

**BRENNERCOM S.p.A.**

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI

DEL DECRETO LEGISLATIVO

8 GIUGNO 2001 N. 231 – PARTE SPECIALE

## Sommario

<b>1. Premessa</b>	4
<b>2. Processi sensibili e famiglie di reato potenzialmente rilevanti nell'ambito della realtà della Società</b>	4
2.1. I Processi Sensibili individuati ai sensi del Decreto 231	4
2.2. Le Attività Sensibili individuate ai sensi del Decreto 231	5
2.3. I reati considerati rilevanti per Brennercom	7
2.4. Standard di controllo generali	8
<b>3. Processo "FINANCE AND ADMINISTRATION"</b>	10
3.1. Le attività sensibili rilevanti	10
3.2. Reati applicabili	10
3.3. Standard di controllo	12
3.3.1. Standard di controllo generali	12
3.3.2. Standard di controllo specifici	12
<b>4. Processo "PROCUREMENT, GENERAL SERVICES AND COMPLIANCE"</b>	19
4.1. Le attività sensibili rilevanti	19
4.2. Reati applicabili	19
4.3. Standard di controllo	21
4.3.1. Standard di controllo generali	21
4.3.2. Standard di controllo specifici	21
<b>5. Processo "AMBIENTE"</b>	28
5.1. Le attività sensibili rilevanti	28
5.2. Reati applicabili	28
5.3. Standard di controllo	28
5.3.1. Standard di controllo generali	28
5.3.2. Standard di controllo specifici	29
<b>6. Processo "SALUTE E SICUREZZA"</b>	31
6.1. Le attività sensibili rilevanti	31
6.1.1. Generalità	31
6.1.2. Attività a rischio di reato	32
6.2. Reati applicabili	32
6.2.1. Modalità di commissione dei reati	32
6.3. Standard di controllo	34
6.3.1. Standard di controllo generali	34
6.3.2. Standard di controllo specifici	34
<b>7. Processo "RISORSE UMANE E ORGANIZZAZIONE"</b>	40
7.1. Le attività sensibili rilevanti	40
7.2. Reati applicabili	40
7.3. Standard di controllo	41
7.3.1. Standard di controllo generali	41
7.3.2. Standard di controllo specifici	41
<b>8. Processo "RESEARCH AND DEVELOPMENT"</b>	46
8.1. Le attività sensibili rilevanti	46
8.2. Reati applicabili	46
8.3. Standard di controllo	46
8.3.1. Standard di controllo generali	46
8.3.2. Standard di controllo specifici	47
<b>9. Processo "INFORMATION TECHNOLOGY"</b>	48

9.1. Le attività sensibili rilevanti	48
9.2. Reati applicabili	48
9.3. Standard di controllo	49
9.3.1. Standard di controllo generali	49
9.3.2. Standard di controllo specifici	49
<b>10. Processo “MARKETING COMMUNICATION”</b>	<b>52</b>
10.1. Le attività sensibili rilevanti	52
10.2. Reati applicabili	52
10.3. Standard di controllo	53
10.3.1. Standard di controllo generali	53
10.3.2. Standard di controllo specifici	53
<b>11. Processo “LEGAL &amp; CORPORATE AFFAIRS”</b>	<b>56</b>
11.1. Le attività sensibili rilevanti	56
11.2. Reati applicabili	56
11.3. Standard di controllo	56
11.3.1. Standard di controllo generali	56
11.3.2. Standard di controllo specifici	57
<b>12. Processo “RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE”</b>	<b>59</b>
12.1. Le attività sensibili rilevanti	59
12.2. Reati applicabili	59
12.3. Standard di controllo	60
12.3.1. Standard di controllo generali	60
12.3.2. Standard di controllo specifici	60
<b>13. Processo “OPERATIONS: PLATFORM &amp; INFRASTRUCTURE”</b>	<b>64</b>
13.1. Le attività sensibili rilevanti	64
13.2. Reati applicabili	64
13.3. Standard di controllo	65
13.3.1. Standard di controllo generali	65
13.3.2. Standard di controllo specifici	65
<b>14. Processo “VENDITE”</b>	<b>73</b>
14.1. Le attività sensibili rilevanti	73
14.2. Reati applicabili	73
14.3. Standard di controllo	74
14.3.1. Standard di controllo generali	74
14.3.2. Standard di controllo specifici	74
<b>15. Processo “BUSINESS OPERATION &amp; DEVELOPMENT”</b>	<b>79</b>
15.1. Le attività sensibili rilevanti	79
15.2. Reati applicabili	79
15.3. Standard di controllo	80
15.3.1. Standard di controllo generali	80
15.3.2. Standard di controllo specifici	80

## 1. Premessa

Il presente documento costituisce la Parte Speciale del Modello 231 ed ha lo scopo di assicurare la definizione, all'interno di Brennercom S.p.A. (di seguito solo "Brennercom" o la "Società"), di un quadro comune di riferimento, che delinea i principi, le norme comportamentali e procedurali, nonché i protocolli di controllo finalizzati a disciplinare concretamente le condotte dei Destinatari del Modello 231 al fine di prevenire, nell'ambito delle specifiche attività svolte e considerate a rischio, la commissione dei reati previsti dal Decreto 231 e garantire condizioni di eticità, correttezza e trasparenza nella conduzione delle attività.

In linea con quanto definito nella Parte Generale del Modello 231 di Brennercom, sono considerati Destinatari i componenti degli organi sociali, il management ed i dipendenti di Brennercom, nonché tutti coloro che operano per il conseguimento degli obiettivi della Società.

La Parte Speciale del Modello 231 è suddivisa per Processo Sensibile e identifica, per ciascuno di essi, le Attività Sensibili che Brennercom ha valutato essere potenzialmente a rischio di commissione dei reati previsti dal Decreto 231 nonché il sistema di controllo adottato ai fini della prevenzione di tali reati.

Il Sistema di Controllo progettato e implementato da Brennercom prevede **standard di controllo generali**, ossia principi di controllo che si applicano indistintamente a ciascun processo e **standard di controllo specifici** che rappresentano protocolli di controllo definiti e progettati per la gestione dei processi e di ciascuna Attività Sensibile.

L'individuazione dei Processi Sensibili e delle Attività Sensibili e la successiva elaborazione della presente Parte Speciale, ha previsto l'adozione dell'approccio metodologico descritto al Paragrafo 5.4 della Parte Generale del presente Modello 231.

Di seguito si riportano le informazioni relative a ciascun Processo Sensibile indicate nelle rispettive sezioni del documento:



## 2. Processi sensibili e famiglie di reato potenzialmente rilevanti nell'ambito della realtà della Società

### 2.1. I Processi Sensibili individuati ai sensi del Decreto 231

A seguito dell'attività di mappatura dei rischi svolta, sono stati individuati i seguenti Processi Sensibili:



## 2.2. Le Attività Sensibili individuate ai sensi del Decreto 231

L'art. 6, comma 2, lett. a), del Decreto 231 prevede che il modello debba individuare le attività nel cui ambito possano essere commessi i reati presupposto. In coerenza con tale previsione, Brennercom ha provveduto ad identificare le Attività Sensibili nel cui ambito potrebbero essere commessi i Reati 231 attraverso l'attività di valutazione dei rischi (*Risk Self Assessment*) richiamata nella Parte Generale del Modello 231.

Di seguito l'elenco delle Attività Sensibili identificate:

- Gestione delle operazioni straordinarie (es. fusioni, acquisizioni, cessioni rami d'azienda, scissioni, joint venture), anche tramite il supporto di advisor esterni (inclusa la valutazione delle terze parti);
- Gestione della finanza (flussi in entrate e uscita) e della tesoreria (inclusi rapporti con le banche e gli istituti finanziari) Amministrazione, contabilità e bilancio (valutazioni e stime di poste di bilancio; rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa, aggiornamento del piano dei conti);
- Gestione degli adempimenti fiscali (calcolo dell'obbligazione tributaria e la predisposizione e la presentazione delle dichiarazioni fiscali);
- Gestione del credito;
- Tenuta e custodia della documentazione obbligatoria e delle scritture contabili;
- Gestione dei rapporti con i soci, il collegio sindacale e la società di revisione;
- Gestione delle operazioni e transazioni infragruppo;
- Capitalizzazione asset e gestione dei piani di ammortamento (Cessione e dismissione asset);
- Gestione del capitale sociale, anche in sede di effettuazione di operazioni di finanza straordinaria o di liquidazione, degli utili e delle riserve;
- Selezione e qualifica dei fornitori di beni, servizi e consulenze;
- Approvvigionamento di beni, di lavori e servizi, incluso l'affidamento di appalti e gestione

subappalti;

- Approvigionamento di consulenze ed incarichi di prestazioni professionali;
- Gestione dei rapporti con enti certificatori;
- Gestione degli accessi fisici ai siti aziendali;
- Gestione dei benefit e delle utilities aziendali;
- Gestione delle assicurazioni (insurance management);
- Gestione della compliance ambientale;
- Gestione dei rifiuti;
- Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali;
- Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL;
- Gestione della documentazione interna (articolazione del sistema normativo) relativa agli aspetti SSL;
- Definizione delle misure per il controllo operativo e la gestione del cambiamento;
- Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso;
- Attività di sorveglianza sanitaria;
- Comunicazione, partecipazione e consultazione: gestione delle riunioni periodiche di sicurezza, consultazione dei lavoratori e delle loro rappresentanze;
- Gestione di incidenti non conformità e azioni correttive;
- Gestione del processo di selezione, assunzione e sviluppo del personale;
- Definizione di ruoli, responsabilità e organizzazione all'interno della Società;
- Gestione delle attività di valutazione, remunerazione ed incentivazione del personale, inclusa l'erogazione di compensi variabili;
- Gestione del payroll e dell'amministrazione del personale;
- Gestione delle trasferte, delle note spese e delle spese di rappresentanza;
- Gestione dei progetti di ricerca e sviluppo di nuovi prodotti e servizi (incluse le indagini in merito a brevetti o altri diritti di proprietà industriale di terzi), anche tramite rapporti con università, enti di ricerca, partner esterni, associazioni o istituzioni;
- Gestione di marchi e brevetti di proprietà, anche tramite terzi;
- Gestione di accessi logici, account e profili;
- Gestione della sicurezza informatica;
- Gestione dei sistemi hardware e software e dell'acquisizione di licenze software;
- Gestione degli accessi fisici ai siti ove risiedono infrastrutture IT;
- Gestione della smart card per firme digitali;
- Gestione delle attività di marketing, pubblicità e comunicazione (compresa la gestione dei contenuti);
- Gestione di sponsorizzazioni, omaggi, donazioni ed erogazioni liberali;
- Gestione dei contenuti del sito Internet della Società e dei relativi social network, anche tramite soggetti terzi;
- Gestione di procedimenti giudiziari, arbitrari e stragiudiziali con la P.A. e con soggetti terzi;
- Gestione delle richieste di informazioni dalla Procura della Repubblica (inclusa la raccolta e la gestione di traffico dati ai fini di giustizia);
- Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione);
- Gestione dei rapporti con la Pubblica Amministrazione per la richiesta e l'ottenimento di

informazioni e di diritti di passaggio, licenze, permessi, autorizzazioni per lo sviluppo dell'infrastruttura;

- Gestione dei rapporti con soggetti istituzionali (inclusa la gestione delle relazioni con AGCOM, Ministeri statali, strutture comunitarie) con altri stakeholder (decision e opinion maker) e attività di lobbying;
- Gestione dei rapporti con gli enti competenti in occasione di ispezioni o verifiche di natura fiscale, previdenziale o lavoristica (ad es. Agenzia delle Entrate, Guardia di Finanza, Ispettorato del lavoro, INPS, INAIL, etc.);
- Gestione del servizio VOCE con tecnologia Voice Over IP e dei servizi di Unified Communication (ad esempio il Direct Routing);
- Gestione delle attività di delivery dei servizi della divisione P&I e contatto finale con i clienti nelle fasi di installazione, collaudo e verifica prodotto;
- Gestione contrattualistica "ultimo miglio" con provider di servizi Wholesale;
- Gestione dei servizi di housing & colocation (inclusa la sicurezza fisica) all'interno dei Data Center su territorio nazionale ed estero;
- Gestione dell'infrastruttura di rete (broadband / ultrabroadband / rete mista), compreso il coordinamento di terze parti per l'implementazione dell'infrastruttura ed erogazione del servizio di connessione;
- Gestione della Cyber Security e dei servizi di sicurezza informatica (inclusa la gestione delle terze parti necessarie per l'erogazione dei servizi di sicurezza);
- Gestione dei servizi Cloud (inclusi lo storage Cloud e il servizio Multicloud aziendale);
- Gestione attività di scouting fornitori sul mercato (es. individuazione di provider di nuove tecnologie tramite analisi di mercato);
- Gestione dei servizi a supporto del cliente (c.d. "Managed Services");
- Gestione del magazzino;
- Vendite dirette alla Pubblica Amministrazione (PAC, PAL, Regioni e altri enti pubblici) mediante la partecipazione a gare e assegnazioni dirette (incluse le assegnazioni MEPA);
- Vendite indirette: Gestione delle attività di vendita di servizi tramite agenzie e procuratori d'affari e partner commerciali;
- Gestione delle attività di vendita;
- Definizione della componente tecnica degli elementi di offerta, inclusa l'individuazione e selezione di eventuali partner ("service integrator") e di quantificazione dei costi;
- Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione).

### 2.3. I reati considerati rilevanti per Brennercom

Sulla base delle analisi condotte ed in considerazione delle finalità statutarie, del contesto aziendale e dei processi di Brennercom, i reati considerati potenzialmente applicabili sono:

- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico<sup>1</sup>;
- Delitti informatici e trattamento illecito di dati;
- Delitti di criminalità organizzata;
- Concussione, induzione indebita a dare o promettere utilità e corruzione<sup>1</sup>;
- Delitti contro l'industria e il commercio;

<sup>1</sup> Di seguito "Reati contro la Pubblica Amministrazione"

- Reati societari;
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- Delitti contro la personalità individuale;
- Abusi di mercato;
- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- Delitti in materia di violazione del diritto d'autore;
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- Reati Ambientali;
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- Razzismo e Xenofobia;
- Reati tributari;
- Reati transnazionali;

#### 2.4. Standard di controllo generali

Gli standard di controllo generali sono individuati dalla Società quali principi-guida dell'intero sistema di controllo interno e di gestione dei rischi e, pertanto, risultano applicabili a tutti i processi aziendali e rispettive Attività Sensibili. Pertanto, per efficacia espositiva e di sintesi, se ne riporta la descrizione nel presente paragrafo anziché nell'ambito della descrizione del sistema di controllo di ciascun processo. Si segnala che, per i processi e le relative attività sensibili gestite in service dalla Capogruppo, gli standard di controllo generali applicabili sono i medesimi, ma svolti da Retelit S.p.A.

