalla normativa in materia di diritto d'autore.

I Destinatari sono inoltre tenuti a:

1. Rispettare le regole per il corretto uso di tutte le opere dell'ingegno, compresi i programmi per elaboratore e le banche di dati;
2. Utilizzare i software installati sui propri terminali conformemente ai brevetti e/o ai termini delle licenze (vincoli d'uso) e per esclusive finalità lavorative;
3. Curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore, nell'ambito della gestione del sistema ICT aziendale e nell'uso del web.

4 PRINCIPI DI CONTROLLO

Justbit, al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale "N", ha previsto i seguenti principi di controllo che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. Tutti i software e applicativi utilizzati sono dotati di regolare licenza. La gestione degli stessi è in carico al CISO;
2. Divieto di installazione e utilizzo non autorizzato di sistemi di file sharing;
3. Nell'ambito delle commesse acquisite, tutte le attività comportanti utilizzo di materiale di proprietà di terzi o coperto da copyright sono gestite secondo le previsioni della normativa applicabile e secondo specifici requisiti contrattuali e accordi di riservatezza;
4. Tutti i dati vengono gestiti in accordo con la normativa sulla privacy, a fronte della quale Justbit ha effettuato preventivamente all'entrata di vigore del GPDR una valutazione dei controlli esistenti con implementazione di azioni di adeguamento.

5. tracciamento degli accessi alle banche dati online o dell'eventuale consultazione dei dati presenti in tali database e conservazione dei log di accesso nei termini previsti dalla normativa vigente.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE O- REATI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

1 TIPOLOGIA DI REATI APPLICABILI

Per quanto concerne la presente Parte speciale "O", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 24-ter del Decreto.

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

Il reato si configura mediante l'induzione, a seguito di violenza, minaccia ovvero offerta o promessa di denaro o altre utilità, del soggetto avente facoltà di non rispondere, a non rendere dichiarazioni - ossia ad avvalersi di tale facoltà - o a rendere dichiarazioni mendaci all'Autorità giudiziaria (Giudice o Pubblico Ministero).

I destinatari della condotta sono, dunque, gli indagati e gli imputati (anche in procedimento connesso o in un reato collegato), ai quali è riconosciuta dall'ordinamento la facoltà di non rispondere.

Quanto alle modalità tipiche della realizzazione della condotta, l'induzione rilevante ai fine della consumazione del reato, si realizza mediante l'azione con la quale un soggetto esplica un'influenza sulla psiche di un altro soggetto, determinandolo a tenere un certo comportamento, esplicata attraverso i mezzi tassativamente indicati dalla norma, ovvero minaccia, violenza o promessa di denaro o altra utilità.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale della Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra indicati.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "O" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità P03- Gestione di contenziosi giudiziali ed extragiudiziali	Gestione dei rapporti con l'Autorità Giudiziaria, i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale
P04- Gestione delle risorse umane	Ricerca e selezione del personale
P04- Gestione delle risorse umane	Gestione del sistema di incentivazione e sviluppo professionale del personale dipendente
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Gestione dei procedimenti penali che vedano coinvolta la Società o suoi amministratori/dipendenti.

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

È previsto l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. indurre attraverso minaccia o violenza o qualsiasi tipo di coercizione fisica o morale un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria nel corso di un procedimento penale, al fine di occultare/omettere fatti che possano arrecare un danno alla Società;
2. offrire o concedere un'indebita utilità o qualsiasi tipo di beneficio aziendale (incentivo, assunzione ecc.) a dipendenti, candidati o terzi che possono avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'Autorità Giudiziaria, con l'intento di ottenere qualsiasi vantaggio per la società.

I Destinatari sono inoltre tenuti a:

3. garantire la massima collaborazione con l'Autorità Giudiziaria e rendere dichiarazioni veritiere ed esaustivamente rappresentative dei fatti;
4. ove chiamati a rispondere da parte dell'Autorità giudiziaria, presentare con chiarezza i fatti e ove desiderato poter esercitare la facoltà di non rispondere riconosciuta dalla legge
5. mantenere la massima riservatezza relativamente alle dichiarazioni rilasciate ed al loro oggetto.
6. avvisare l'OdV di ogni violenza o minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da rendere all'Autorità Giudiziaria o di non renderle.

4 PRINCIPI DI CONTROLLO

Al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale "O", considerate le peculiarità connesse alla sua ipotetica realizzazione, valgono essenzialmente i principi di carattere generale individuati nel Modello e nei suoi allegati e le regole comportamentali indicate al punto 3, che disciplinano, complessivamente, gli aspetti etico-comportamentali che devono essere osservati dai Destinatari.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE P- REATI AMBIENTALI

1 TIPOLOGIA DI REATI APPLICABILI

Il legislatore comunitario ha elaborato principi importanti in materia di tutela penale dell'ambiente, recepiti dall'ordinamento italiano con l'introduzione dell'art. 25 undecies che ha introdotto i c.d. Reati Ambientali all'interno della disciplina del Decreto trattati dalla presente Parte Speciale.

C'è da rilevare che considerata la natura delle attività di Justbit, i reati applicabili sono:

Gestione non autorizzata di rifiuti (art. 256, comma 1, del D.Lgs. 152/2006)

Il primo comma dell'art. 256 del D.Lgs. 162/2006 punisce una pluralità di condotte connesse alla gestione non autorizzata dei rifiuti, ossia le attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti di qualsiasi genere – pericolosi e non pericolosi – poste in essere in mancanza della specifica autorizzazione, iscrizione o comunicazione prevista dagli artt. da 208 a 216 del D.Lgs. 152/2006. Si precisa che, ai sensi dell'art. 193, comma 9, del D.Lgs. 152/2006, per le "attività di trasporto" non rilevano gli spostamenti di rifiuti all'interno di un'area privata.

Traffico illecito di rifiuti (art. 259, comma 1, del D.Lgs. 152/2006)

Ai sensi dell'art. 259, comma 1, del D.Lgs. 152/2006, sono punite due fattispecie di reato connesse ai traffici e alle spedizioni transfrontaliere dei rifiuti. Il traffico illecito di rifiuti si concretizza allorché vengono poste in essere le condotte espressamente previste dall'art. 2 del Regolamento CEE del 1° febbraio 1993, n. 259, ossia qualsiasi spedizione di rifiuti effettuata:

(a) senza invio di notifica e/ o senza il consenso delle autorità competenti interessate;

(b) con il consenso delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frode;

(c) senza essere concretamente specificata nel documento di accompagnamento;

(d) in modo tale da comportare uno smaltimento o un recupero in violazione delle norme comunitarie o internazionali;

(e) in violazione dei divieti di importazione ed esportazione dei rifiuti previsti dagli articoli 14, 16, 19 e 21 del suddetto Regolamento 259/1993/CEE.