#### **SOD – Segregazione dei compiti**

Nell'ambito di ciascun processo aziendale rilevante, al fine di garantire indipendenza e obiettività, la Società assicura l'intervento di più soggetti e la separazione delle attività tra coloro che sono incaricati di assumere le decisioni/autorizzare gli atti, di eseguire le operazioni stabilite, e di svolgere sulle stesse gli opportuni controlli previsti dalla legge e dalle procedure del sistema di controllo interno. Tale presidio è funzionale, nel suo complesso, a mitigare la discrezionalità gestionale nelle attività e nei singoli processi. Un intero processo sensibile ai sensi del Decreto 231 non può, dunque, essere affidato a un unico soggetto.

#### **NORME – Sistema procedurale**

Esistenza di specifiche procedure aziendali, disponibili e conosciute all'interno di Brennercom, che stabiliscono responsabilità, modalità operative e controlli per lo svolgimento delle Attività Sensibili. La regolamentazione interna declina ruoli e responsabilità di gestione, coordinamento e controllo delle strutture aziendali a tutti i livelli, descrivendo, in maniera omogenea, le attività proprie di ciascuna struttura. Tale principio, attuato dalla Società, è funzionale ad assicurare la conformità dei comportamenti rispetto alle linee di indirizzo e gestionali definite dalla Società.

#### **POTERI – Poteri autorizzativi e di firma**

Esistenza di un sistema di poteri autorizzativi interni e di procure e deleghe coerente con le responsabilità organizzative e gestionali assegnate, contenente la specifica indicazione di poteri, limiti e deroghe, anche di approvazione delle spese, ai soggetti che hanno titolo per impegnare la Società nei confronti dei Soggetti Terzi. Tale sistema consente la riconducibilità degli atti aziendali, aventi rilevanza esterna o interna, alle persone fisiche che li hanno adottati, risultando utile ai fini dell'identificazione successiva dei soggetti responsabili dell'adozione di atti attraverso i quali, direttamente o indirettamente, sia stato commesso un reato.

#### **TRACCIABILITA' – Documentabilità e tracciabilità**

L'iter decisionale, autorizzativo e lo svolgimento di ciascun Processo Sensibile deve poter essere ricostruito e verificato ex post. Più precisamente, per ciascuna operazione e attività relativa a ogni Processo Sensibile, deve essere conservata e archiviata adeguata evidenza su supporto documentale o informatico.

Qualora nello svolgimento delle Attività Sensibili siano utilizzati sistemi informatici, tali sistemi devono assicurare:

- l'accesso al sistema ai soli soggetti in possesso di abilitazione;
- la corretta imputazione di ogni singola operazione ai soggetti che ne sono responsabili;
- la tracciabilità delle operazioni effettuate in tutte le fasi;
- l'archiviazione e conservazione delle registrazioni prodotte.

### 3. Processo “FINANCE AND ADMINISTRATION”

#### 3.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Finance & Administration”<sup>2</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione delle operazioni straordinarie (es. fusioni, acquisizioni, cessioni rami d'azienda, scissioni, joint venture), anche tramite il supporto di advisor esterni (inclusa la valutazione delle terze parti);
- Gestione della finanza (flussi in entrate e uscita) e della tesoreria (inclusi rapporti con le banche e gli istituti finanziari);
- Amministrazione, contabilità e bilancio (valutazioni e stime di poste di bilancio; rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nelle relazioni, nei bilanci e in altri documenti di impresa, aggiornamento del piano dei conti);
- Gestione degli adempimenti fiscali (*calcolo dell'obbligazione tributaria e la predisposizione e la presentazione delle dichiarazioni fiscali*);
- Gestione del credito;
- Tenuta e custodia della documentazione obbligatoria e delle scritture contabili;
- Gestione dei rapporti con i soci, il collegio sindacale e la società di revisione;
- Gestione delle operazioni e transazioni infragruppo;
- Capitalizzazione asset e gestione dei piani di ammortamento (Cessione e dismissione asset);
- Gestione del capitale sociale, anche in sede di effettuazione di operazioni di finanza straordinaria o di liquidazione, degli utili e delle riserve;

#### 3.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

##### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 316 bis Malversazione a danno dello Stato o di altro ente pubblico
- art 316 c.p. Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee
- art. 317 c.p. Concussione
- art. 318 c.p. Corruzione per esercizio della funzione
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio
- art. 319 bis c.p. Circostanze aggravanti
- art. 319 ter c.p. Corruzione in atti giudiziari
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità
- art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p. Pene per il corruttore
- art. 322 c.p. Istigazione alla corruzione
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 640 c.p. Truffa
- art 640 bis c.p. Truffa aggravata per il conseguimento di erogazioni pubbliche

<sup>2</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A

**Reati societari (art. 25 ter)**

- art. 2621 c.c. False comunicazioni sociali
- art. 2621 bis c.c. Fatti di lieve entità
- art. 2622 c.c. False comunicazioni sociali delle società quotate
- art. 2625 c.c. Impedito controllo
- art. 2628 c.c. Illecite operazioni sulle azioni o quote sociali o della società controllante
- art. 2629 c.c. Operazioni in pregiudizio dei creditori
- art. 2629 c.c. Omessa comunicazione del conflitto di interessi
- art. 2632 c.c. Formazione fittizia del capitale
- art. 2635 c.c. Corruzione tra privati
- art. 2635 bis c.c. Istigazione alla corruzione tra privati
- art. 2636 c.c. Illecita influenza sull'assemblea
- art. 2637 c.c. Aggiotaggio
- art. 2638 c.c. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

**Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

**Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso

**Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art. 25 octies)**

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

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

- art. 270 bis c.p. Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
- L. n. 153/2016, art.270 quinques 1 c.p. Finanziamento di condotte con finalità di terrorismo
- art. 2 Convenzione di New York del 9 dicembre 1999

**Reati tributari (art. 25 quinquies)**

- art 2 D. Lgs 74/2000 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- art. 3 D. Lgs 74/2000 Dichiarazione fraudolenta mediante altri artifici
- art. 4 D. Lgs 74/2000 Dichiarazione infedele
- art. 5 D. Lgs 74/2000 Omessa dichiarazione
- art. 8 D. Lgs 74/2000 Emissione di fatture o altri documenti per operazioni inesistenti
- art. 10 D. Lgs 74/2000 Occultamento o distruzione di documenti contabili
- art. 10quater D. Lgs 74/2000 Indebita compensazione
- art. 11 D. Lgs 74/2000 Sottrazione fraudolenta al pagamento di imposte

### 3.3. Standard di controllo

#### 3.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

#### 3.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

**a) Gestione delle operazioni straordinarie (es. fusioni, acquisizioni, cessioni rami d'azienda, scissioni, joint venture), anche tramite il supporto di advisor esterni (inclusa la valutazione delle terze parti)**

- ogni operazione straordinaria venga approvata dal Consiglio di Amministrazione della Società;
- sia previsto, anche attraverso il supporto di eventuali Advisor specialistici, l'avvio di attività di Due Diligence esterna (in caso di acquisizione) o interna (in caso di cessioni) sull'oggetto della compravendita. Il rapporto di Due Diligence deve contenere:
  - nominativi delle persone che hanno condotto le attività di due diligence;
  - esami effettuati e relativi esiti;
  - deduzioni e raccomandazioni fatte;
  - eventuali modifiche agli accordi da proporre alla controparte;
- prima di effettuare qualsiasi operazione di costituzione e/o acquisizione del controllo, anche in via indiretta, di società o enti assimilabili aventi sede legale in uno Stato estero, sia verificato che lo Stato in cui la società ha sede:
  - garantisca un regime di trasparenza dell'informazione societaria compatibile con il regime di trasparenza in materia garantito dagli Stati dell'Unione Europea;
  - non sia presente nell'elenco dei Paesi a regime fiscale privilegiato (c.d. "black list");
- sia predisposta idonea documentazione a supporto dell'operazione proposta, nonché una relazione informativa preliminare che illustri i contenuti, l'interesse sottostante e le finalità strategiche dell'operazione;
- sia verificata preliminarmente la completezza, inerenza e correttezza della documentazione di supporto dell'operazione;
- sia previsto il sistematico coinvolgimento della Legal & Corporate Affairs affinché valuti i riflessi fiscali dell'operazione e l'eventuale necessità di pareri indipendenti;
- siano definite le modalità di coinvolgimento di Advisor esterni, nonché le modalità di accesso da parte di questi ultimi ad informazioni e documentazione della Società e/o dell'operazioni straordinaria;
- ove richiesto o opportuno, la società di revisione e il Collegio Sindacale esprimano motivato parere sull'operazione.

**b) Gestione della finanza e della tesoreria**

- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta della disposizione di pagamento per assolvere l'obbligazione;
  - effettuazione del pagamento;
  - controllo/riconciliazioni a consuntivo.
- ogni pagamento o altra uscita di cassa sia autorizzato sulla base delle procure assegnate, previa acquisizione della documentazione di supporto debitamente verificata e validata;
- sia svolta una verifica preventiva affinché le transazioni finanziarie siano effettuate, nel rispetto

delle normative applicabili, nei confronti di controparti effettivamente esistenti e per prestazioni effettivamente ricevute;

- sia effettuato un costante monitoraggio dei flussi finanziari aziendali, prestando la massima attenzione alle notizie riguardanti i soggetti con i quali Brennercom ha rapporti di natura finanziaria o societaria, con particolare riferimento a quelli che possano ingenerare il sospetto della commissione di uno dei reati di cui alla presente parte speciale;
- sia fatto divieto di intrattenere rapporti commerciali con soggetti in relazione ai quali sia nota o sospetta, sulla base di indizi precisi e concordanti, i) l'appartenenza ad organizzazioni criminali, ii) la provenienza illecita di fondi, iii) l'operatività al di fuori della legge;
- sia garantita correttezza e completezza delle operazioni di pagamento anche finalizzate ad accertare che: i) l'importo sia corrispondente a quanto effettivamente dovuto e previsto contrattualmente; ii) vi sia corrispondenza tra l'appoggio bancario indicato in fattura e quello presente in anagrafica; iii) l'operazione sia stata debitamente autorizzata;
- sia fatto obbligo di: i) utilizzare esclusivamente i canali bancari e altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi; ii) collaborare esclusivamente con operatori che rispondano a requisiti di professionalità, etica, onorabilità e trasparenza; iii) utilizzare esclusivamente, nella gestione delle transazioni finanziarie, operatori che si ritenga non siano coinvolti in operazioni di impiego o raccolta di denaro di dubbia o illecita provenienza; iv) effettuare i pagamenti solo a favore della controparte designata contrattualmente e nel Paese in cui la controparte ha la propria sede legale o nel Paese in cui la fornitura di beni e servizi viene eseguita;
- siano previsti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative. Il superamento dei limiti quantitativi di spesa assegnati sia ammesso solo ed esclusivamente per comprovati motivi di urgenza e in casi eccezionali: in tali casi è previsto che si proceda alla sanatoria dell'evento eccezionale attraverso il rilascio delle debite autorizzazioni;
- sia previsto il divieto di utilizzo del contante, ad eccezione dell'uso per importi non significativi della cassa interna, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie;
- siano definite le modalità di apertura e chiusura di conti correnti bancari, inclusa l'identificazione dei soggetti aziendali delegati per tale compito;
- siano effettuate riconciliazioni dei conti correnti bancari e sia verificata l'accuratezza della documentazione a supporto;
- vi sia una chiara attribuzione dei compiti per la custodia e gestione della piccola cassa (es. autorizzazione all'utilizzo della cassa; reintegro della cassa; controlli periodici di monitoraggio sulle giacenze di cassa; ecc.);
- siano definiti i limiti di giacenza e le tipologie di spesa che possono essere sostenute a mezzo piccola cassa;
- sia verificata la completezza ed accuratezza della richiesta di anticipo spese in termini di limiti di importo e di caratteristiche quali-quantitative dei beni oggetto della richiesta;
- sia effettuata una riconciliazione periodica tra giacenza fisica del fondo cassa, giustificativi e registrazione in contabilità;
- siano definite le modalità di archiviazione della documentazione relativa all'utilizzo della piccola cassa, al fine di permettere un controllo ex post;
- sia garantita trasparenza e tracciabilità degli accordi con altre imprese per la realizzazione di investimenti in partnership, verificandone la congruità economica rispetto ai prezzi mediamente

praticati sul mercato;

- sia fatto divieto di porre in essere operazioni simulate o altri artifici su strumenti finanziari della Società e di società del Gruppo;
- siano effettuate verifiche ex-post sulle transazioni tramite adeguati supporti documentali/informatici, verificando in particolare il processo di decisione, l'autorizzazione e svolgimento dell'attività sensibile, anche tramite apposite evidenze archiviate e, in ogni caso, dettagliando la disciplina della possibilità di cancellare o distruggere le registrazioni effettuate;

**c) Gestione della contabilità generale, tenuta e custodia della documentazione obbligatoria e delle scritture contabili**

- siano identificati i soggetti deputati alla gestione della contabilità e alla predisposizione ed approvazione delle comunicazioni sociali o documentazione equivalente;
- sia garantita la segregazione delle funzioni tra chi provvede all'esecuzione dei pagamenti e chi effettua una verifica di coerenza del pagamento con la prestazione o i servizi ricevuti;
- sia fatto divieto di predisporre, rappresentare o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non rispondente alla realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società e del Gruppo;
- sia garantita la comunicazione di tutti i dati e informazioni imposti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- sia fatto divieto di disattendere i principi, le norme e le procedure in materia di redazione dei bilanci, relazioni ed informativa;
- sia verificata e accertata la coerenza contabile tra ordini di vendita e incassi;
- sia garantita la tracciabilità, anche attraverso i sistemi informativi aziendali, di tutte le fatture e sia verificata l'esistenza di un benestare (entrata merce a sistema e/o conferma di avvenuta prestazione nel caso di servizi, fattura firmata, e-mail, comunicazione interna o altro) al fine di rendere la fattura pagabile;
- i profili di accesso al sistema contabile siano identificati dal Responsabile dei Sistemi Informativi sotto la supervisione del Responsabile Amministrazione di Gruppo, nel rispetto dei principi di separazione delle funzioni e di coerenza dei livelli autorizzativi con le mansioni;
- siano pianificate le attività necessarie alla chiusura dell'esercizio sociale e alla redazione del progetto di Bilancio secondo un calendario che deve essere comunicato a tutti i soggetti coinvolti nel processo;
- si provveda ad elencare i dati e le informazioni che ciascuna funzione aziendale deve comunicare, i criteri di elaborazione e predisposizione del bilancio, nonché la tempistica di consegna e sia supervisionata la raccolta e l'elaborazione tempestiva da parte dei soggetti delegati ai fini della predisposizione del bilancio;
- siano definite le regole per la valutazione e la stima delle poste di bilancio (quali revenue recognition, valutazioni di magazzino, valutazione dei crediti, regole di cut off, fondo rischi oneri, ecc.);
- tutte le assunzioni e le informazioni strumentali al processo valutativo o di stima delle voci di bilancio siano archiviate sotto la responsabilità delle Funzioni aziendali che producono/ricevono tali informazioni;
- ogni modifica ai dati contabili possa essere effettuata dalla sola Direzione/Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Direttore/Responsabile di Funzione;
- siano definite le modalità di utilizzo dei conti transitori e di verifica periodica degli stessi;
- sia disposta una verifica, con cadenza periodica, dei saldi di contabilità generale con i relativi partitari per garantirne la quadratura;
- siano definite le regole per la gestione del piano dei conti, prevedendo apposita autorizzazione

per l'accensione di un nuovo conto, modifica o eliminazione di conti esistenti;