La fattispecie di reato si configura anche in relazione alla spedizione di rifiuti destinati al recupero (specificamente elencati nell'Allegato II del suddetto Regolamento 259/1993/CEE).

La condotta criminosa si configura ogni qualvolta vengano violate le condizioni espressamente previste dall'art. 1, comma 3, dello stesso (i rifiuti devono sempre essere destinati ad impianti autorizzati, devono poter essere oggetto di controlli da parte delle autorità competenti ecc.).

Attività organizzate per il traffico illecito di rifiuti (art. 260, commi 1 e 2, del D.Lgs. 152/2006)

Ai sensi dell'art. 260, comma 1, del D.Lgs. 152/2006 è punito chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti. Il reato è aggravato qualora i rifiuti siano ad alta radioattività, secondo quanto previsto dall'art. 260, comma 2, del D.Lgs. 152/2006.

Abbandono di rifiuti (art. 255 del D. Lgs. 152/2006)[24]

L'articolo punisce chiunque, in violazione delle disposizioni degli articoli 192, commi 1 e 2, 226, comma 2, e 231, commi 1 e 2 del D.lgs. 152/2006, abbandona o deposita rifiuti ovvero li immette nelle acque superficiali o sotterranee.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale della Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra indicati.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

C'è da rilevare che considerate le attività di Justbit che non prevedono, svolgendo unicamente attività di servizi:

- la produzione di rifiuti speciali industriali e di scarichi industriali e la presenza di impianti con emissioni in atmosfera;
- la possibile contaminazione del suolo e sottosuolo;

[24] Reato introdotto nell'art. Art.25-undecies D. Lgs. 231/01 dalla Legge di conversione n.137 del 9 ottobre 2023 "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia personale della magistratura e della pubblica amministrazione"

- il commercio di qualsiasi tipo di specie animale.

la concreta possibilità di commissione di reati di natura ambientale appare difficilmente ravvisabile.

Inoltre, tutte le attrezzature informatiche utilizzate sono acquisite in forza di contratti di leasing con società fornitrici, alle quali vengono restituite ove non ritenute più idonee e sostituite con altre più performanti.

Ciò premesso, in relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "P" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

ID	Processi	Attività sensibile
A72	P06- Gestione della Sicurezza e Ambiente	Gestione rifiuti speciali prodotti presso le sedi e tracciabilità

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

È previsto l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. abbandonare o depositare rifiuti, in modo incontrollato e/o immetterli allo stato solido o liquido negli scarichi;
2. affidare l'attività di gestione di rifiuti speciali eventualmente prodotti presso la sede a soggetti non dotati di un'apposita autorizzazione per il loro trasporto, smaltimento e recupero;
3. ostacolare o impedire l'accesso alla sede da parte dei soggetti incaricati del controllo.

I Destinatari sono inoltre tenuti a rispettare scrupolosamente la normativa vigente in materia ambientale.

4 PRINCIPI DI CONTROLLO

Al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale “P”, considerate le peculiarità connesse alla sua ipotetica realizzazione, valgono essenzialmente i principi di carattere generale individuati nel Modello e nei suoi allegati e le regole comportamentali indicate al punto 3, che disciplinano, complessivamente, gli aspetti etico-comportamentali che devono essere osservati dai Destinatari.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE Q- IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

1 TIPOLOGIA DI REATI APPLICABILI

Il 9 agosto 2012 è entrato in vigore il d.lgs. 16 luglio 2012 n. 109 che ha dato attuazione alla direttiva 2009/52/CE, e ha introdotto norme minime relative a sanzioni e a provvedimenti nei confronti dei datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare.

La norma ha inoltre introdotto nel Decreto il nuovo art. 25 duodecies, intitolato "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare", che ha esteso la responsabilità dell'ente anche al delitto previsto dall'art. 22 comma 12 bis del d.lgs. 25 luglio 1998 n. 286.

Tale articolo (a sua volta modificato dal d.lgs. 109/2012) punisce la condotta del datore di lavoro che occupa 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, revocato o annullato, se: (i) i lavoratori sono in numero superiore a tre, (ii) sono minori in età lavorativa, (iii) sono sottoposti a condizioni lavorative di particolare sfruttamento ai sensi dell'art. 603 bis comma 3 c.p. (ossia sono esposti a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro).

È prevista la sanzione pecuniaria da 100 a 250 quote, entro il limite di Euro 150.000, in relazione alla commissione del delitto.

Inoltre, la Legge 161 del 17.10.2017 riguardante "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" entrata in vigore il 19.11.2017 ha introdotto all'interno del D. Lgs. 231/2001 anche il reato di "sfruttamento dell'immigrazione clandestina", intendendo per tale la promozione, direzione, organizzazione, finanziamento o effettuazione del trasporto di stranieri nel territorio dello Stato ovvero compimento di altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente.

Analogamente, viene anche punito lo "sfruttamento della permanenza clandestina" nel territorio dello Stato di immigrati che non ne hanno titolo, che si configura nel caso in cui al fine di trarre un ingiusto profitto dalla condizione di illegalità dello straniero o nell'ambito delle attività punite a norma della legislazione vigente, viene favorita la permanenza di questi nel territorio dello Stato in

violazione delle norme vigenti. Tale reato costituisce presupposto per la responsabilità amministrativa degli enti se commesso in modalità transnazionale.

Infine, con l'art. 8 del Capo II del Decreto Legge n.20 del 10 Marzo 2023, è stato modificato l'Art.12 ed inserito l'Art. 12-bis "Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina" nel D. Lgs n. 286/1998 "Testo unico sull'immigrazione"[25].

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra indicati.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

in relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "Q" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

Processi	Attività sensibile
P07- Approvvigionamento P11- Gestione della commessa	Richieste di acquisto e selezione del fornitore Nota: Un ulteriore possibilità di commissione del reato può infatti concretizzarsi favorendo volutamente il ricorso a fornitori che impieghino personale non in regola con i permessi di soggiorno o che sfruttino la permanenza nello Stato di immigrati irregolari, al fine di trarne un ingiusto profitto.
P04- Gestione delle risorse umane	Ricerca e selezione del personale

[25] Con l'Art. 12-bis il legislatore ha inteso punire non solo chi promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato, ma con pene detentive severissime anche coloro che attuano ciò con modalità tali da esporre le persone a pericolo per la loro vita, per la loro incolumità o sottoponendole a trattamento inumano e degradante.

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

È previsto l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

1. impiegare lavoratori stranieri del tutto privi del permesso di soggiorno, o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale;
2. ospitare all'interno della sede della società o in qualsiasi luogo riconducibile alla società, seppur per scopi umanitari, cittadini stranieri il cui soggiorno sia irregolare;
3. procedere all'assunzione di personale per il tramite di intermediari per il reclutamento del lavoro che non siano le Agenzie per il lavoro autorizzate dal Ministero del Lavoro.

4 PRINCIPI DI CONTROLLO

Justbit, al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale "Q", ha previsto i seguenti principi di controllo che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. verificare in caso di assunzione di lavoratori extracomunitari il rilascio in loro favore di valido documento di soggiorno che li abiliti a prestare lavoro in Italia;
2. in caso di assunzione di lavoratori extracomunitari, verificare periodicamente la regolarità del documento di soggiorno, verificando altresì che il lavoratore abbia tempestivamente provveduto alla richiesta di rinnovo prima della sua scadenza;
3. nel caso di cui sopra, inviare comunicazione ai dipendenti in prossimità della scadenza del permesso di soggiorno;

4. inviare le comunicazioni agli enti pubblici competenti, assicurando che le informazioni trasmesse siano veritiere, complete e basate su un'idonea documentazione; nel modello di comunicazione dovranno essere riportate tutte le informazioni richieste dalle specifiche sezioni, assicurando in particolare la correttezza dei dati trasmessi per il lavoratore extracomunitario relativamente a:
   - titolo del permesso di soggiorno;
   - numero del titolo di soggiorno;
   - motivo del soggiorno;
   - scadenza del titolo di soggiorno;
   - questura che ha rilasciato il permesso di soggiorno
5. fornire delucidazioni adeguate e complete ai propri collaboratori e ad aziende terze che operano nelle attività sensibili sopra indicate, in merito al procedimento da seguire in caso di assunzione ed impiego di cittadini extracomunitari, qualora essi sottopongano ipotesi di dubbio o casi di particolare criticità;
6. in caso di accertamento di mancata regolarità del soggiorno da parte del cittadino o della constatazione che i documenti presentati probanti la stessa sono stati contraffatti, dallo stesso soggetto o da terzi, occorre procedere all'immediato licenziamento del lavoratore e alla denuncia della circostanza alla Autorità giudiziaria;
7. verificare, in caso di ricorso alle Agenzie autorizzate dal Ministero del lavoro per il reclutamento del personale, il rispetto della normativa vigente in merito alla corresponsione dei trattamenti retributivi e dei contributi previdenziali, attraverso l'obbligo a carico di tali Agenzie, e, pena la risoluzione del rapporto con la società, di fornire idonea documentazione comprovante l'adempimento dei relativi obblighi retributivi e previdenziali.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

PARTE SPECIALE R- REATI DI NATURA TRIBUTARIA

1 TIPOLOGIA DI REATI APPLICABILI

L'articolo 39, del Dl n. 124/2019 (il decreto fiscale rubricato "Disposizioni urgenti in materia fiscale e per esigenze indifferibili) ha introdotto nell'ambito della responsabilità amministrativa degli enti ex Dlgs n. 231/2001 gli illeciti penali di natura tributaria (il cui quadro normativo di riferimento è rappresentato dal Dlgs n. 74/2000), commessi dai soggetti persone fisiche cosiddetti apicali (generalmente, il rappresentante legale della società, o membro dell'organo di dirigenza o comunque soggetti suoi sottoposti) nell'interesse o a vantaggio dell'ente stesso.

Con l'integrazione pertanto dell'art. 25 quinquiesdecies nel D.lgs. 231/2001, sono stati pertanto vengono ricompresi i seguenti delitti:

Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (articolo 2 del Dlgs. 74/2000)

L'articolo 2 della disciplina sui reati tributari prevede, sotto il profilo oggettivo, che sia punito chiunque indichi in dichiarazione elementi passivi fittizi, avvalendosi di fatture e altri documenti per operazioni inesistenti.

Il termine "dichiarazione", è riferito sia alla dichiarazione ai fini delle imposte sul reddito, sia alle dichiarazioni periodiche o annuali ai fini Iva: mentre nel primo caso, l'indicazione di un elemento passivo fittizio (il sostenimento di un costo di acquisto di un determinato bene o di un servizio, inerente all'esercizio di impresa) comporterà l'indebita deducibilità di quel costo dal reddito complessivo d'impresa, derivandone una minore base imponibile su cui applicare l'aliquota d'imposta; nel secondo caso, comporterà l'indebita detrazione dell'imposta sul valore aggiunto. È altresì previsto che "Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria".

Nel comma 2-bis dell'art. 2 la norma, pur non prevedendo una soglia minima di punibilità, si limita oggi ad indicare una generica attenuante, qualora l'ammontare degli elementi passivi fittizi risulti comunque inferiore a centomila euro. Nel qual caso, infatti, si applicherà la reclusione da un anno e sei mesi a sei anni.

Il delitto di operazione inesistente si può configurare in diverse fattispecie:

- l'operazione commerciale non sia mai stata effettuata in rerum natura, ma comunque sia stata fraudolentemente documentata (operazione "oggettivamente" inesistente);

- l'operazione sia stata sì effettuata, ma tra soggetti (emittente della fattura o beneficiario della stessa), comunque diversi da quelli che appaiono nella relativa documentazione (operazione "soggettivamente" inesistente);
- l'operazione sia stata effettuata, tra soggetti effettivi, ma con l'indicazione, nella documentazione medesima, di un corrispettivo o di una imposta in misura superiore a quella reale (cosiddetta inesistenza da sovrafatturazione o inesistenza parziale).

In caso di condanna della persona fisica (rappresentante legale o dirigente, anche di fatto), verranno contestate le seguenti sanzioni in capo alla Casa di Cura, a seconda se ricorrano, o meno, le circostanze attenuanti del comma 2-bis:

- per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, (se non ricorre la circostanza attenuante), la sanzione pecuniaria fino a cinquecento quote;
- per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 2-bis, (se ricorre la circostanza attenuante dell'ammontare complessivo degli elementi passivi fittizi inferiore a centomila euro), la sanzione pecuniaria fino a quattrocento quote.

Dichiarazione fraudolenta mediante altri artifici (articolo 3 del Dlgs n. 74/2000 come modificato da Decreto Legislativo 14 luglio 2020, n. 75 di attuazione della Direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale)

L'articolo 3 della disciplina sui reati tributari prevede, sotto il profilo oggettivo, che sia punito chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, compia operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indicando in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, purché ricorrano congiuntamente le seguenti condizioni:

- l'imposta effettivamente evasa, deve comunque essere superiore, con riferimento a taluna singola imposta, a trentamila euro;
- l'ammontare complessivo degli elementi attivi sottratti ad imposizione, anche mediante l'indicazione di elementi passivi fittizi, è comunque superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è

superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Non sono considerati mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

La norma prevede, con l'applicazione della sanzione penale a carico della persona fisica (rappresentante legale dell'ente, o dirigente, anche di fatto), "per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote".