- la rilevazione e l'aggregazione dei dati e delle informazioni necessarie ai fini della redazione del bilancio siano effettuata secondo modalità tali da assicurare la tracciabilità dei dati e l'individuazione dei soggetti che li hanno elaborati ed inseriti nel sistema contabile. Eventuali criticità o situazioni anomale devono essere tempestivamente segnalate ai soggetti gerarchicamente sovraordinati;
- la redazione del bilancio di esercizio e del bilancio consolidato siano effettuate nel rispetto dei principi stabiliti dalle procedure amministrativo-contabili adottate dalla Società e conformemente ai principi contabili applicabili. Eventuali variazioni non giustificate nell'applicazione dei principi contabili stabiliti dalle procedure o nei dati già contabilizzati in base alle procedure in essere, siano tempestivamente segnalate all'Organismo di Vigilanza;

**d) Gestione degli adempimenti fiscali (calcolo dell'obbligazione tributaria e la predisposizione e la presentazione delle dichiarazioni fiscali)**

- siano formalmente identificati i soggetti deputati ad intrattenere i rapporti e a rappresentare la Società nei confronti dell'Amministrazione Finanziaria e dell'Agenzia delle Dogane, anche in sede di ispezioni ed accertamenti da parte di queste ultime;
- sia garantita segregazione tra chi effettua il calcolo delle imposte e predispone i modelli di versamento e dichiarativi e chi approva il pagamento delle imposte;
- siano formalmente definite le modalità e i criteri per la determinazione delle imposte, correnti e differite, nel rispetto della normativa fiscale vigente;
- sia verificata la completezza e correttezza del calcolo delle imposte, correnti e differite, nonché la completa e corretta registrazione contabile;
- sia prevista una sottoscrizione formale, nel rispetto delle responsabilità in essere, dei modelli di versamento e dichiarativi;
- sia prevista l'adozione di modalità operative per verificare, anche con il supporto di soggetti autonomi ed indipendenti, la corretta predisposizione delle dichiarazioni fiscali (es. invio a consulenti fiscali esterni dei modelli dichiarativi definitivi unitamente alla documentazione di supporto);
- sia disposto il rilascio di attestazioni da parte della Funzione Amministrazione, dopo la chiusura dell'esercizio e prima della contabilizzazione delle imposte, alla Funzione Fiscale a conferma che: (i) sia stata data completa, corretta e tempestiva informazione scritta dei fatti e degli atti riguardanti la Società; (ii) le rilevazioni contabili delle operazioni riguardanti la Società siano state eseguite nel rispetto dei principi di inerenza, competenza e documentazione; (iii) non si sia a conoscenza, alla data di rilascio dell'attestazione, di altre informazioni e dati che possano avere rilevanza ai fini della corretta e completa rappresentazione della situazione economica e patrimoniale della Società;
- siano predisposti, ove necessario, prospetti di confronto con i dati dell'esercizio precedente evidenziando i principali fenomeni, in termini di significatività e di complessità di valutazione, che hanno caratterizzato la determinazione dell'imponibile e l'elaborazione della dichiarazione;
- sia prevista l'analisi delle principali variazioni fiscali (in aumento e in diminuzione) di carattere permanente e temporaneo ai fini IRES al fine sia di individuare i fenomeni che hanno concorso a determinare le stesse, sia di valutarne l'incidenza attraverso il raffronto con il corrispondente periodo dell'esercizio precedente;
- sia effettuato un monitoraggio costante dell'evoluzione della normativa di riferimento e delle tempistiche da rispettare per le comunicazioni/denunce/adempimenti nei confronti dell'Amministrazione Finanziaria e dell'Agenzia delle Dogane;
- siano definite le modalità operative di gestione degli adempimenti doganali nonché del monitoraggio delle loro scadenze;

- siano preventivamente verificate le informazioni e i dati da trasmettere all'agenzia delle dogane;
- sia garantita completezza, correttezza e trasparenza delle informazioni e dei dati trasmessi al fine di assolvere agli adempimenti richiesti dall'agenzia delle dogane;
- gli atti, le richieste e le comunicazioni formali che hanno come controparte l'Amministrazione Finanziaria e l'Agenzia delle Dogane e gli enti certificatori siano gestiti e autorizzati da personale dotato di idonei poteri in base alle norme interne;
- sia garantita la tracciabilità, anche attraverso i sistemi informativi aziendali, di tutte le dichiarazioni, la reportistica relativa alla gestione degli adempimenti fiscali;

**e) Gestione del credito**

- siano identificate le funzioni responsabili nell'ambito del processo di affidamento dei clienti e di determinazione dei limiti di credito;
- sia garantita la segregazione delle funzioni tra chi gestisce il rapporto con il cliente e autorizza la vendita e chi ne gestisce l'eventuale credito derivante;
- siano declinate le modalità operative interne di effettuazione di controlli preventivi:
  - sulla situazione economico-finanziaria nonché su altre tipologie di informazioni relative al cliente funzionali alla verifica dell'affidabilità finanziaria del cliente e determinazione dei limiti di fido;
  - qualitativi sul cliente, a titolo d'esempio: l'ottenimento del certificato antimafia, l'ultimo beneficiario, la verifica della presenza di carichi pendenti o passati in giudicato su amministratori, la verifica dei soci e dei principali dirigenti, ecc.
  - l'eventuale ottenimento di garanzie attive a fronte delle valutazioni preliminari effettuate;
- i limiti di fido siano sottoposti all'approvazione di soggetti interni responsabili;
- siano formalmente definite le modalità attraverso le quali attuare la procedura di recupero del credito;
- siano identificati i soggetti autorizzati a concordare un eventuale piano di rientro;
- sia adottato un approccio progressivo nella gestione del credito scaduto al crescere dell'*ageing* della posizione.

**f) Gestione dei rapporti con i soci, il collegio sindacale e la società di revisione**

- sia fatto divieto di porre in essere comportamenti che impediscano materialmente o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale, della società di revisione o dei soci;
- sia fatto divieto di determinare o influenzare le deliberazioni dell'assemblea, mediante atti simulati o fraudolenti volti ad alterare la regolare formazione della volontà assembleare;
- sia garantita la segregazione dei compiti tra chi prepara la documentazione per le riunioni del Consiglio di Amministrazione, dell'Assemblea dei Soci e del Collegio Sindacale, chi ne verifica la correttezza e completezza e chi ne autorizza la trasmissione;
- siano definite chiare modalità di convocazione delle adunanze del Consiglio di Amministrazione, dell'Assemblea dei Soci e del Collegio Sindacale, in linea con la normativa applicabile;
- la bozza di bilancio, le relazioni accompagnatorie e tutti i documenti contabili relativi agli argomenti indicati nell'ordine del giorno delle riunioni del Consiglio di Amministrazione, siano completi e messi a disposizione degli amministratori e degli organi di controllo con ragionevole anticipo rispetto alla data fissata per la riunione;
- sia svolto un monitoraggio delle scadenze per depositare gli atti degli adempimenti societari;
- sia svolto un monitoraggio periodico mirato a verificare eventuali aggiornamenti normativi in materia societaria;
- siano formalizzate regole volte a garantire la correttezza e la trasparenza delle informazioni da inviare ai Soci, al Consiglio di Amministrazione e al Collegio Sindacale;

- ai Sindaci ed alla Società di revisione sia sempre assicurata la possibilità di prendere contatto con l'OdV per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione alle ipotesi di reato considerate;
- siano definite le modalità di tenuta e archiviazione della documentazione e dei relativi documenti ufficiali, degli atti e delle decisioni del Consiglio di Amministrazione, del Collegio Sindacale e dell'Assemblea dei Soci, ad opera del Responsabile, in un apposito archivio, con modalità tali da impedire la modifica successiva, se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**g) Gestione delle operazioni e transazioni infragruppo**

- siano identificati i soggetti deputati ad intrattenere i rapporti e a rappresentare la Società nell'ambito delle operazioni e transazioni infragruppo;
- sia garantita la segregazione tra chi predispone i contratti infragruppo, chi verifica la coerenza degli stessi rispetto alle attività infragruppo da svolgere e/o ricevere, chi effettua i controlli sulla coerenza con la normativa di riferimento dei transfer pricing inseriti nei contratti infragruppo e chi autorizzata/sottoscrive il contratto infragruppo;
- tutte le operazioni intercorse tra la Società e le Società controllate e controllanti, con particolare riguardo alle reciproche situazioni debitorie e creditorie e sulle operazioni compiute tra le stesse nel corso dell'esercizio, compresa la prestazione di garanzie per gli strumenti finanziari emessi in relazione alle operazioni previste nell'oggetto sociale, siano avvenute nel rispetto dello Statuto sociale e delle normative di legge vigenti;
- tutte le operazioni Infragruppo siano riportate in bilancio e periodicamente consuntivate e riconciliate;
- tutte le operazioni Infragruppo, di natura sia commerciale che finanziaria, siano formalizzate con contratti preventivamente autorizzati dai rispettivi Consigli di Amministrazione;
- siano definiti i criteri di determinazione e gestione dei prezzi di trasferimento, con indicazione del perimetro di applicazione degli stessi, ove sia necessario (es. ambito Transfer Price);
- siano descritte all'interno del contratto intercompany le modalità di definizione dei prezzi di trasferimento e le attività svolte per conto della controparte;
- siano definite delle attività di monitoraggio dei rapporti infragruppo;
- sia verificata l'esistenza e la coerenza delle transazioni intercompany, dove per le fatture ricevute o emesse dalla Società a fronte dell'acquisto o della vendita di beni e servizi infragruppo, la registrazione contabile sia effettuata successivamente alla verifica dell'effettiva corrispondenza delle stesse – con riferimento sia all'esistenza della transazione, sia all'importo della stessa come indicato in fattura – ai contratti, agli ordini di acquisto o alle conferme d'ordine in essere;
- sia svolto un monitoraggio costante dell'evoluzione della normativa fiscale di riferimento sulle operazioni e transazioni infragruppo;
- sia garantita la tracciabilità, anche attraverso i sistemi informativi aziendali, di tutta la documentazione e della reportistica relativa alla gestione delle operazioni e transazioni infragruppo e definizione e monitoraggio dei prezzi di trasferimento.

**h) Capitalizzazione asset e gestione dei piani di ammortamento (Cessione e dismissione asset)**

- siano stabilite le funzioni aziendali da cui possono pervenire le richieste di iscrizione di un nuovo asset;
- sia definito un set minimo di dati necessari e di evidenze documentali per la richiesta di iscrizione di un nuovo asset;
- sia definito l'iter approvativo per autorizzare l'inserimento, la modifica o la cancellazione di un asset;
- sia verificata e approvata la classificazione di un nuovo asset quale "bene pronto all'uso" (per il quale il processo di ammortamento contabile e fiscale ha inizio a seguito dell'entrata merce) o

"bene che richiede ulteriori lavorazioni" (immobilizzazioni in corso per le quali il processo di ammortamento contabile e fiscale ha inizio in un momento successivo all'entrata merce);

- sia previsto il monitoraggio delle immobilizzazioni in corso al fine di identificare prontamente e correttamente gli asset ultimati per i quali può essere avviato il processo di ammortamento;
- siano effettuati controlli a campione, post registrazione a libro cespiti, sull'adeguata contabilizzazione degli asset nella corretta categoria e controlli sull'identificazione dei costi effettivamente capitalizzabili, nonché verifiche sul corretto passaggio da "immobilizzazioni in corso" a "immobilizzazioni ordinarie";
- sia previsto un monitoraggio degli effetti fiscali (variazioni in aumento e diminuzione per la dichiarazione dei redditi) connessi a disallineamenti tra il valore civilistico e il valore fiscale dei cespiti;
- siano definite le regole per l'approvazione della cessione o dismissione degli asset, con la previsione di un processo approvativo per cui:
  - sia fornita autorizzazione da parte delle funzioni aziendali competenti;
  - sia attuata la gestione contabile e fiscale della registrazione associata alla cessione o dismissione;
- nel caso di dismissione di asset destinato alla distruzione/rottamazione, siano previsti controlli atti a verificare che:
  - la richiesta di autorizzazione contenga un set minimo di informazioni circa le ragioni dello smaltimento, le modalità dello stesso, i soggetti (smaltitori) da coinvolgere e la data di effettuazione;
  - sia data informativa alla GdF e AE territoriali circa lo smaltimento programmato, la lista dei cespiti da distruggere e i relativi valori.

**i) Gestione del capitale sociale, anche in sede di effettuazione di operazioni di finanza straordinaria o di liquidazione, degli utili e delle riserve**

- ove richiesto, la società di revisione e il Collegio Sindacale esprimano motivato parere sull'operazione;
- sia fatto espresso divieto di:
  - restituire conferimenti ai soci o liberarli dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
  - ripartire utili (o acconti su utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve che non possono per legge essere distribuite;
  - acquistare o sottoscrivere azioni della Società o dell'eventuale società controllante fuori dai casi previsti dalla legge;
  - effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
  - procedere a formazione o aumento fittizio del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale;
  - distrarre o ripartire i beni sociali tra i soci, in fase di liquidazione, prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
- la Funzione proponente l'operazione, o competente in base alle procedure aziendali, predisponga idonea documentazione a supporto dell'operazione proposta, nonché una relazione informativa preliminare che illustri i contenuti, l'interesse sottostante e le finalità strategiche dell'operazione;
- ai fini della registrazione contabile dell'operazione, che la Direzione competente verifichi preliminarmente la completezza, l'inerenza e la correttezza della documentazione di supporto dell'operazione.

## 4. Processo “PROCUREMENT, GENERAL SERVICES AND COMPLIANCE”

### 4.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Procurement, General Services and Compliance”<sup>3</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Selezione e qualifica dei fornitori di beni, servizi e consulenze
- Approvvigionamento di beni, di lavori e servizi, incluso l'affidamento di appalti e gestione subappalti
- Approvvigionamento di consulenze ed incarichi di prestazioni professionali
- Gestione dei rapporti con enti certificatori
- Gestione degli accessi fisici ai siti aziendali
- Gestione dei benefit e delle utilities aziendali
- Gestione delle assicurazioni (insurance management).