Il suddetto reato è punibile a titolo di tentativo ove sia compiuto anche nel territorio di altro Stato membro dell'Unione Europea, al fine di evadere l'imposta sul valore aggiunto per un valore complessivo non inferiore a dieci milioni di euro.

Dichiarazione infedele (art. 4 del Dlgs n. 74/2000) nell'ambito dei sistemi fraudolenti transfrontalieri[26]

L'art. 4 della disciplina sui reati tributari prevede che sia punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni

Sono esclusi in casi in cui:

a) non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri

[26] Reato introdotto nell'art. 25 *quinquiesdecies* dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

b) Fuori dal caso precedente, le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette.

Ai fini della responsabilità amministrativa di impresa, è punibile solo il caso in cui il reato sia 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.

Il suddetto reato è punibile a titolo di tentativo ove sia compiuto anche nel territorio di altro Stato membro dell'Unione Europea, al fine di evadere l'imposta sul valore aggiunto per un valore complessivo non inferiore a dieci milioni di euro.

Omessa dichiarazione (art. 5 del D.lgs n. 74/2000)[27]

L'art. 5 della disciplina sui reati tributari prevede che sia punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.

Non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto.

Emissione di fatture per operazioni inesistenti – Articolo 8 del D.lgs n. 74/2000

L'articolo 8 della disciplina sui reati tributari prevede che sia punito chiunque al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

L'emissione di fatture per operazioni inesistenti rappresenta una fattispecie di reato di tipo non dichiarativo, a differenza dei precedenti. Inoltre, rispetto alle due tipologie sopra descritte, la commissione del reato, anziché essere finalizzato alla evasione d'imposta da parte dello stesso soggetto che ha emesso il documento fiscale (obiettivamente, non riscontrabile), deve piuttosto essere finalizzato alla evasione d'imposta da parte del soggetto che è destinatario e percettore del documento stesso.

Sono previste le seguenti sanzioni in capo alla società, a seconda se ricorrano, o meno, le circostanze attenuanti del comma 2-bis dell'articolo 8 (ammontare complessivo degli importi non

[27] Reato introdotto nell'art. 25 *quinquiesdecies* : dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

rispondenti al vero indicati nella fattura o in altri documenti emessi, comunque inferiore a centomila euro):

- per il delitto di emissione di fatture per operazioni inesistenti, articolo 8, comma 1, del Dlgs n. 74/2001, (se non ricorre la circostanza attenuante), la sanzione pecuniaria fino a cinquecento quote;
- per il delitto di emissione di fatture per operazioni inesistenti, articolo 8, comma 2-bis del D.lgs n. 74/2001, (se ricorre la circostanza attenuanti), la sanzione pecuniaria fino a quattrocento quote.

Occultamento o distruzione di documenti contabili (Articolo 10 del D.lgs n. 74/2000)

L'articolo 10 della disciplina sui reati tributari sanziona le condotte costituite dall'occultamento e dalla distruzione materiale delle scritture contabili o dei documenti di cui è obbligatoria la conservazione, allorché ne derivi l'impossibilità della ricostruzione dei redditi e del volume degli affari.

Quanto alla distruzione, essa consiste nell'eliminazione fisica in tutto o in parte delle scritture, ovvero nel renderla illeggibile e quindi non idonea all'uso tramite abrasioni, cancellature o altro.

Quanto invece all'occultamento, esso consiste nel nascondimento materiale delle scritture: il semplice rifiuto della consegna delle scritture, ove non si traduca, in un loro mancato rinvenimento, viene sanzionato solo in via amministrativa.

È inoltre necessario che alla condotta appena descritta (di occultamento e di distruzione), segua l'impossibilità della ricostruzione del reddito o del volume degli affari.

Accertata la responsabilità in capo alla persona fisica rappresentante legale dell'ente, il giudice applicherà una sanzione pecuniaria in capo a quest'ultimo, fino ad un massimo di quattrocento quote.

Indebita compensazione (art. 10 quater del D.lgs n. 74/2000) nell'ambito dei sistemi fraudolenti transfrontalieri[28]

L'articolo 10 quater della disciplina sui reati tributari prevede che sia punito chiunque non versi le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti o non spettanti, per un importo annuo superiore a cinquantamila euro.

[28] Reato introdotto nell'art. 25 *quinquiesdecies* dal Decreto legislativo 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale

Ai fini della responsabilità amministrativa di impresa, è punibile solo il caso in cui il reato sia 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.

Sottrazione fraudolenta al pagamento di imposte (articolo 11 del D.lgs n. 74/2000)

L'articolo 11 della disciplina sui reati tributari prevede che sia punito chiunque al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

Inoltre, è previsto che sia punito chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

In sostanza, viene punita la condotta di colui che aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni, idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

Non è quindi necessario che si sia concretizzato un effettivo nocumento alle pretese erariali, ma solo il pericolo (concreto) che ciò possa accadere, in virtù dell'alienazione dei beni individuati per consentire la riscossione coatta del credito tributario.

La norma prevede che per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, sia comminata la sanzione pecuniaria fino a quattrocento quote.

2 AREE DI RISCHIO

In occasione dell'attività di mappatura, sono state individuate nell'ambito della struttura organizzativa ed aziendale di Justbit, delle aree considerate "a rischio di reato", ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati sopra indicati.

Nell'ambito di ciascuna area "a rischio di reato", sono state individuate le relative attività c.d. "sensibili", ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati. I risultati di tale attività sono riportati nella "Matrice di rischio e controlli interni" in allegato al Modello.

in relazione ai reati e alle condotte criminose sopra esplicitate, ai fini della presente Parte Speciale "R" del Modello, le aree ritenute più specificamente a rischio risultano essere le seguenti:

ID	Processi	Attività sensibile
A14	P07- Approvvigionamento P11- Gestione della commessa	Nell'ambito dei contratti con i fornitori, - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento - gestione e segnalazione delle anomalie
A15	P09- Processo Amministrativo	Stipula ed esecuzione dei contratti, avendo riguardo anche agli aspetti inerenti all'applicazione di penali e le risoluzioni transattive in caso di contestazioni
A16	P09- Processo Amministrativo	Processi di ciclo passivo e contabilità
A17	P12- Operazioni sul capitale e destinazione dell'utile	Operazioni societarie straordinarie
A18	P01- Commerciale P04- Gestione delle risorse umane	Gestione degli incentivi per partner ai fini del pieno raggiungimento degli obiettivi commerciali
A19	P08- Processo finanziario	Gestione dei conti correnti bancari
A20	P07- Approvvigionamento P11- Gestione delle commesse	Richieste di acquisto e selezione del fornitore
A21	P04- Gestione delle risorse umane	Ricerca e selezione del personale
A22	P04- Gestione delle risorse umane	Gestione del sistema di incentivazione e sviluppo professionale del personale dipendente
A23	P08- Processo finanziario	Gestione delle risorse finanziarie
A27	P04- Gestione delle risorse umane	Gestione delle spese di rappresentanza
A37	P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità P05- Gestione dei sistemi informativi	Creazione, trattamento, archiviazione di documenti elettronici con valore probatorio.
A38	P05- Gestione dei sistemi informativi	Gestione degli accessi fisici alle aree riservate
A40	P09- Processo Amministrativo	Predisposizione delle dichiarazioni fiscali periodiche
A41	P09- Processo Amministrativo	Liquidazione delle imposte