### 4.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 318 c.p. Corruzione per esercizio della funzione
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio
- art. 319 bis c.p. Circostanze aggravanti
- art. 319 ter c.p. Corruzione in atti giudiziari
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità
- art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p. Pene per il corruttore
- art. 322 c.p. Istigazione alla corruzione
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 346 bis Traffico di influenze illecite

#### **Reati societari (art. 25 ter)**

- art. 2635 c.c. Corruzione tra privati
- art. 2635 bis c.c. Istigazione alla corruzione tra privati

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

#### **Delitti contro la personalità individuale (art. 25 quinquies):**

- art 603 c.p. Intermediazione illecita e sfruttamento del lavoro

#### **Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso

<sup>3</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A

- art. 12, c. 3, 3-bis, 3-ter e 5, del testo unico di cui al D.Lgs. 25/07/1998, n.286 Disposizioni contro le immigrazioni clandestine

**Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art. 25 octies)**

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

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

- art. 270 c.p. Associazioni sovversive
- art. 270 bis c.p. Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
- L. n. 153/2016, art.270 quinques 1 c.p. Finanziamento di condotte con finalità di terrorismo

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

- art. 513 c.p. Turbata libertà dell'industria o del commercio
- art. 515 c.p. Frode nell'esercizio del commercio
- art. 513bis c.p. Illecita concorrenza con minaccia o violenza

**Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)**

- art. 22, c. 12 D. Lgs 25/07/1998, n. 286 Impiego di lavoratori irregolari

**Reati di omicidio colposo e lesioni gravi o gravissime, commessi con violazione delle norme antiinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies)**

- art. 589 Omicidio colposo
- art. 589 c.3 Lesioni personali colpose

**Reati ambientali (art. 25 undecies)**

- art. 256 c.p., c.1 Attività di gestione di rifiuti non autorizzata
- art. 256 c.p., c.3 Discarica non autorizzata
- art. 256 c.p., c.5 Miscelazione di rifiuti
- art. 256c.p., c.4 Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
- art. 2569c.p., c.1 Traffico illecito di rifiuti
- art. 452 bis c.p. Inquinamento ambientale
- art. 452 quinques c.p. Delitti colposi contro l'ambiente
- art. 452 quaterdecies c.p. Attività organizzate per il traffico illecito di rifiuti.

**Reati tributari (art. 25 quinquiesdecies)**

- art 2 D. Lgs 74/2000 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- art. 3 D. Lgs 74/2000 Dichiarazione fraudolenta mediante altri artifici
- art. 4 D. Lgs 74/2000 Dichiarazione infedele
- art. 5 D. Lgs 74/2000 Omessa dichiarazione
- art. 8 D. Lgs 74/2000 Emissione di fatture o altri documenti per operazioni inesistenti
- art. 10 D. Lgs 74/2000 Occultamento o distruzione di documenti contabili
- art. 10 quater D. Lgs 74/2000 Indebita compensazione
- art. 11 D. Lgs 74/2000 Sottrazione fraudolenta al pagamento di imposte

### 4.3. Standard di controllo

#### 4.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

#### 4.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

##### **a) Selezione e qualifica dei fornitori di beni, servizi e consulenze**

- siano identificati i ruoli, compiti e responsabilità dei soggetti aziendali responsabili della gestione dell'albo fornitori e del processo di valutazione e approvazione dei fornitori qualificabili;
- sia garantita la segregazione dei compiti tra chi manifesta la necessità e richiede la qualifica di un nuovo fornitore, chi esegue le attività di verifica e qualifica, raccolta e analisi della documentazione ricevuta dal fornitore e chi approva l'esito della qualifica del fornitore;
- consulenti e collaboratori siano scelti sulla base di precisi requisiti di onorabilità, professionalità e competenza, ed in relazione alla loro reputazione e affidabilità;
- sia previsto l'invio al fornitore di un questionario da compilare per la raccolta di informazioni, con struttura e domande variabili in base al grado di rischio assegnato al fornitore medesimo;
- sia previsto un controllo circa l'eventuale presenza dei fornitori nelle blacklist di riferimento stilate da organizzazioni nazionali ed internazionali / elenco dei paradisi fiscali;
- sia rilevata l'esistenza di eventuali condizioni di incompatibilità o conflitto di interessi, anche con riguardo ai rapporti di parentela o a relazioni di carattere personale o professionale del fornitore con i soggetti coinvolti nell'attività di qualifica dello stesso;
- sia accertato che i fornitori non siano sottoposti a sanzioni a livello internazionale (economic sanctions) che possano precludere il mantenimento dei rapporti di fornitura con Brennercom;
- siano previsti i casi di sospensione o revoca della qualifica dei fornitori;
- siano definiti i criteri, le regole e le condizioni in cui è necessario procedere ad una qualifica urgente del fornitore;
- siano definiti i criteri in base ai quali il subappaltatore viene considerato idoneo al fine del relativo inserimento nell'elenco subappaltatori verificati;
- sia previsto un costante monitoraggio dei requisiti essenziali dei fornitori per il loro mantenimento nell'Albo fornitori qualificati;
- sia garantita tracciabilità dell'iter di qualifica, del contributo delle funzioni competenti al processo e degli esiti delle valutazioni effettuate.

##### **b) Approvvigionamento di lavori e servizi, incluso l'affidamento di appalti e subappalti**

- siano definiti i principi fondamentali di comportamento per tutti gli attori che, a vario titolo, intervengono all'interno del processo di approvvigionamento di beni (es. approccio strategico al mercato, etica e correttezza professionale, rispetto delle normative, economicità ed efficacia, competitività e trasparenza, tutela dell'ambiente e della SSL, ecc.);
- sia garantita segregazione delle funzioni tra chi esegue la valutazione tecnica, chi effettua la valutazione economica e chi è responsabile dell'aggiudicazione della gara / assegnazione della fornitura e chi ne verifica la corretta esecuzione;
- la modalità di approvvigionamento da adottare (es. pubblicazione del bando, fornitore unico, utilizzo di vendor list qualificate) siano formalizzate e autorizzate da adeguato livello gerarchico;
- sia fatto obbligo di produrre richieste di acquisto chiare, univoche e complete e contenenti una

descrizione precisa del bene da acquistare, delle tempistiche di consegna e della stima del relativo valore, il tutto corredato da adeguata e chiara documentazione;

- ogni acquisto sia sempre disciplinato da un contratto o da un ordine scritto, firmato da soggetti dotati di idonei poteri, nel quale siano chiaramente prestabiliti il prezzo del bene o della prestazione o i criteri per determinarlo;
- i contratti stipulati con Fornitori e Partner siano redatti per iscritto in tutte le loro condizioni e termini, con l'indicazione del compenso pattuito e delle condizioni economiche in generale e siano negoziati, verificati e approvati da almeno due soggetti appartenenti a Brennercom;
- le prestazioni risultino congrue, in considerazione delle prassi esistenti sul mercato e/o delle tariffe vigenti;
- nei rapporti con Soggetti Terzi sia garantita la presa visione e la conformità ai principi contenuti nel Codice Etico e nel Modello Organizzativo di Brennercom;
- sia fatto obbligo di procedere con trattative competitive nei confronti di più fornitori, salvo che non ricorrano esplicite condizioni, connesse a ragioni di urgenza e/o unicità o specificità della prestazione, formalmente documentate, che possano consentire il ricorso ad un fornitore diretto (es. single sourcing);
- siano previsti controlli, anche con sopralluoghi presso le sedi dei fornitori, per verificare l'adeguatezza tecnica, organizzativa, professionale nonché il rispetto dei requisiti connessi a specifiche materie quali, a titolo esemplificativo e non esaustivo, quelle di salute e sicurezza e tutela ambientale;
- sia garantita la tracciabilità dell'intero iter di approvvigionamento (es. approvazione richieste di acquisto e di ordine, raccolta e valutazione offerte, ecc.), comprendendo ogni contributo proveniente dalle diverse funzioni che possono intervenire, a vario titolo, all'interno del processo;
- siano definite le modalità di archiviazione (cartacea e digitale) di tutta la documentazione prodotta dal processo di approvvigionamento, atte a garantire la sua perfetta conservazione e l'impossibilità di alterazione o successive modifiche/integrazioni;
- siano previste chiare modalità di controllo atte a regolamentare il monitoraggio in caso di appalto, compresa l'effettuazione di sopralluogo ed altre attività di verifica anche preliminari;
- sia fatto divieto di subappalto, ovvero, nei casi in cui sia consentito, sia fatto obbligo per il fornitore di ottenere la previa autorizzazione da parte di Brennercom (in ogni caso sia vietato il subappalto totale delle attività previste dall'ordine / contratto);
- sia reso obbligatorio, da parte del fornitore, di attestare, sotto la propria responsabilità, il possesso, da parte del subappaltatore, di idonei requisiti di affidabilità legale e reputazionale, economico-finanziaria e tecnico-organizzativa, ferma restando la verifica preventiva del fornitore da parte delle funzioni competenti atte ad accertare l'affidabilità dello stesso anche sotto il profilo etico e di onorabilità nonché economico e patrimoniale;

Con specifico riferimento alla possibilità per i fornitori di sub-appaltare parte delle attività, le procedure aziendali prevedono i seguenti protocolli di controllo:

- obbligo, da parte del fornitore, di attestare sotto la propria responsabilità che:
  - le retribuzioni siano in linea con quanto previsto dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale o locale, o comunque proporzionato rispetto alla quantità e qualità del lavoro prestato;
  - sia sempre rispettata la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
  - lo svolgimento delle attività dei soggetti alle dipendenze o che agiscono per conto della Società avvenga nel rispetto della normativa in materia di sicurezza e igiene nei luoghi di lavoro;

- nel caso in cui siano impiegati lavoratori extracomunitari, questi ultimi siano in possesso di regolare permesso di soggiorno; di sollevare la Società da qualsiasi responsabilità che dovesse derivare dal mancato adempimento di tale obbligo.

**c) Approvvigionamento di consulenze ed incarichi di prestazioni professionali**

- gli incarichi conferiti ai consulenti siano definiti per iscritto in tutte le loro condizioni e termini, con l'indicazione del compenso pattuito;
- i compensi dei consulenti e collaboratori trovino adeguata giustificazione nell'incarico conferito e siano congrui, in considerazione delle prassi esistenti sul mercato e/o delle tariffe vigenti;
- non vi sia identità soggettiva tra chi richiede l'affidamento degli incarichi e chi l'autorizza, salvo nel caso di consulenze richieste dall'Amministratore Delegato; in tali casi, l'Amministratore Delegato relazioni periodicamente al Consiglio di Amministrazione in merito alle consulenze assegnate dallo stesso, previa verifica dell'esistenza della controparte;
- siano definiti i livelli di approvazione per la formulazione delle richieste di consulenza e per la certificazione/validazione del servizio reso;
- sia fatto divieto di riconoscere compensi o effettuare prestazioni in favore di consulenti, partner o fornitori che non trovino adeguata giustificazione in relazione al tipo di controprestazione o incarico da svolgere, al tipo di compenso ricevuto, alle caratteristiche del rapporto di partnership ed alle prassi vigenti in ambito locale;
- nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la Pubblica Amministrazione, siano previsti dei meccanismi di verifica preventiva dell'assenza di contemporanea collaborazione sulla medesima materia con le stesse amministrazioni pubbliche (per esempio mediante auto-certificazione del consulente esterno);
- nei contratti con partner, consulenti e professionisti sia contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dalla presente Parte Generale, compatibilmente con la normativa sulla protezione dei dati personali;
- siano predisposti documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati;
- in assenza di un'attività selettiva tra diversi operatori del settore, sia data un'evidenza formale delle ragioni della deroga ed esecuzione da parte del responsabile di una valutazione sulla congruità del compenso pattuito (rispetto agli standard di mercato);
- nei rapporti con Soggetti Terzi sia garantita la presa visione e la conformità ai principi contenuti nel Codice Etico e nel Modello Organizzativo di Brennercom;
- il consulente si impegni formalmente ad astenersi dall'effettuare pagamenti, regali ovvero offerte o promesse di pagamento, mediante risorse proprie o messe a disposizione dalla Società, a pubblici ufficiali, enti pubblici, partiti politici, a persona fisica o giuridica che possa avere influenza sull'acquisizione del contratto col cliente;
- tutte le fatture ricevute siano a fronte di impegni di spesa formalizzati attraverso un contratto o un ordine di acquisto;
- sia presente un'adeguata e documentabile giustificazione di tutti i compensi e le somme corrisposte ai Fornitori nel rapporto contrattuale in essere con il Fornitore;
- non siano corrisposti compensi in misura non congrua rispetto alle prestazioni rese alla Società o non conformi all'incarico conferito, alle condizioni o prassi esistenti sul mercato o alle tariffe professionali vigenti per la categoria interessata.

Con riferimento alle Attività Sensibili di cui sopra, in relazione ai *“reati di omicidio colposo e lesioni gravi o gravissime commessi in violazione delle norme sulla tutela della Salute e Sicurezza sul Lavoro”*, sono previsti i seguenti protocolli di controllo:

- le attività di acquisto di attrezzature, macchinari ed impianti sono condotte, previa valutazione

dei requisiti di salute e sicurezza delle stesse tenendo conto anche delle considerazioni dei lavoratori attraverso le loro rappresentanze;

- le attrezzature, i macchinari e gli impianti devono essere conformi a quanto previsto dalla normativa vigente (es. marcatura CE, possesso di dichiarazione di conformità rilasciata dall'installatore, ecc.). Se del caso, in ragione dei disposti legislativi applicabili, la loro messa in esercizio sarà subordinata a procedure di esame iniziale o di omologazione;
- preliminarmente all'utilizzo di nuove attrezzature, macchinari o impianti il lavoratore incaricato dovrà essere opportunamente formato e/o addestrato.

Le attività di acquisto sono svolte con lo scopo di:

- definire i criteri e le modalità per la qualificazione e la verifica dei requisiti dei fornitori;
- definire le modalità per la verifica della conformità delle attrezzature, impianti e macchinari da acquistare alle normative vigenti (es. marcatura CE), nonché i criteri e le modalità per la valutazione dei requisiti di accettabilità;
- prevedere, qualora applicabili, le modalità di esecuzione dei controlli in accettazione, degli esami iniziali e delle omologazioni necessarie alla messa in esercizio;

Nel caso di acquisti di servizi, anche di natura intellettuale (es. acquisto di servizi di progettazione da rendersi a favore della società), la società subordina l'attività di affidamento alla verifica preliminare delle competenze dei propri fornitori, anche sulla base della sussistenza di esperienze pregresse ed eventuali requisiti cogenti (es. iscrizione ad albi professionali). La Società attua il controllo del loro operato attraverso le modalità previste dagli accordi definiti. Qualora le attività condotte da detti soggetti possano avere impatti sull'esposizione a rischi per la salute e la sicurezza dei propri lavoratori, la Società attiva preventivamente le misure di controllo definite ai fini della valutazione dei rischi.

Le attività in appalto e le prestazioni d'opera sono disciplinate dall'art. 26 e dal Titolo IV del D.Lgs. 81/2008.

Il soggetto esecutore delle lavorazioni deve possedere idonei requisiti tecnico-professionali, verificati anche attraverso l'iscrizione alla CCIAA. Esso dovrà dimostrare il rispetto degli obblighi assicurativi e previdenziali nei confronti del proprio personale, anche attraverso la presentazione del Documento Unico di Regolarità Contributiva. Se necessario, il soggetto esecutore deve inoltre presentare all'INAIL apposita denuncia per le eventuali variazioni totali o parziali dell'attività già assicurata (in ragione della tipologia di intervento richiesto e sulla base delle informazioni fornite dalla Società).

L'impresa esecutrice, nei casi contemplati dalla legge, al termine degli interventi deve rilasciare la dichiarazione di conformità a regola d'arte.

Con particolare riferimento a fornitori, installatori e manutentori esterni di macchinari, impianti e di qualsiasi tipo di presidio di sicurezza e attrezzature di lavoro da realizzarsi o installare all'interno di pertinenze poste sotto la responsabilità giuridica del datore di lavoro della Società, sono attuati specifici presidi di controllo che prevedono:

- procedure di verifica dei fornitori che tengano conto anche del rispetto da parte degli stessi e dei loro lavoratori delle procedure di sicurezza;
- definizione dell'ambito di intervento e degli impatti dello stesso all'interno di un contratto scritto;
- definizione degli accessi e delle attività esercitate sul sito da parte dei terzi, con valutazione specifica dei rischi interferenti legati alla loro presenza e relativa redazione della prevista documentazione di coordinamento (es. DUVRI, PSC) sottoscritta da tutti i soggetti esterni coinvolti e prontamente adeguata in caso di variazioni nei presupposti dell'intervento;
- clausole contrattuali in merito ad eventuali inadempimenti di lavoratori di terzi presso i siti aziendali relativamente alle tematiche sicurezza, che prevedano l'attivazione di segnalazioni apposite e l'applicazione di penali;

- sistemi di rilevamento presenze di lavoratori terzi presso il sito aziendale e di controllo sulle ore di lavoro effettivamente svolte e sul rispetto dei principi di sicurezza aziendali, come integrati eventualmente dai contratti;
- indicazione ai predetti soggetti di dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione all'attività della Società;
- cooperazione tra committente e appaltatore, o in genere esecutore dell'opera o del servizio, per l'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro e incidenti sull'attività lavorativa oggetto dell'appalto, dell'opera o del servizio. Nel caso in cui il personale dell'appaltatore operi sotto la direzione o il controllo di incaricati della Società, o utilizzando strumenti messi a disposizione da quest'ultima, anche queste fasi dell'attività devono essere ritenute sensibili, così come la verifica della sicurezza e dell'idoneità dei locali se la prestazione di lavoro viene svolta presso la sede della committente;
- formalizzazione e tracciabilità del controllo da parte dei dirigenti e del datore di lavoro del rispetto dei presidi di controllo sin qui elencati.

In relazione ai *“reati ambientali commessi in violazione delle norme sulla tutela dell'ambiente”*, sono previsti i seguenti protocolli di controllo:

- individuazione dei soggetti incaricati e preposti alla gestione del processo di selezione di acquisto di beni e servizi;
- definizione di ruoli, responsabilità e modalità di selezione dei fornitori e subappaltatori;
- qualifica iniziale e riqualifica periodica dei fornitori a rilevanza ambientale e, laddove applicabile, di recuperatori/smaltitori/intermediari/trasportatori di rifiuti, in particolare per la verifica del rispetto di requisiti normativi ad essi applicabili e delle loro prestazioni ambientali, anche attraverso:
  - acquisizione della copia integrale di iscrizioni/comunicazioni/autorizzazioni, di tutta la documentazione idonea a dimostrare il rispetto degli adempimenti di natura amministrativa e di copia di eventuali certificati di conformità dei loro Sistemi di Gestione alle norme internazionali;
  - verifica iniziale e periodica della documentazione ricevuta;
  - eventuale definizione di un elenco/database di recuperatori, smaltitori, intermediari, trasportatori qualificati;
  - tenuta sotto controllo delle scadenze di iscrizioni/comunicazioni/autorizzazioni;
- (nel caso di intermediari) definizione di clausole contrattuali che prevedano che l'intermediario fornisca, oltre ai documenti attestanti la propria abilitazione, anche le iscrizioni/autorizzazioni relative ai trasportatori utilizzati ed agli impianti cui saranno destinati i rifiuti;
- tracciabilità di tutte le attività relative al processo di monitoraggio delle prestazioni dei fornitori;
- tracciabilità di tutte le attività relative al processo di selezione dei fornitori a rilevanza ambientale e, laddove applicabile, dei recuperatori/smaltitori/intermediari/trasportatori di rifiuti in particolare e successivo affidamento dei contratti;
- monitoraggio sull'operatività dei fornitori attraverso sopralluoghi/visite ispettive durante le attività e eventualmente, laddove applicabile, anche presso le loro sedi;
- segnalazione alle Funzioni responsabili e all'OdV di eventuali potenziali scostamenti rispetto a quanto previsto dalle norme ambientali vigenti e dai requisiti specifici stabiliti dalla Società;
- verifica preliminare dei requisiti tecnico-professionali in capo ai fornitori (ad es., laddove previsto, iscrizione albo gestori ambientali per soggetti preposti alla gestione dei rifiuti, accreditamento mediante ACCREDIA per i laboratori di analisi, ecc.).

#### **d) Gestione dei rapporti con enti certificatori nazionali ed internazionali**

- siano formalizzate le motivazioni connesse all'attribuzione del servizio di certificazione nonché

evidenza delle ragioni qualora si proceda ad assegnazione diretta;

- siano identificate le figure aziendali che assumono il ruolo di *focal point* nei rapporti con gli enti certificatori nonché quelle autorizzate a trasmettere la documentazione e i dati richiesti dagli enti certificatori;
- siano definite le modalità di pianificazione annuale e/o pluriennale degli interventi degli audit e delle ispezioni da parte degli enti certificatori;
- sia fatto obbligo, in sede di ispezioni o verifiche da parte dell'ente certificatore, per le funzioni deputate di operare con trasparenza, correttezza e spirito di collaborazione, agevolando l'attività dell'ente e fornendo, in maniera completa e corretta, fornendo le informazioni ed i dati eventualmente richiesti in adempimento dei compiti attribuiti all'ente stesso;
- sia fatto obbligo di assicurare la completezza, veridicità e trasparenza dei dati trasmessi, con riguardo alla trasmissione di documentazione, dati o informazioni all'ente;
- sia garantita tempestività, correttezza e buona fede in tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti dell'ente certificatore, non frapponendo alcun ostacolo all'esercizio delle funzioni da questo intraprese;
- siano definite le modalità di archiviazione, tracciabilità e documentazione dei rapporti intrattenuti con gli enti certificatori.

#### **e) Gestione degli accessi fisici ai siti aziendali**

- siano identificate le responsabilità e le modalità di gestione dei processi di assegnazione, modifica e revoca ai dipendenti dell'accesso ai siti aziendali nei casi di assunzione, cambio mansione, assenza prolungata e cessazione del rapporto di lavoro;
- siano identificate le responsabilità e le modalità di gestione dei processi di valutazione e approvazione di richieste e permessi di ingresso per dipendenti di ditte esterne, sia per la consegna di beni/materiali acquistati, sia per l'esecuzione di attività/servizi che per la consegna e trasporto di prodotti finiti;
- siano definiti i ruoli autorizzativi ed operativi nei suddetti processi di gestione degli accessi fisici, garantendo una corretta segregazione dei compiti;
- sia definito un sistema che garantisca la tracciabilità delle richieste di ingresso e della relativa documentazione a supporto;
- siano svolte verifiche e monitoraggi degli ingressi e delle scadenze dei permessi di ingresso allo stabilimento.

#### **f) Gestione dei benefit e delle utilities aziendali**

- siano definiti i criteri e le modalità per l'utilizzo dei benefit aziendali;
- sia mantenuto un inventario aggiornato dei beni attribuiti agli assegnatari;
- siano definiti i criteri e le modalità per la loro restituzione in caso di dimissioni o licenziamento o comunque di interruzione del rapporto di lavoro con la Società;
- i premi risultino riconosciuti unicamente nell'ambito del budget approvato e previa autorizzazione congiunta della Direzione Risorse Umane e della Direzione di riferimento;
- la Società riconosca ai dipendenti benefits di varia natura in relazione al ruolo ricoperto (es. autovettura, tablet, etc.) e ne definisca l'iter approvativo.

#### **g) Gestione delle assicurazioni**

- sia garantita la segregazione tra chi predispone la documentazione di supporto alla valutazione del rischio, chi la autorizza e chi la invia all'agenzia assicurativa per l'elaborazione della quotazione del premio;
- siano definiti i criteri di valutazione per la selezione di una polizza assicurativa;
- sia garantita segregazione tra chi svolge le attività di selezione delle società di assicurazione e chi autorizza il contratto di assicurazione;
- siano definiti i criteri utilizzati nella selezione del broker/perito;

- siano identificati i soggetti dotati di adeguati poteri autorizzativi per approvare il contratto;
- sia svolta una verifica sulla completezza ed accuratezza dei dati riportati nella fattura rispetto al contenuto del contratto/ordine con broker/periti, nonché rispetto alla prestazione ricevuta;
- siano definite le modalità di gestione delle assicurazioni, inclusa la eventuale gestione dell'invio dei claim e dei rapporti con le agenzie/broker assicurativi.

## 5. Processo “AMBIENTE”

### 5.1. Le attività sensibili rilevanti

In ragione delle attività svolte e dell'esecuzione delle attività di risk assessment, la Società ha individuato le seguenti attività sensibili, periodicamente aggiornate in relazione a nuove ed eventuali esigenze di prevenzione secondo le modalità previste dal Modello, nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati ambientali previsti dall'art. 25-undecies del Decreto e ritenuti ad essa applicabili:

- Gestione della compliance ambientale
- Gestione dei rifiuti

### 5.2. Reati applicabili

Sulla base delle analisi effettuate nell'ambito dell'attività di risk self assessment condotta sui processi identificati in seno alla Società, è stata considerata astrattamente possibile, da parte dei soggetti dipendenti o riconducibili all'organizzazione societaria, la commissione dei seguenti reati ambientali:

- **reati connessi alla gestione dei rifiuti**, previsti dall'art. 256, commi 1 a), b), 3, 4 e 5 del D. Lgs. n. 152/2006;
- **predisposizione o utilizzo di un certificato di analisi rifiuti falso**, previsto dall'art. 258, comma 4, secondo periodo, D. Lgs. n. 152/2006;
- **attività organizzate per il traffico illecito di rifiuti**, reato previsto dall'art. 452-quaterdecies;
- **reati commessi nell'ambito del Registro elettronico nazionale per la tracciabilità dei rifiuti** (di cui al Decreto-legge 14 dicembre 2018, n.135<sup>4</sup>): previsti dall'art. 260-bis, comma 6, 7 e 8, del D. Lgs. n. 152/2006;
- **Reati connessi alla tutela dell'ozono**, previsto dall'art. 3, comma 6, L. 28 dicembre 1993, n. 549;
- **circostanze aggravanti**, previste dal Art. 452-octies c.p.

### 5.3. Standard di controllo

#### 5.3.1. Standard di controllo generali

Per presidiare le attività sensibili individuate, Brennercom S.p.A. ha reputato strategico dotarsi di procedure per la gestione di aspetti ambientali principali, ispirate al Sistema di Gestione Ambientale conforme alla norma UNI ISO 14001:2015. Tali procedure integrano il presente Modello e sono volte a declinare operativamente, documentare e comunicare a tutti gli interessati e a tutti i livelli della Società i ruoli, le responsabilità e le autorità assegnate alle diverse strutture organizzative in ambito ambientale volte a:

- stabilire un modello di organizzazione per la gestione dell'ambiente nel rispetto della normativa vigente;
- stabilire una chiara e strutturata organizzazione aziendale nella gestione dell'ambiente e definire chiare linee di comunicazione;
- definire obiettivi e traguardi in accordo con gli obiettivi definiti nella Politica Ambientale;
- promuovere e diffondere la cultura in materia ambientale attraverso attività di informazione e

<sup>4</sup> Decreto-legge 14 Dicembre 2018, n.135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, convertito con Legge n. 12/2019, ha soppresso il sistema SISTRI; pertanto, allo stato, non risulta possibile commettere il presente reato, pur non essendo stata formalmente abrogata la relativa fattispecie di criminosa. In particolare, il Decreto introduce una nuova regolamentazione in merito alla tracciabilità dei rifiuti, in attesa dei decreti attuativi, statuisce che:

Art 3. A decorrere dalla data di entrata in vigore della legge di conversione del presente decreto è istituito il Registro elettronico nazionale per la tracciabilità dei rifiuti, gestito direttamente dal Ministero dell'ambiente e della tutela del territorio e del mare, [omissis].

Art. 3-ter. Dal 1° gennaio 2019 e fino al termine di piena operatività del Registro elettronico nazionale come individuato con il decreto di cui al comma 3-bis, la tracciabilità dei rifiuti è garantita effettuando gli adempimenti di cui agli articoli 188, 189, 190 e 193 del decreto legislativo 3 aprile 2006, n. 152, [omissis].

formazione riguardo i propri lavoratori, al fine di diffondere a tutti i livelli aziendali i principi descritti nella politica ambientale;

- garantire la gestione dei processi, adottando azioni di prevenzione e di protezione dell'ambiente;
- garantire la gestione delle attività di controllo, per la prevenzione e per la risposta rapida in caso di incidenti;
- garantire il monitoraggio ed il miglioramento continuo delle prestazioni ambientali.
- Per tutti gli ambiti e le attività sensibili identificate, in considerazione dell'impatto che potrebbero avere sull'ambiente, il loro corretto svolgimento è assicurato attraverso l'adozione di specifici strumenti organizzativi documentati che prevedono:
  - l'identificazione di tutti gli aspetti ambientali interessati;
  - l'identificazione di tutte le disposizioni normative applicabili all'organizzazione e dei relativi adempimenti;
  - la condivisione delle disposizioni normative con i soggetti responsabili di attuare quanto previsto dalle stesse;
  - la programmazione delle misure tecnico-organizzative e finanziarie necessarie all'adempimento delle prescrizioni;
  - il monitoraggio periodico della conformità alla normativa applicabile;
  - aggiornamento legislativo periodico;
  - la comunicazione interna ed esterna in materia ambientale;
  - la tracciabilità e disponibilità della relativa documentazione.

### 5.3.2. Standard di controllo specifici

I Destinatari della presente Parte Speciale, al fine di prevenire la commissione dei reati ambientali nello svolgimento delle attività sensibili, sono tenuti, oltre che al rispetto dei sopra descritti Protocolli, altresì al rispetto dei Protocolli specifici di controllo di seguito riportati.

Nella presente sezione sono rappresentati i controlli specifici relativi alle sole attività sensibili afferenti al processo "Ambiente". Con riferimento alle altre attività sensibili che possono avere un impatto sui reati ambientali si fa rimando ai controlli specifici relativi ai rispettivi processi.

Tale ambito, con riferimento ai reati ambientali, richiamati dall'art. 25-undecies del Decreto, risulta sensibile per le seguenti attività:

- Gestione della compliance ambientale.
- Gestione dei rifiuti.

Con riferimento all'attività **Gestione della compliance ambientale**, le procedure e le prassi vigenti devono garantire il rispetto di protocolli specifici di controllo.