ID	Processi	Attività sensibile
A53	P11- Gestione delle commesse	Gestione delle rendicontazioni delle commesse ai fini dei pagamenti
A56	P07- Approvvigionamento	Valutazione e qualificazione dei fornitori
A62	P07- Approvvigionamento	Pagamento e contabilizzazione
A63	P07- Approvvigionamento	Gestione dei subaffidamenti
A67	P08- Processo finanziario	Gestione dei flussi finanziari in uscita (ciclo passivo)
A73	P12- Operazioni sul capitale e destinazione dell'utile	Operazioni societarie in caso di procedura coattiva di riscossione di crediti per reati tributari

Per quanto attiene i cosiddetti “reati di contrabbando” (il cui quadro normativo di riferimento è rappresentato dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, così detto “testo unico doganale”, di seguito “TULD”),, che il Decreto Legislativo 14 luglio 2020, n. 75 di attuazione della Direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell’Unione mediante il diritto penale, ha introdotto nell’ambito della responsabilità amministrativa degli enti ex D. Lgs n. 231/2001, c’è da rilevare che gli stessi sono difficilmente applicabili alla realtà di Justbit. Tuttavia, nel caso remoto di ricorso ad approvvigionamenti da paesi terzi (facenti parte esclusivamente della Unione Europea), le conseguenti operazioni di acquisto intracomunitarie passive sono oggetto di dichiarazione periodica e assolvimento dei relativi tributi. In tale ottica, pur non essendo immediatamente assimilabili a oneri relativi ai diritti di frontiera, così come definiti dal TULD, la predisposizione delle dichiarazioni afferenti a tali operazioni intracomunitarie e relativi versamenti (pur essendo più strettamente correlate ai reati di tipo tributario), possono essere astrattamente considerate nel novero delle attività sensibili correlate ai reati descritti nella presente parte speciale, in linea con gli attuali orientamenti giurisprudenziali. Conseguentemente, possono essere ritenute applicabili come misure di comportamenti e principi di controllo ai fini della prevenzione dei suddetti reati di contrabbando, le stesse misure identificate nella presente parte speciale “R”.

3 PRINCIPI GENERALI DI COMPORTAMENTO E ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere dai componenti del CdA, dall'AD, dai soci, da eventuali altri soggetti apicali e dipendenti di Justbit nonché da collaboratori esterni e partner, come già definiti nella Parte Generale (qui di seguito tutti definiti "Destinatari").

Tutte le regole comportamentali indicate sono finalizzate a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

Obiettivo della presente Parte speciale è che tutti i Destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi dei reati previsti nel Decreto ed in particolare sono tenuti a osservare i seguenti principi generali:

1. stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività di Justbit, con particolare riferimento alle attività che comportano contatti e rapporti con società esterne (partner commerciali, fornitori, consulenti ecc.) e soggetti ad esse subordinati o comunque riconducibili;
2. instaurazione e mantenimento di qualsiasi rapporto con i terzi in tutte le attività relative allo svolgimento di una funzione o di un servizio sulla base di criteri di correttezza e trasparenza che garantiscano il buon andamento della funzione o servizio e l'imparzialità nello svolgimento degli stessi.
3. instaurazione e mantenimento di qualsiasi rapporto con le altre società sulla base di criteri di massima correttezza e trasparenza;
4. stretta osservanza della normativa fiscale, con particolare riguardo al rispetto regolamentazione del diritto alla detrazione nei limiti previsti dalla legislazione di settore;
5. Verifica costante delle scritture contabili relative dei servizi/prodotti di cui si avvale la società, denunciando prontamente alla Unità amministrativa qualsiasi anomalia o presunta irregolarità fiscale;
6. verifica della corretta applicazione del diritto alla detrazione fiscale in caso di dichiarazioni periodiche;
7. informazione immediata a tutti i soci e all'OdV di messa in essere di procedure di riscossione coattiva per irregolarità fiscali, anche in caso di applicazione di transazioni;
8. Il personale ha altresì l'obbligo in particolare di informare l'AD e l'OdV:

a) di richieste esplicite o implicite di benefici reciproci finalizzati alla frode fiscale, da parte di un fornitore/collaboratore;

b) di qualsiasi alterazione presunta o comprovata delle scritture contabili da parte di un fornitore/collaboratore, ove sia chiaro l'intento di porre in essere una frode fiscale;

c) di operazioni di incasso che presentino anomalie rispetto agli standard di pagamento, sotto il profilo dell'importo, della tempistica e della dilazione e dello stralcio;

d) di operazioni di fatturazione attiva che presentino anomalie rispetto agli standard di pagamento, sotto il profilo dell'importo, della tempistica e della dilazione e dello stralcio;

e) più in generale, di ogni operazione di acquisto e/o vendita che abbia caratteristiche "anomale", secondo l'esperienza personale.

La presente Parte Speciale prevede l'espresso divieto a carico di tutti i Destinatari, come sopra individuati (limitatamente agli obblighi contemplati nei principi di controllo e nei codici comportamentali adottati e agli obblighi contemplati nelle specifiche clausole contrattuali), di:

1. elargire e/o promettere di elargire a chiunque somme di denaro, regali e/o altre utilità che possano essere interpretati come eccedenti le normali pratiche commerciali o di cortesia rivolti ad acquisire benefici fiscali;
2. intraprendere accordi con fornitori/collaboratori per l'emissione di scritture contabili per i servizi non resi o resi per importi non congruenti con quanto definito contrattualmente;
3. omettere di denunciare qualsiasi tentativo da parte di fornitori/collaboratori/partner di intraprendere accordi per l'emissione da parte di Justbit di fatture relative a prestazioni non rese, rese parzialmente o con importi alterati rispetto a quelli previsti contrattualmente;
4. riportare nelle dichiarazioni fiscali periodiche dati non veritieri ottenuti tramite artifizi, anche se proposti da intermediari qualificati, per l'ottenimento di benefici fiscali non spettanti;
5. accettare qualsiasi proposta di pratica o misura finalizzata alla riduzione fraudolenta dell'importo imponibile nelle dichiarazioni fiscali periodiche al di fuori di quelle previste dalla normativa di settore;
6. effettuare le attività di cui ai punti precedenti, ricorrendo a terzi o a intermediari;
7. porre in essere, in generale, pratiche non consentite dalla legge, dagli usi commerciali o dai codici etici delle aziende e degli enti con cui hanno rapporti;

8. effettuare accessi informatici non autorizzati agli archivi delle scritture contabili che non siano giustificati da valide motivazioni.
9. alterare in qualsiasi modo il software utilizzato per la registrazione delle scritture contabili, ferma restando la possibilità di modifiche finalizzate al miglioramento, all'efficienza e alla personalizzazione effettuate da personale esterno qualificato, previa contrattualizzazione delle stesse attività.

4 PRINCIPI DI CONTROLLO

C'è innanzitutto da rilevare che le seguenti aree di rischio:

1. la gestione delle attività di approvvigionamento per la fornitura da parte di soggetti terzi di beni e servizi, inclusiva delle attività di richiesta di acquisto, richiesta di offerta nei confronti del fornitore e accettazione della stessa con successiva emissione dell'ordine;
2. la gestione commerciale delle offerte e dei contratti per servizi resi a nome di Justbit nei confronti di soggetti terzi;
3. la gestione del contratto in fase di fornitura del servizio da parte di soggetti terzi;
4. la gestione del contratto in fase di erogazione da parte di Justbit dei servizi pattuiti con i soggetti beneficiari degli stessi.

sono state già considerate come tali nell'ambito dei reati di corruzione tra privati, dove sono state infatti considerate a rischio tutte le attività inerenti al c.d. ciclo attivo, quali, a titolo esemplificativo, la definizione del prezzo di offerta di un servizio, la definizione delle condizioni e dei termini di pagamento, della scontistica e della definizione di eventuali risoluzioni transattive in caso di contestazioni.

Nello stesso modo, sono state, sempre nell'ambito dei reati di corruzione tra privati, valutate come aree a rischio tutte quelle attività attraverso le quali sarebbe possibile costituire la provvista o i fondi necessari per le illecite dazioni o promesse di denaro. Si tratta quindi di tutte le attività relative al c.d. ciclo passivo quali, a titolo esemplificativo, gli acquisti di beni e servizi e l'affidamento di consulenze e altre prestazioni professionali.

La definizione delle misure e principi di controllo già implementati per la riduzione e il contenimento degli stessi rischi di commissione del reato di corruzione tra privati, sono altresì da considerare valide ed efficaci ai fini della prevenzione della commissione reati presupposto anche con riferimento all'ambito dei reati oggetto di analisi nella presente parte speciale (c.d. "Reati di natura tributaria"), considerando quale possibile vantaggio per la società non meramente la semplice

dazione o promessa di denaro o altro beneficio futuro intercorrente tra soggetto che cede un servizio o prodotto e soggetto che lo riceve, ma specificatamente un vantaggio di natura fiscale per uno o entrambi i soggetti contraenti che potrebbe realizzarsi attraverso un accordo comportante il compimento di attività delittuose quali la proposta di offerte e successiva contrattualizzazione di erogazione di servizi o fornitura di prodotti mai resi o resi in parte o con una quotazione economica del tutto o in parte alterate rispetto all'oggettivo o ragionevole valore di mercato, con conseguente emissione di false o alterate scritture contabili secondo le modalità di pagamento pattuite tra le parti.

Per le altre aree di rischio, Justbit, al fine di evitare il verificarsi dei reati oggetto della presente Parte speciale "R", ha previsto i seguenti principi di controllo che i Destinatari sono tenuti a rispettare e che potranno, ove opportuno, essere implementati in specifiche procedure aziendali:

1. sono definiti criteri che regolano, tra l'altro, i processi di selezione e qualifica dei principali fornitori e i processi di affidamento degli incarichi in base ad appositi criteri di valutazione;
2. sono segregate per fasi e distribuite tra più funzioni le attività di selezione dei fornitori in senso ampio, di fruizione di beni e servizi, di verifica del rispetto delle condizioni contrattuali (attive e passive) all'atto della predisposizione/ricevimento delle fatture;
3. Il processo di preparazione e redazione dell'offerta di servizi si basa su criteri oggettivi;
4. Il processo di acquisti è tracciato in modo puntuale sul sistema informatico "Alyante" e prevede la fase di richiesta di acquisto, approvazione della stessa, richiesta offerta ad almeno tre fornitori coinvolti salvo casi eccezionali;
5. I preventivi vengono valutati unicamente sulla base della convenienza economica a parità di qualità del prodotto/servizio reso; per offerte con quotazioni anormalmente fuori mercato possono essere richieste giustificazioni integrative al fornitore candidato;
6. Tutte le fatture passive relative a prodotti e servizi vengono verificate, a fronte di importi e prestazioni pattuite; inoltre, è previsto un secondo controllo da parte dell'area amministrativa prima della messa in pagamento delle fatture;
7. La contabilità viene gestita attraverso software dedicato cui accedono gli addetti dell'Unità amministrativa previa adeguata profilazione e identificazione delle modifiche, in modo che sia possibile tracciare e risalire in qualsiasi momento all'autore di eventuali alterazioni dei set up di sistema e ad eventuali alterazioni informatiche dello stesso;

8. Le dichiarazioni mensili per il pagamento dell'IVA vengono derivate dall'unità amministrativa attraverso lo stesso software di contabilità. Il dato di IVA periodica risulta immodificabile una volta estratto il report. La stessa contabilità verifica la corretta applicazione del diritto alla detrazione, in caso di esercizio di un'attività imponibile e di un'attività esente da IVA, spettante in misura proporzionale alle operazioni imponibili effettuate. L'Unità amministragiva, prima del versamento dell'IVA, verifica la correttezza dell'F24 con i report forniti dalla contabilità anche con l'ausilio dei report trasmessi dalla contabilità comprensiva di distinta di versamento, prima della trasmissione tramite UNIWEB; la stessa procedura viene seguita in caso di liquidazione/conguaglio annuo dell'IVA;
9. Per quanto attiene le imposte sui redditi, Justbit si avvale del supporto uno studio esterno specializzato in Diritto del Lavoro, atto anche al supporto nel processo di Gestione del personale, e di un intermediario fiscale, incaricato contrattualmente di verificare la correttezza dell'applicazione dei benefici fiscali e del diritto alla detrazione delle spese, secondo normativa vigente;
10. Le scritture contabili sono costantemente e immediatamente verificabili dalle Autorità competenti attraverso consultazione del software gestionale di contabilità che prevede una profilazione in funzione del ruolo;
11. Per la archiviazione delle scritture contabili, nessun componente di Justbit può avere accesso a tali dati una volta archiviati.
12. In caso di comunicazione da parte dell'Autorità competente di messa in esecuzione di procedura coattiva di confisca/sequestro di beni riconducibili al patrimonio di Justbit in conseguenza di reati di natura tributaria, AD è tenuto alla comunicazione immediata della circostanza al CdA i quali, per importi superiori ai cinquantamila euro convocheranno una assemblea straordinaria, atta alla discussione sull'eventualità di sospensione di qualsiasi operazione finanziaria sul patrimonio della società programmata ma non ancora intrapresa.