In considerazione dell'impatto che la menzionata attività potrebbe avere sulla gestione dei rifiuti e sulla protezione dell'ozono, il corretto svolgimento della stessa è assicurato attraverso l'adozione di specifici strumenti organizzativi documentati che prevedono:

- l'identificazione e la valutazione degli impatti ambientali legati alle attività aziendali;
- il monitoraggio e l'aggiornamento della normativa applicabile e la sua conseguente comunicazione e informazione alle funzioni interessate;
- la definizione, l'implementazione, la manutenzione e l'aggiornamento dei sistemi procedurali definiti a presidio degli aspetti ambientali e dei processi significativi identificati;
- l'adozione di apposite procedure che regolamentino le attività, i ruoli e le responsabilità delle operazioni relative alla gestione dei rifiuti;
- la gestione delle attività relative al censimento e l'aggiornamento di piani di utilizzo, dismissione e autorizzazioni necessarie delle apparecchiature che contengono sostanze lesive dell'ozono;
- il monitoraggio delle prestazioni ambientali sulla base dell'eventuale definizione di un set di indicatori afferenti alle diverse matrici ambientali identificate;

- la definizione di opportuni strumenti di reporting anche in aderenza alle prescrizioni autorizzative e di legge;
- la formalizzazione di un piano di audit e la sua attuazione in considerazione di tutti gli impatti ambientali descritti;
- la comunicazione delle risultanze degli audit condotti ai soggetti preposti, affinché siano oggetto di valutazione di opportune misure correttive, in considerazione di tutti gli impatti ambientali descritti;

Con riferimento all'attività Gestione dei rifiuti comprendente le attività di raccolta, caratterizzazione, classificazione, deposito, recupero e smaltimento, le procedure e le prassi vigenti devono garantire il rispetto di protocolli specifici di controllo.

In considerazione dell'impatto che la menzionata attività potrebbe avere sulla gestione dei rifiuti, il corretto svolgimento della stessa è assicurato attraverso l'adozione di specifici strumenti organizzativi documentati per la definizione di ruoli e responsabilità che prevedono le modalità gestionali ed operative per:

- garantire la corretta caratterizzazione e classificazione dei rifiuti;
- prevedere la differenziazione dei rifiuti al fine di prevenire ogni illecita miscelazione;
- garantire la corretta gestione dei depositi temporanei dei rifiuti sulla base della tipologia e dei quantitativi di rifiuti prodotti;
- verificare la congruità del rifiuto prodotto con la qualificazione CER dello stesso, anche qualora il servizio sia eseguito da laboratori terzi;
- verificare il possesso, nel caso di trasporto condotto in proprio, dei prescritti requisiti richiesti dalla normativa vigente;
- verificare, nel caso di trasporto eseguito da soggetti terzi, del rispetto delle necessarie prescrizioni autorizzative;
- verificare la corretta gestione degli adempimenti necessari al trasporto dei rifiuti dal momento della consegna al trasportatore fino al conferimento finale allo smaltitore (gestione dei formulari e dei registri carico/scarico);
- verificare la corretta tenuta della documentazione relativa allo smaltimento (ad es. registri, formulari, documentazione analitica di accompagnamento, ecc.), nonché la congruità dei quantitativi inviati a smaltimento con quelli rappresentati nella documentazione resa;
- verificare la corretta gestione dei FIR (Formulari di Identificazione dei Rifiuti), anche avvalendosi di database e di riepiloghi per codice CER, propedeutico alla corretta compilazione del MUD annuale (Modello Unico di Dichiarazione ambientale);
- comunicare eventuali superamenti delle concentrazioni di inquinanti e/o di eventuali sversamenti al responsabile della compliance ambientale;
- verificare la disponibilità e la corretta archiviazione della documentazione relativa alla gestione dei rifiuti.

## 6. Processo “SALUTE E SICUREZZA”

Nella presente sezione sono esplicitati linee e principi di comportamento che tutti i destinatari del Modello

dovranno seguire al fine di prevenire e contenere, nell’ambito delle specifiche attività svolte da Brennercom S.p.A. e considerate “a rischio”, la commissione dei reati previsti dall’art. 25-septies del Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

In particolare, la presente Parte Speciale concerne i comportamenti che devono essere tenuti dai soggetti - Amministratori e personale in posizione apicale operante in nome e per conto della Società, dirigenti, manager e dipendenti di Brennercom S.p.A., anche per il tramite di fornitori, consulenti e lavoratori autonomi e parasubordinati, che svolgono la propria prestazione a favore della Società, indipendentemente dalla qualificazione giuridica del loro rapporto con la Società - che sono coinvolti nei processi e nelle attività sensibili ed operano pertanto nelle aree a rischio reato (qui di seguito i “destinatari”).

Nello specifico, la presente Parte Speciale del Modello fornisce una rappresentazione degli strumenti organizzativi, gestionali e di controllo stabiliti e attuati dalla Società al fine di:

- promuovere il raggiungimento degli obiettivi di tutela della salute e della sicurezza dei lavoratori;
- fornire indicazioni circa le misure comportamentali che tutti i soggetti coinvolti nei processi aziendali che possono influenzare le prestazioni di Salute e Sicurezza sul Lavoro (“attività sensibili”) devono porre in essere al fine di contenere i rischi di commissione dei reati richiamati dall’art. 25-septies del Decreto e ai fini della corretta applicazione del Modello;
- fornire all’Organismo di Vigilanza ed alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

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

### 6.1. Le attività sensibili rilevanti

#### 6.1.1. Generalità

Per definire preliminarmente le attività sensibili, ai sensi del D.Lgs. 231/2001, occorre considerare le attività entro le quali si possono verificare gli infortuni e quelle nell’ambito delle quali può essere commesso, da parte di membri dell’organizzazione, un reato per violazione colposa della normativa e delle misure di prevenzione esistenti a tutela della salute, dell’igiene e della sicurezza sui luoghi di lavoro. A tale fine, la Società ha reputato strategico trarre spunto da due importanti strumenti di controllo e di gestione:

- la valutazione dei rischi prevista dalla vigente normativa in materia di tutela della salute e della sicurezza;
- la Norma ISO 45001:2018.

Attraverso la valutazione dei rischi si sono individuate le condizioni ove, ragionevolmente, è possibile si manifestino degli eventi lesivi.

L’adozione efficace di un Sistema di Gestione Salute e Sicurezza sul Lavoro realizzato in conformità con la Norma ISO 45001:2018 è riconosciuta dal legislatore, nelle parti in cui può trovare applicabilità, come una modalità atta a cogliere gli obiettivi di corretta gestione della salute e sicurezza sul lavoro; pertanto, così come previsto dall’art. 30 del D.Lgs. 81/2008, un modello organizzativo realizzato secondo tale norma risulterebbe presumibilmente conforme ai fini esimenti previsti dal D.Lgs. 231/2001.

La Società ha perciò tratto ispirazione dalla Norma ISO 45001:2018, con l’obiettivo di mettere sotto controllo le proprie attività, controllare che le stesse siano, dal punto di vista della tutela della

sicurezza e salute, conformi a quanto previsto da leggi, norme e regolamenti locali, nazionali ed europei e organizzare nel complesso l'intera struttura.

Le attività individuate con riferimento ai reati richiamati dall'art. 25-septies del D. Lgs. n. 231/2001 sono pertanto classificate come segue:

- **attività a rischio di infortunio e malattia professionale**, individuate nella documentazione predisposta dal Datore di Lavoro in accordo con le pertinenti prescrizioni normative al fine di riportare gli esiti del processo di valutazione dei rischi, in base alle quali possono potenzialmente verificarsi gli infortuni e le malattie professionali;
- **attività a rischio di reato**, intese come le attività che possono potenzialmente originare i reati di cui all'art. 25-septies del Decreto e che, in caso di inefficace attuazione delle misure di controllo dei rischi, potrebbero integrare una responsabilità colposa dell'ente.

#### 6.1.2. Attività a rischio di reato

Fatta salva la trattazione delle attività a rischio di infortunio e malattia professionale desunte dalla documentazione definita dal Datore di Lavoro ai fini della valutazione dei rischi, a cui il presente elaborato rimanda, la Società ha posto in essere un'attività di risk assessment finalizzata all'individuazione, nell'ambito dei processi aziendali, delle attività a rischio di reato. Coerentemente con quanto previsto dall'art. 30 del D. Lgs. n. 81/2008 e considerando i requisiti previsti dalle Norme BS OHSAS 18001:2007 e UNI ISO 45001:2018, l'analisi dei processi aziendali ha consentito di individuare le attività che possono potenzialmente originare i reati di cui all'art. 25-septies del Decreto, come descritto di seguito:

- Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali.
- Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL.
- Gestione della documentazione interna (articolazione del sistema normativo) relativa agli aspetti SSL.
- Definizione delle misure per il controllo operativo e la gestione del cambiamento.
- Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso.
- Attività di sorveglianza sanitaria.
- Comunicazione, partecipazione e consultazione: gestione delle riunioni periodiche di sicurezza, consultazione dei lavoratori e delle loro rappresentanze.
- Gestione di incidenti non conformità e azioni correttive.

#### 6.2. Reati applicabili

Sulla base delle analisi effettuate nell'ambito dell'attività di risk assessment condotta sui processi identificati in seno alla Società, è stata considerata astrattamente possibile, da parte dei destinatari, la commissione dei seguenti reati previsti dal codice penale e commessi in violazione della normativa antinfortunistica e sulla tutela della salute e della sicurezza nei luoghi di lavoro, per i quali, il D. Lgs n. 231/2001 integra, all'art. 25-septies, l'ipotesi di responsabilità amministrativa dell'ente:

- omicidio colposo, previsto dall'art. 589 c.p.
- lesioni personali colpose gravi o gravissime previsto dall'art. 590, comma 3 c.p.

##### 6.2.1. Modalità di commissione dei reati

L'evento delittuoso, sia esso rappresentato dalla lesione grave o gravissima o dalla morte, può essere perpetrato tramite un comportamento attivo (l'agente pone in essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante un atteggiamento omissivo (l'agente non interviene al fine di impedire il verificarsi dell'evento dannoso che ha il dovere giuridico di impedire). Si ravviserà una condotta attiva nel caso in cui il soggetto arrechi materialmente un danno ad altri,

mentre la condotta omissiva sarà ravvisabile, ad esempio, nel soggetto che, non ottemperando agli obblighi di vigilanza e controllo (ad es. Datore di Lavoro, dirigente, preposto), non intervenga per impedire il verificarsi dell'evento.

Sotto il profilo soggettivo, i reati rilevanti ai fini della presente Parte Speciale dovranno essere realizzati con colpa: tale profilo di imputazione soggettiva può essere generico (violazione di regole di condotta cristallizzate nel tessuto sociale in base a norme di esperienza imperniate sui parametri della diligenza, prudenza e perizia) o specifico (violazione di regole di condotta previste in leggi, regolamenti, ordini o discipline). In ciò vi è una profonda differenza rispetto ai criteri di imputazione soggettiva previsti per altre figure delittuose richiamate dal D. Lgs. n. 231/2001, in gran parte punite a titolo di dolo: in tali casi è necessario, infatti, che il soggetto agisca rappresentandosi e volendo la realizzazione dell'evento - conseguenza della propria condotta delittuosa, non essendo sufficiente un comportamento imprudente o imperito in relazione alla stessa.

Ai fini della possibile contestazione dei reati di cui agli artt. 589 e 590, comma 3 c.p., la condotta lesiva dell'agente deve essere necessariamente aggravata, ossia conseguire alla violazione di norme antinfortunistiche concernenti la tutela dell'igiene e della salute sul lavoro.

Ai fini dell'implementazione del Modello è necessario comunque considerare che:

- il rispetto degli standard minimi di sicurezza previsti dalla normativa specifica di settore non esaurisce l'obbligo di diligenza complessivamente richiesto;
- l'adozione di standard di sicurezza deve essere orientata a garantire la tutela dell'integrità fisica e della personalità morale dei prestatori di lavoro al fine di ridurre e, se possibile, eliminare ogni rischio di infortunio e malattia;
- non sono escluse le responsabilità in capo alla persona fisica o all'ente nel caso in cui il comportamento dello stesso lavoratore infortunato abbia dato occasione all'evento, qualora quest'ultimo sia da ricondurre, comunque, alla mancanza o insufficienza di cautele che, se adottate, avrebbero neutralizzato il rischio sotteso a un siffatto comportamento. La responsabilità è esclusa solo in presenza di comportamenti del lavoratore che presentino il carattere dell'eccezionalità, dell'abnormità o dell'esorbitanza rispetto al procedimento lavorativo, alle direttive organizzative ricevute e alla comune prudenza.

Per quanto concerne i soggetti attivi, possono commettere queste tipologie di reato coloro che, in ragione della loro mansione, svolgono attività sensibili in materia; ad esempio:

- i Datori di Lavoro, quali principali attori nell'ambito della prevenzione e protezione (il Datore di Lavoro è, in prima istanza, il garante "dell'integrità fisica e della personalità morale dei prestatori di lavoro");
- i dirigenti ed i preposti, ai quali possono competere, tra gli altri, compiti organizzativi o di supervisione delle attività;
- i medici competenti ai quali è attribuito, nei limiti e sulla base delle disposizioni di legge, il presidio della salute del lavoratore;
- i lavoratori che, attraverso le proprie azioni e/o omissioni, possono pregiudicare la propria e/o l'altrui salute e sicurezza;
- i progettisti, ai quali compete il rispetto dei principi di prevenzione in materia di Salute e Sicurezza sul Lavoro, sin dal momento dell'individuazione delle soluzioni progettuali e tecniche;
- i fabbricanti, gli installatori ed i manutentori che, nell'ambito delle rispettive competenze, devono assicurare la rispondenza alle pertinenti disposizioni legislative e regolamentari applicabili, comprese le "norme di prodotto";
- i committenti o i soggetti da loro individuati, ai quali competono, secondo le modalità definite dalla normativa, la gestione ed il controllo dei lavori affidati in appalto.

### 6.3. Standard di controllo

#### 6.3.1. Standard di controllo generali

La presente sezione è volta, in ossequio all'art. 30 del d.lgs. 9 aprile 2008, n. 81, al fine di garantire al Modello l'efficacia esimente della responsabilità amministrativa prevista dal Decreto, alla puntuale individuazione ed alla regolamentazione degli obblighi:

- a) di rispetto degli standard tecnico-strutturali di legge relativi alle attrezzature, agli impianti, ai luoghi di lavoro;
- b) di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) inerenti alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) concernenti le attività di sorveglianza sanitaria;
- e) attinenti alle attività di informazione e formazione dei lavoratori;
- f) riguardanti le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) di acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) di verifica periodica dell'applicazione e dell'efficacia delle procedure adottate.

La presente Parte Speciale prevede altresì l'espresso obbligo, a carico di tutti i destinatari del modello - in via diretta per gli esponenti aziendali, tramite apposite clausole contrattuali per i Partner o dei Collaboratori Esterni - di:

- astenersi dal porre in essere comportamenti tali da integrare le fattispecie di Reato sopra considerate (art. 25-octies del Decreto);
- astenersi dal porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di Reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Nell'ambito dei suddetti comportamenti è fatto inoltre obbligo di:

- adempiere alle disposizioni di legge e regolamenti vigenti;
- operare nel rispetto dei poteri di rappresentanza e di firma sociale, delle deleghe e procure loro conferite;
- rispettare le prescrizioni previste dalle procedure di riferimento;
- ottemperare alle istruzioni impartite dai superiori gerarchici.

Nell'ambito del sistema organizzativo, Brennercom S.p.A. ha definito una struttura che prevede, tra l'altro, i compiti, le responsabilità e gli eventuali poteri in materia di Salute e Sicurezza sul Lavoro.

In accordo con i protocolli specifici di controllo descritti nel seguito, sono state individuate le figure di riferimento previste dalla normativa applicabile, quali:

- Datore di Lavoro;
- Dirigenti e Preposti;
- Responsabile del Servizio di Prevenzione e Protezione;
- Medico Competente.

I lavoratori hanno provveduto a individuare il proprio Rappresentante dei Lavoratori per la Sicurezza.

Le strutture organizzative e le figure di riferimento sono rappresentate attraverso appositi strumenti quali, ad esempio, gli Organigrammi, le Comunicazioni Organizzative e le *Job Description*.

#### 6.3.2. Standard di controllo specifici

Il presente Modello è adottato e attuato al fine di garantire l'adempimento di tutti gli obblighi giuridici volti a prevenire il rischio di commissione dei reati di cui al Decreto Legislativo 81/2008.

Nella presente sezione sono rappresentati i controlli specifici relativi alle sole attività sensibili afferenti al processo "SALUTE E SICUREZZA". Con riferimento alle altre attività sensibili che possono avere un impatto sui reati salute e sicurezza si fa rimando ai controlli specifici relativi ai rispettivi processi.

Tale ambito, con riferimento ai reati di omicidio colposo e lesioni gravi o gravissime commesse in violazione delle norme sulla tutela della Salute e Sicurezza sul Lavoro, richiamati dall'art. 25-septies del Decreto, risulta sensibile per le seguenti attività:

- Individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali.
- Identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la SSL.
- Gestione della documentazione interna (articolazione del sistema normativo) relativa agli aspetti salute e sicurezza sul luogo di lavoro.
- Definizione delle misure per il controllo operativo e la gestione del cambiamento.
- Gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso.
- Attività di sorveglianza sanitaria.
- Comunicazione, partecipazione e consultazione: gestione delle riunioni periodiche di sicurezza, consultazione dei lavoratori e delle loro rappresentanze.
- Gestione di incidenti non conformità e azioni correttive.

Con riferimento all'attività di **individuazione delle disposizioni normative applicabili, a cui uniformarsi per il rispetto degli standard tecnico-strutturali, la conformità alle disposizioni normative applicabili** è assicurata attraverso l'adozione di specifici strumenti organizzativi documentati, i quali prevedono la definizione di ruoli, responsabilità e modalità operative per:

- l'identificazione di tutte le disposizioni normative applicabili all'organizzazione e dei relativi adempimenti;
- l'individuazione dei responsabili dell'attuazione, e messa a loro disposizione, delle pertinenti disposizioni normative;
- il monitoraggio periodico della conformità alla normativa applicabile;
- l'aggiornamento legislativo periodico.

La Direzione Affari Legali e Societari è tenuta a coinvolgere costantemente il Responsabile del Servizio di Prevenzione e Protezione in relazione a qualsivoglia processo (assunzione di una nuova risorsa, modifiche strutturali nei luoghi di lavoro, nuove tipologie di attività, etc.) che possa incidere sulla sicurezza e salute dei lavoratori.

Con riferimento all'attività di **identificazione e valutazione dei rischi, predisposizione delle misure di prevenzione e protezione conseguenti per eliminare i pericoli e ridurre i rischi per la Salute e Sicurezza sul Luogo di Lavoro**, l'operazione di individuazione e di rilevazione dei rischi è effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza, previa definizione del perimetro normativo di riferimento e in accordo con le pertinenti prescrizioni di settore (a titolo esemplificativo e non esaustivo: artt. 17 e 96, D. Lgs. n. 81/2008).

La responsabilità finale è attribuita, senza ipotesi di delegabilità, a ciascun Datore di Lavoro che si avvale del supporto di altri soggetti quali, tra gli altri, il Responsabile del Servizio di Prevenzione e Protezione ed il Medico Competente, nonché di ulteriori soggetti, quali ad esempio il personale incaricato di attività specialistiche, previa consultazione delle rappresentanze dei lavoratori per la sicurezza.

Tutti i dati e le informazioni funzionali alla valutazione dei rischi e, conseguentemente, all'individuazione delle misure di tutela (ad esempio la documentazione tecnica, le misure

strumentali, gli esiti dei sondaggi interni, ecc.) devono essere chiari, completi e devono rappresentare in modo veritiero lo stato e la situazione reale della Società.

Il processo di valutazione dei rischi e di definizione dei relativi documenti, nonché il loro aggiornamento, è condotto in accordo con le pertinenti prescrizioni normative ed è descritto in apposita documentazione organizzativa societaria. Detta documentazione deve prevedere l'espletamento delle seguenti attività:

- identificazione degli elementi di pericolo;
- definizione ed applicazione dei criteri per la valutazione del rischio;
- individuazione delle figure professionali oggetto di valutazione dei rischi e aggiornamento dei funzionigrammi;
- identificazione delle misure di prevenzione e protezione dai rischi;
- validazione e applicazione delle misure di prevenzione e protezione dai rischi;
- formalizzazione, approvazione ed emissione della prescritta documentazione di valutazione dei rischi;
- attuazione del piano di azione.

Il processo di Valutazione dei Rischi deve essere condotto considerando:

- le attività routinarie e non routinarie;
- le attività di tutte le persone che hanno accesso al posto di lavoro (compresi i terzi);
- il comportamento umano;
- i pericoli provenienti dall'esterno;
- i pericoli legati alle operazioni o creati nell'ambiente circostante;
- le infrastrutture, attrezzature e materiali presenti presso il luogo di lavoro;
- gli eventuali obblighi giuridici applicabili in materia di valutazione dei rischi e di attuazione delle necessarie misure di controllo;
- la progettazione di ambienti di lavoro, macchinari ed impianti;
- le procedure operative e di lavoro.

Il Datore di Lavoro, attraverso le proprie strutture organizzative, assicura che il personale della Società svolga attività solo se condotte nell'ambito di processi che sono stati oggetto di valutazione dei rischi.

Con riferimento all'attività di **Gestione della documentazione interna (articolazione del sistema normativo) relativa agli aspetti di Salute e Sicurezza sul Luogo di Lavoro**, la Società, a seguito dell'analisi dei processi aziendali e coerentemente con i risultati della valutazione dei rischi ha definito un sistema di informazioni documentate (ad esempio procedure, registrazioni, modulistica, documentazione progettuale, etc.) per controllare che le attività siano svolte nel rispetto della normativa in materia di Salute e Sicurezza sul Lavoro.

Sono stabiliti opportuni criteri affinché, ove necessario e applicabile, siano definiti ruoli, responsabilità e modalità operative per:

- l'identificazione e l'approvazione delle informazioni documentate per assicurare la loro adeguatezza, prima della emissione;
- la revisione e l'aggiornamento delle informazioni documentate, assicurando la tracciabilità delle modifiche apportate;
- la conservazione delle informazioni documentate in maniera opportuna, assicurandone la reperibilità, l'integrità e la completezza.

Con riferimento all'attività di **definizione delle misure per il controllo operativo e la gestione del cambiamento**, la Società assicura il controllo e la verifica periodica delle condizioni di lavoro in modo da evitare e prevenire rischi per la salute e la sicurezza.

Il controllo operativo è finalizzato alla prevenzione dei reati, in totale analogia a quanto emerso nell'ambito della conduzione della valutazione dei rischi in ambito Salute e Sicurezza sul Lavoro e del suo aggiornamento.

In ragione della complessità delle attività, sono previste specifiche istruzioni di lavoro o procedure operative che, unitamente alla documentazione riguardante le modalità d'uso di macchinari ed attrezzature, ecc., disciplinano le attività.

La Società prevede la definizione di modalità di lavoro, condotte in conformità alle prescrizioni normative vigenti:

- definendo nelle procedure i criteri operativi sulla base dei quali devono operare i diversi soggetti;
- stabilendo e aggiornando la documentazione che concerne i rischi Salute e Sicurezza sul Lavoro significativi relativi ai beni e ai servizi utilizzati dall'organizzazione e comunicando ai fornitori e agli appaltatori le procedure e i requisiti di loro pertinenza.

Tutte le attrezzature, i macchinari e gli impianti che possono avere impatti significativi in materia di Salute e Sicurezza sono assoggettati a protocolli di manutenzione programmata con tempistiche e modalità anche definite dai fabbricanti. Gli eventuali interventi specialistici sono condotti da soggetti in possesso dei requisiti di legge che devono produrre le necessarie documentazioni.

Le attività di manutenzione su dispositivi di sicurezza sono oggetto di registrazione.

In presenza di attrezzature ed impianti per i quali siano previsti, dalla legislazione vigente, periodici interventi di verifica per la cui esecuzione siano individuati specifici enti esterni (es. ASL, Organismi Notificati, Organismi di Ispezione, ecc.), si provvede a stipulare con l'ente preposto uno specifico contratto di verifica; qualora l'ente preposto non eroghi il servizio con le tempistiche previste dalla normativa si procederà come segue:

- in caso di esistenza di ulteriori soggetti in possesso delle abilitazioni/autorizzazioni all'esecuzione degli interventi di verifica, si provvederà ad affidare loro l'incarico;
- in caso di assenza di soggetti alternativi si provvederà, a titolo di auto diagnosi, attraverso strutture tecniche esistenti sul mercato (es. imprese di manutenzione, società di ingegneria, ecc.).

Le attività di manutenzione sono condotte in maniera da:

- definire le modalità, le tempistiche e le responsabilità per la programmazione e lo svolgimento delle manutenzioni e delle verifiche periodiche, ove previste, di attrezzature, impianti, macchinari (individuati puntualmente in appositi protocolli/schede), immobili ed il controllo periodico della loro efficienza;
- definire le modalità di registrazione delle manutenzioni effettuate e le relative responsabilità;
- definire le modalità di segnalazione delle anomalie, individuati i mezzi più idonei per comunicare tali modalità, individuate le funzioni tenute ad attivare il relativo processo di manutenzione (manutenzioni non programmate);
- definire i protocolli di manutenzione programmata con tempistiche e modalità, anche definite dai fabbricanti, per tutte le attrezzature, i macchinari e gli impianti che possono avere impatti significativi in materia di salute e sicurezza. Al proposito sono definite le modalità di registrazione di tutte le manutenzioni su dispositivi di sicurezza;
- in caso di esistenza di ulteriori soggetti in possesso delle abilitazioni/autorizzazioni all'esecuzione degli interventi di verifica, provvedere ad affidare loro l'incarico;
- in caso di assenza di soggetti alternativi provvedere, a titolo di auto diagnosi, attraverso strutture tecniche esistenti sul mercato (es. imprese di manutenzione, società di ingegneria, ecc.);
- prevedere che sia garantita la tracciabilità degli interventi di manutenzione effettuati.

Con riferimento all'attività **gestione delle emergenze, delle attività di lotta agli incendi e di primo soccorso**, la Società ha predisposto specifici piani che prevedono la definizione di ruoli, responsabilità e modalità operative per:

- l'identificazione delle situazioni che possano causare una potenziale emergenza;
- la definizione delle modalità per rispondere alle condizioni di emergenza e prevenire o mitigare le relative conseguenze negative in tema di Salute e Sicurezza sul Lavoro;
- la pianificazione della verifica dell'efficacia dei piani di gestione delle emergenze;
- l'aggiornamento delle procedure di emergenza in caso di incidenti o di esiti negativi delle simulazioni periodiche;
- la formalizzazione e tracciabilità delle attività di verifica sul rispetto dei presidi di controllo individuati.

Sono inoltre individuati gli addetti agli interventi di emergenza, in numero sufficiente e preventivamente formati ed aggiornati secondo i requisiti di legge.

Sono disponibili e mantenuti in efficienza idonei sistemi per la lotta agli incendi, scelti per tipologia e numero in ragione della specifica valutazione del rischio di incendio ovvero delle indicazioni fornite dall'autorità competente.

Sulla base della rischiosità del sito, sono inoltre presenti strutture organizzative e dotazioni, più o meno complesse, poste a presidio degli interventi di primo soccorso.

L'efficienza dei piani è garantita attraverso la periodica attività di prova, finalizzata ad assicurare la piena conoscenza, da parte del personale, delle corrette misure comportamentali e l'adozione di idonei strumenti di registrazione atti a dare evidenza degli esiti di dette prove e delle attività di verifica e di manutenzione dei presidi predisposti.

Con riferimento all'attività di **sorveglianza sanitaria**, preliminarmente all'attribuzione di una qualsiasi mansione al lavoratore, la Società ne verifica i requisiti sia per quanto riguarda gli aspetti tecnici, sia per quanto riguarda gli aspetti sanitari, se riscontrati in sede di valutazione del rischio.

La verifica circa l'idoneità è attuata dal Medico Competente della Società che, in ragione delle indicazioni fornite dai Datori di Lavoro e sulla base della propria conoscenza dei luoghi di lavoro e delle lavorazioni, verifica preventivamente l'idoneità sanitaria del lavoratore. Il Medico Competente rilascia giudizi sull'idoneità, totale o parziale, ovvero sull'inidoneità del lavoratore allo svolgimento della mansione alla quale è preposto. In ragione della tipologia di lavorazione richiesta e sulla base degli esiti della visita preliminare, il Medico Competente definisce un protocollo di sorveglianza sanitaria a cui sottopone il lavoratore.

Con riferimento all'attività **comunicazione, partecipazione e consultazione: gestione delle riunioni periodiche di sicurezza, consultazione dei lavoratori e delle loro rappresentanze** sono stabiliti specifici strumenti organizzativi e di monitoraggio e controllo. In generale, e a titolo esemplificativo, la Società definisce:

- i ruoli, le responsabilità e le modalità operative di gestione della comunicazione con i lavoratori;
- le modalità di registrazione e monitoraggio delle riunioni periodiche;
- le modalità di partecipazione del personale alle tematiche in ambito Salute e Sicurezza sul Lavoro;
- la comunicazione e il coinvolgimento dei rappresentanti dei lavoratori per la valutazione dei rischi.

Con riferimento all'attività **gestione di incidenti, non conformità e azioni correttive**, sono stabiliti opportuni strumenti che regolamentano ruoli, responsabilità e modalità operative per:

- la rilevazione, tracciabilità/registrazione e investigazione interna degli infortuni, incidenti occorsi e "near miss";
- la regolamentazione delle attività di comunicazione da parte dei responsabili operativi alle pertinenti funzioni sugli infortuni/incidenti occorsi;

- il monitoraggio degli infortuni occorsi (tenendo conto di eventuali controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro) al fine di identificare le aree a maggior rischio infortuni;
- la formalizzazione e tracciabilità delle attività di verifica sul rispetto dei presidi di controllo individuati.