I principi di controllo indicati sono finalizzati a prevenire la commissione di reati presupposto sia in vantaggio di Justbit, sia in vantaggio di altre società che detengono quote societarie.

APPENDICE

1 ELENCO PROCESSI AZIENDALI

ID	Processo
P.01	Processo commerciale (partecipazione a gare ed appalti pubblici e trattative private)
P.02	Gestione delle prescrizioni legali e regolamentari verso la Pubblica amministrazione o altre Autorità
P.03	Gestione di contenziosi giudiziali ed extragiudiziali
P.04	Gestione delle risorse umane
P.05	Gestione dei sistemi informativi
P.06	Gestione della sicurezza e dell'ambiente
P.07	Processo di approvvigionamento
P.08	Processo finanziario
P.09	Processo amministrativo
P.10	Processo Societario
P.11	Gestione delle commesse

2 ELENCO ATTIVITÀ SENSIBILI

ID	Attività sensibile
A01	Valutazione delle opportunità a partecipare a gare pubbliche
A02	Valutazione delle opportunità a presentare offerta per clienti privati
A03	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con la Pubblica Amministrazione, Enti o Società Pubbliche
A04	Rapporti con le Autorità di controllo, altri organismi di diritto pubblico o enti pubblici nonché il rilascio di informazioni alla P.A
A05	Rapporti con pubblici ufficiali e incaricati di pubblico servizio relativamente sia agli adempimenti fiscali, tributari, previdenziali, ambientali e in materia di salute e sicurezza sui luoghi di lavoro che alle visite ispettive condotte dai funzionari pubblici in tali ambiti
A06	Negoziazione diretta con l'amministrazione pubblica, la stazione appaltante o ente aggiudicatore
A07	Predisposizione della documentazione (tecnica e amministrativa) e riesame dell'offerta
A08	Partecipazione a procedure per l'ottenimento di sovvenzioni, erogazioni, contributi o finanziamenti da parte di enti e organizzazioni pubblici italiani o comunitari e modalità di impiego dei finanziamenti erogati
A09	Richiesta di provvedimenti amministrativi occasionali, di autorizzazioni, licenze e concessioni per lo svolgimento di attività strumentali a quelle tipiche della Società
A10	Gestione dei rapporti con l'Autorità Giudiziaria, i pubblici ufficiali e gli incaricati di pubblico servizio nell'ambito del contenzioso penale, civile, del lavoro, amministrativo, tributario e fiscale
A11	Gestione delle partnership nelle attvità di partecipazione a gare e richiesta finanziamenti (es.: joint venture, anche in forma di ATI, RTI, consorzi, ecc.)
A12	Assegnazione, ai fini della partecipazione alle procedure di cui alle attività commerciali di uno specifico incarico di consulenza o di rappresentanza a un soggetto terzo
A13	Nell'ambito dei contratti con i fornitori, - ricevimento dei beni e le attività di avvenuta prestazione dei servizi e di benestare al pagamento - gestione e segnalazione delle anomalie
A14	Stipula ed esecuzione dei contratti, avendo riguardo anche agli aspetti inerenti all'applicazione di penali e le risoluzioni transattive in caso di contestazioni
A15	Processi di ciclo passivo e contabilità
A16	Operazioni societarie straordinarie (tra cui modifiche statuarie)
A17	Gestione degli incentivi ai fini del pieno raggiungimento degli obiettivi commerciali
A18	Gestione dei conti correnti bancari
A19	Richieste di acquisto e selezione del fornitore
A20	Ricerca e selezione del personale
A21	Gestione del sistema di incentivazione e sviluppo professionale del personale

⊆	Attività sensibile
	dipendente
A22	Gestione delle risorse finanziarie
A23	Recupero dei crediti, nonché le transazioni commerciali remissive a fronte di reclami o contestazioni
A24	Amministrazione del personale e pagamento delle retribuzioni, gestione dei permessi e delle ferie
A25	Gestione dei rimborsi spese a dipendenti
A26	Gestione delle spese di rappresentanza
A27	Eventuale conferimento di utilità a titolo gratuito (donazioni, regali, omaggi, ecc.) nei confronti di esponenti pubblici o di altre realtà organizzative private influenti
A28	Gestione della sicurezza logica dei sistemi, con particolare attenzione a: - controllo accessi a sistemi informativi e rete dati (rete aziendale, internet, extranet); - crittografia dei dati e/o del canale di comunicazione (ad esempio infrastrutture firewall, Reti private virtuali, ecc.);
A29	Sviluppo e attuazione di sistemi di monitoraggio e revisione per la prevenzione e individuazione di attività non autorizzate/illecite sulla rete, sistemi e banche dati aziendali
A30	Attività di amministrazione applicativa/sistemistica di: - applicazioni a supporto dei processi di business; - database/archivi elettronici; - sistemi operativi.
A31	Attività informatiche che potrebbero comportare la diffusione di software malevoli, esecuzione di attacchi informatici che potrebbero essere condotte attraverso strumenti/dispositivi/informazioni aziendali;
A32	Gestione di caselle di posta e domini di rete;
A33	Gestione di servizi online finalizzati alla dematerializzazione (es. Cedolino/CUD online, iter autorizzativo ferie/permessi/missioni).
A34	Utilizzo da parte del personale delle postazioni di lavoro fisse (es. desktop) e mobili (es. laptop, PDA); utlizzo della posta elettronica e di internet
A35	Utilizzo del sistema informatico per: - accesso in via telematica, o direttamente on site, a sistemi elettronici di clienti e fornitori; - acquisizione delle informazioni utili per la qualificazione dei fornitori;
A36	Creazione, trattamento, archiviazione di documenti elettronici con valore probatorio.
A37	Gestione degli accessi fisici alle aree riservate
A38	Compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini fiscali e degli altri documenti di cui è obbligatoria la conservazione
A39	Predisposizione delle dichiarazioni fiscali periodiche
A40	Liquidazione delle imposte
A41	Attività di selezione, negoziazione, stipula ed esecuzione dei contratti con privati
A42	Acquisto e gestione di software tutelati da brevetti (es. antivirus, applicativi)

⊆	Attività sensibile
A43	Gestione del sito internet aziendale
A44	Redazione del bilancio, del bilancio consolidato e delle altre comunicazioni sociali
A45	Determinazioni in materia di compenso degli amministratori, destinazioni degli utili e delle riserve
A46	Tenuta dei libri sociali
A47	Redazione dei documenti e dei prospetti informativi concernenti la Società e le società appartenenti al Gruppo
A48	Convocazione e verbalizzazione assemblea dei soci
A49	Operazioni sul capitale
A50	Comunicazione tra soci
A51	Operazioni societarie effettuate in danno ai creditori
A52	Gestione delle risorse finanziarie
A53	Gestione delle rendicontazioni delle commesse ai fini dei pagamenti
A54	Gestione della proprietà intellettuale del cliente
A55	Gestione del materiale coperto da copyright nell'ambito di gestione delle commesse
A56	Valutazione e qualificazione dei fornitori
A57	Pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro;
A58	Sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro
A59	Individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro; tra questi anche quelli derivanti dall'insorgenza di fattori esterni straordinari (emergenza sanitaria)
A60	Attività di formazione e informazione in tema di salute, sicurezza e igiene sul lavoro
A61	Pagamento e contabilizzazione
A62	Gestione dei subaffidamenti
A63	Rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro
A64	Controllo operativo delle attività
A65	Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza nei luoghi di lavoro ai sensi del D.Lgs. 81/2008 e s.m.i.
A66	Gestione dei flussi finanziari in uscita
A67	Gestione dei flussi finanziari in entrata, con particolare riguardo alla gestione dei crediti
A68	Gestione delle banche dati e degli archivi elettronici
A69	Gestione dei procedimenti penali che vedano coinvolta la Società o suoi amministratori/dipendenti.
A70	Gestione rifiuti speciali prodotti presso le sedi e tracciabilità
A71	Operazioni societarie in caso di procedura coattiva di riscossione di crediti per reati tributari
A72	Operazioni societarie in caso di procedura coattiva di riscossione di crediti per reati tributari

⊆	Attività sensibile
A73	Utilizzo di strumenti informatici per inoltro pagamenti

3 PROCESS OWNERS

Processo	Aree sensibili	Ruolo
P01- Processo commerciale	Scouting, gestione delle partnership, partecipazione alle gare e alle ricerche di mercato, Elaborazione delle offerte a clienti pubblici e privati e preparazione della documentazione, riesame delle offerte, Costituzione di consorzi e ATI, stipula contratti, richiesta di finanziamenti	Chief Executive Officer & Partner
		Chief Sales Officer & Partner
		Chief Technology Officer & Partner
		Chief Operating Officer & Partner
		Administration Manager
		Business Unit Director
		Project manager
P02- Gestione delle prescrizioni legali e regolamentari verso la PA o altre Autorità	Predisposizione e trasmissione della documentazione inerente agli adempimenti/accertamenti/ispezioni di natura fiscale e contributiva da parte dell'Amministrazione Finanziaria. Predisposizione e trasmissione della documentazione inerente agli adempimenti/accertamenti/ispezioni in merito all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata	Chief Executive Officer
P03- Gestione dei contenziosi e recupero crediti	Gestione di contenziosi giudiziali ed extragiudiziali nei confronti di soggetti pubblici e privati, recupero crediti	Chief Executive Officer & Partner
		Administration Manager
		External legal support
P04- Gestione delle risorse umane	Selezione e assunzione del personale, gestione delle presenze, delle ferie e dei permessi, pagamento retribuzioni,	Chief Executive Officer & Partner
		Business Unit Director

	gestione delle contestazioni disciplinari	HR
		Administration Manager
P05- Gestione dei sistemi informativi	Gestione e protezione dei dati relativi a clienti pubblici e privati, partner, personale e fornitori, modalità di protezione fisica, gestione delle privacy, utilizzo dei sistemi informativi da parte del personale	Chief Executive Officer & Partner
		Chief Technology Officer & Partner
		Administration Manager
		Business Unit Director
		Account Director
		Project manager
		Unit Specialist
P06- Gestione della Salute e Sicurezza sul lavoro (SSL) e dell'Ambiente	Valutazione e gestione dei rischi di SSL, ruoli e responsabilità in ambito di SSL e ambiente, coordinamento e cooperazione per la SSL in caso di affidamenti a persone fisiche e giuridiche, gestione infortuni e malattie professionali, gestione sorveglianza sanitaria, gestione dei rifiuti prodotti presso la sede.	Chief Executive Officer & Partner
P07- Approvvigionamento	Qualifica e monitoraggio dei fornitori e consulenti, emissione degli ordini di acquisto, tipologia di contratti e incarichi conferiti, gestione delle contestazioni contrattuali	Chief Executive Officer & Partner
		Account Director
		Administration Manager
		Business Unit Director
		Project manager
		Unit Specialist

P08- Processo finanziario	Gestione dei flussi finanziari e relative autorizzazioni, gestione dei conti correnti bancari, accesso al credito e richiesta finanziamenti	Chief Operating Officer & Partner
		Financial Officer & Partner
P09- Processo amministrativo	Ciclo passivo e contabilità, autorizzazione alla liquidazione delle fatture passive, redazione del bilancio, modalità di redazione e liquidazione delle relazioni fiscali periodiche (IVA e imposte sui redditi)	Chief Executive Officer & Partner
		Project manager
		Administration Manager
P10- Processo societari	Convocazione e verbalizzazione delle assemblee, gestione dei rapporti con i soci	Board
		Chief Executive Officer & Partner
		Chief Operating Officer & Partner
		Chief Financial Officer & Partner
		Chief Sales Officer & Partner
P11- Gestione delle commesse	Rapporti/incontri con i clienti pubblici e privati durante lo svolgimento delle attività, rendicontazione attività, approvazione interna ed esterna degli output di commessa, Emissione SaL attivi e certificati di pagamento/benestare alla fatturazione, gestione fatturazione e incassi	Chief Executive Officer & Partner
		Chief Operating Officer & Partner
		Chief Financial Officer & Partner
		Chief Sales Officer & Partner
		Project manager

RIFERIMENTI LEGISLATIVI E NORMATIVI

- Decreto Legislativo 8 giugno 2001, n. 231 "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" pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001;

- Confindustria- Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231 approvate il 7 marzo 2002

- D.lgs. 10 marzo 2023, n. 24 recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (c.d. "Decreto Whistleblowing").

ELENCO ALLEGATI

1 Codice etico comportamentale

2 Sistema disciplinare

3 Regolamento Organismo di Vigilanza

4 Matrice dei rischi e dei controlli interni

4_1 Mappatura livello 0

4_2 Mappatura livello 1