## 7. Processo “RISORSE UMANE E ORGANIZZAZIONE”

### 7.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Risorse Umane e Organizzazione”<sup>5</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione del processo di selezione, assunzione e sviluppo del personale.
- Definizione di ruoli, responsabilità e organizzazione all’interno della Società.
- Gestione delle attività di valutazione, remunerazione ed incentivazione del personale, inclusa l'erogazione di compensi variabili.
- Gestione del payroll e dell'amministrazione del personale.
- Gestione delle trasferte, delle note spese e delle spese di rappresentanza.

### 7.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 318 c.p. Corruzione per l’esercizio della funzione;
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio;
- art. 319 bis c.p. Circostanze aggravanti;
- art. 319 ter c.p. Corruzione in atti giudiziari;
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità;
- art. 320 Corruzione di persona incaricata di un pubblico servizio;
- art. 321 c.p. Pene per il corruttore;
- art. 322 c.p. Istigazione alla corruzione;
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 346 bis c.p. Traffico di influenze illecite.

#### **Reati societari (art. 25 ter)**

- art. 2629-bis c.c. Omessa comunicazione del conflitto di interessi;
- art. 2635 c.c. Corruzione tra privati;
- art. 2635 bis c.c. Istigazione alla corruzione tra privati.

#### **Delitti con finalità di terrorismo o di eversione dell’ordine democratico (art. 25 quater)**

- art. 270 bis c.p. Associazioni con finalità di terrorismo anche internazionale o di eversione dell’ordine democratico.

#### **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)**

- art. 22, comma 12 bis D. Lgs 25 luglio 1998, n. 286 Impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere;
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere.

#### **Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci

<sup>5</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A

all'autorità giudiziaria;

- art. 416 c.p. Associazione per delinquere;
- art. 416 bis c.p. Associazioni di tipo mafioso.

#### **Delitti contro la personalità individuale (art. 25 quinquies)**

- art. 603-bis c.p. Intermediazione illecita e sfruttamento del lavoro.

#### **Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25 septies)**

- art. 589 c.p. Omicidio colposo;
- art. 590, terzo comma, c.p. Lesioni personali colpose.

#### **Reati ambientali (art. 25 undecies)**

- art. 452-bis c.p. Inquinamento ambientale;
- art. 452-quinquies c.p. Delitti colposi contro l'ambiente;
- D.Lgs n.152/2006, art.256 Attività di gestione di rifiuti non autorizzata.

### 7.3. Standard di controllo

#### 7.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

#### 7.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

##### **a) Gestione del processo di selezione, assunzione e sviluppo del personale**

- siano definite le esigenze di risorse da parte della Società attraverso l'approvazione del budget del personale;
- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  - approvazione del budget delle assunzioni;
  - manifestazione della necessità di assumere personale;
  - autorizzazione all'assunzione;
  - valutazione e selezione dei candidati;
  - sottoscrizione del contratto di assunzione;
- la richiesta di selezione e assunzione sia formalizzata da parte delle funzioni richiedenti attraverso la compilazione di modulistica specifica e nell'ambito del budget annuale approvato;
- l'autorizzazione della richiesta dal responsabile competente sia formulata secondo le procedure interne;
- sia garantito che le richieste di assunzione fuori dai limiti di budget siano debitamente motivate dalla funzione richiedente e autorizzate dal vertice aziendali in accordo con le procedure interne;
- per ogni profilo ricercato siano valutate almeno tre candidature, salvo motivi di oggettiva impossibilità dovuta alla particolarità del profilo stesso;
- siano definite formalmente le fonti di reperimento dei Curricula Vitae;
- siano preventivamente definiti formalmente i requisiti richiesti per la posizione da ricoprire in termini di ruolo/responsabilità, competenze professionali, attitudini e requisiti, livelli retributivi e tipologia contrattuale;
- sia definito l'iter di selezione mediante colloqui conoscitivi e tecnici e sia verificata la documentazione necessaria all'assunzione, ivi compresa, in caso di assunzione di cittadini extra

- comunitari, la copia del passaporto e del permesso di soggiorno in corso di validità;
- siano formalizzate le valutazioni dei candidati in apposita documentazione di cui è garantita l'archiviazione a cura del responsabile del personale;
  - sia sottoscritta formalmente da parte del candidato una dichiarazione relativa all'assenza di conflitti di interesse;
  - siano accertati e valutati preventivamente i rapporti, diretti o indiretti, tra il candidato e la PA.
  - In caso di assunzione di lavoratori extracomunitari:
    - sia individuato il responsabile del controllo iniziale e successivo della validità e dei permessi di soggiorno;
    - siano codificati i controlli da effettuare nel corso del rapporto di lavoro;
    - sia sottoposto all'attenzione del Direttore Generale l'eventuale cittadinanza straniera del candidato ed il relativo permesso di soggiorno;
    - sia inserito nel contratto con il consulente del lavoro un richiamo agli obblighi derivanti dalla normativa;
    - siano richiesti gli estremi del permesso di soggiorno del lavoratore extracomunitario assunto;
    - sia data comunicazione dell'instaurazione del rapporto di lavoro agli organi preposti territorialmente competenti, assicurando 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;
    - siano monitorate periodicamente le scadenze dei permessi di soggiorno dei lavoratori extracomunitari;
    - sia inviata, con congruo preavviso rispetto alla data di scadenza del permesso di soggiorno, una comunicazione scritta al dipendente, evidenziando l'approssimarsi della data di scadenza del permesso di soggiorno e sia richiesto di consegnare all'azienda copia del documento attestante l'avvenuto rinnovo;
    - siano trasmesse, anche per il tramite di soggetti esterni, le informazioni relative al rinnovo del permesso di soggiorno agli uffici pubblici competenti territorialmente;

In relazione ai *“reati di omicidio colposo e lesioni gravi o gravissime commessi in violazione delle norme sulla tutela della Salute e Sicurezza sul Lavoro”*, sono previsti i seguenti protocolli di controllo:

- per tutte le figure individuate in materia di gestione di problematiche inerenti la Salute e Sicurezza sul Lavoro, siano predefiniti requisiti tecnico-professionali che il personale di Brennercom deve possedere e che possono trarre origine anche da specifici disposti normativi;
- predetti requisiti, in possesso del personale di Brennercom già nella fase antecedente l'assunzione o comunque preliminarmente alla “messa in posizione”, siano mantenuti nel corso della vita lavorativa di ciascun soggetto, anche in base alla mansione lavorativa ricoperta. I requisiti possono sempre e comunque essere conseguiti anche attraverso specifici corsi di formazione;
- tutto il personale:
  - riceva opportune informazioni circa le corrette modalità di espletamento dei propri incarichi
  - sia formato;
  - sia addestrato (nei casi previsti dalla normativa);
- della formazione e/o addestramento del personale sia prevista una verifica documentata al fine di valutare l'efficacia delle attività di formazione o di altre azioni eventualmente attuate, altresì mantenendo le relative registrazioni. In tutti i casi le attività di informazione, formazione e

addestramento siano documentate. La documentazione inerente alla formazione del personale è registrata ed è impiegata anche al fine dell'attribuzione di nuovi incarichi;

- l'attività di formazione sia condotta con l'obiettivo di:
  - garantire, anche attraverso un'opportuna pianificazione, che qualsiasi persona sotto il controllo dell'organizzazione sia competente sulla base di un'adeguata istruzione, formazione o esperienza;
  - identificare le esigenze di formazione connesse con lo svolgimento delle attività;
  - erogare la formazione o prendere in considerazione altre azioni per soddisfare tale esigenza;
  - garantire che il personale sia consapevole dell'impatto, effettivo o potenziale, del proprio lavoro, dei corretti comportamenti da adottare, del proprio ruolo e delle proprie responsabilità.
- la scelta del soggetto formatore può essere vincolata da specifici disposti normativi.

In relazione ai *“reati ambientali commessi in violazione delle norme sulla tutela dell'ambiente”*, sono previsti i seguenti protocolli di controllo:

- siano identificate le esigenze di formazione connesse con lo svolgimento delle attività ed erogazione della formazione o altre azioni per soddisfare tali esigenze;
- sia garantito, anche attraverso un'opportuna pianificazione, che qualsiasi persona sotto il controllo dell'organizzazione sia competente sulla base di un'adeguata istruzione, formazione o esperienza;
- sia garantita la formazione circa le modalità di espletamento dei propri incarichi qualora questi possano avere rilevanti impatti ambientali;
- sia garantita la valutazione dell'efficacia delle attività di formazione o di altre azioni eventualmente attuate e la tenuta delle relative registrazioni;
- siano attuate misure volte a garantire che il personale prenda coscienza circa l'impatto effettivo o potenziale del proprio lavoro sull'ambiente, i corretti comportamenti da adottare, i propri ruoli e responsabilità;
- la documentazione attinente alla gestione delle attività di informazione, formazione e addestramento sia tracciabile e disponibile;
- siano definiti opportuni strumenti di reporting anche in aderenza alle prescrizioni autorizzative e di legge;
- sia formalizzato ed attuato un piano di audit che consideri tutti gli impatti ambientali descritti;
- sia data comunicazione delle risultanze degli audit ai soggetti preposti e conseguentemente siano valutate opportune misure correttive da intraprendere in considerazione di tutti gli impatti ambientali descritti.

#### **b) Definizione di ruoli, responsabilità e organizzazione all'interno della Società**

In relazione ai *“reati di omicidio colposo e lesioni gravi o gravissime commessi in violazione delle norme sulla tutela della Salute e Sicurezza sul Lavoro”*, sono previsti i seguenti protocolli di controllo:

- sia istituito il servizio di prevenzione e protezione, siano designati il responsabile ed eventuali addetti;
- sia nominato il medico competente;
- siano formalizzate le responsabilità di gestione, coordinamento e controllo all'interno della Società;
- siano correttamente nominati i soggetti previsti dalla normativa in materia di igiene, Salute e Sicurezza sul Lavoro (ivi incluso il Rappresentante dei lavoratori per la sicurezza) e siano loro conferiti i poteri necessari allo svolgimento del ruolo assegnato;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale sia congruente con le posizioni di responsabilità e con la rilevanza e/o la criticità delle sottostanti situazioni di rischio;
- i soggetti preposti e/o nominati ai sensi della normativa vigente in materia di igiene, Salute e

Sicurezza sul Lavoro possiedano competenze adeguate ed effettive in materia;

- sia costruito, ove necessario, il sistema di deleghe, dei poteri di firma e dei poteri di spesa coerentemente con le responsabilità assegnate, realizzato in accordo con i requisiti stabiliti dall'art. 16 del D. Lgs. n. 81/2008.

In relazione ai *“reati ambientali commessi in violazione delle norme sulla tutela dell'ambiente”*, sono previsti i seguenti protocolli di controllo:

- siano identificate le esigenze di formazione connesse con lo svolgimento delle attività ed erogazione della formazione o altre azioni per soddisfare tali esigenze;
- sia garantito, anche attraverso un'opportuna pianificazione, che qualsiasi persona sotto il controllo dell'organizzazione sia competente sulla base di un'adeguata istruzione, formazione o esperienza;
- sia garantita la formazione circa le modalità di espletamento dei propri incarichi qualora questi possano avere rilevanti impatti ambientali;
- sia garantita la valutazione dell'efficacia delle attività di formazione o di altre azioni eventualmente attuate e la tenuta delle relative registrazioni;
- siano poste in essere misure volte a garantire che il personale prenda coscienza circa l'impatto effettivo o potenziale del proprio lavoro sull'ambiente, i corretti comportamenti da adottare, i propri ruoli e responsabilità;
- la documentazione attinente la gestione delle attività di informazione, formazione e addestramento sia tracciabile e disponibile;
- siano definiti opportuni strumenti di reporting anche in aderenza alle prescrizioni autorizzative e di legge;
- sia formalizzato un piano di audit e sia attuato in considerazione di tutti gli impatti ambientali descritti;
- sia data comunicazione delle risultanze degli audit ai soggetti preposti e conseguentemente siano valutate opportune misure correttive da intraprendere in considerazione di tutti gli impatti ambientali descritti.

**c) Gestione delle attività di valutazione, remunerazione ed incentivazione del personale, inclusa l'erogazione di compensi variabili**

- siano identificati ruoli e responsabilità in ordine all'elaborazione, valutazione e approvazione di un budget relativo ai premi ed incentivi;
- sia definito un processo interno per la valutazione delle performance e per la definizione della remunerazione, incentivazione e sviluppo del personale sulla base di obiettivi quali-quantitativi definiti;
- siano definiti dei criteri di valutazione delle performance e siano formalmente approvati gli esiti di tali valutazioni, nonché dei relativi provvedimenti retributivi adottati;
- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  - definizione e attribuzione degli obiettivi;
  - verifica del raggiungimento degli stessi;
  - autorizzazione all'erogazione della relativa incentivazione e remunerazione variabile;
- siano definite le modalità di corretta archiviazione e conservazione della documentazione in relazione alle attività di valutazione, remunerazione, incentivazione del personale.

**d) Gestione del payroll e dell'amministrazione del personale**

- sia identificate le responsabilità e le modalità di gestione, creazione e modifica dell'anagrafica dei dipendenti;
- sia verificata la correttezza e la completezza dei dati inseriti nell'anagrafica dipendente;
- gli accessi al sistema delle presenze/assenze siano limitati alle sole funzioni competenti ed in linea con una corretta segregazione dei compiti;

- le anagrafiche dipendenti siano monitorate periodicamente con conseguente chiusura dei profili in quiescenza/dimissionari;
- sia determinato un sistema di rilevazione delle presenze e delle omesse timbrature nonché verifica e formale autorizzazione delle ferie / straordinari / permessi dei dipendenti;
- siano verificate le disposizioni di pagamento relative alle retribuzioni ed agli oneri fiscali, assistenziali e previdenziali, nonché delle dichiarazioni da trasmettere agli enti di assistenza e previdenza;
- sia data giustificazione a supporto delle voci di retribuzione straordinarie;
- siano verificate e monitorate le scadenze relative alla validità del permesso di soggiorno durante il prosieguo del rapporto di lavoro.

**e) Gestione delle trasferte, delle note spese e delle spese di rappresentanza**

- l'esecuzione di trasferte sia autorizzata preventivamente da parte del responsabile gerarchico su presentazione di adeguati giustificativi;
- siano predefinite le tipologie di spese rimborsabili, i limiti di importo relativi alle varie tipologie di spese (ad esempio di viaggio, di soggiorno, ecc.), gli importi massimi e le relative modalità di rendicontazione;
- sia attribuita la responsabilità di verificare la coerenza tra le spese sostenute, le attività svolte e la documentazione di supporto;
- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  - autorizzazione all'esecuzione di trasferte;
  - verifica delle note spese e autorizzazione del rimborso.
- sia definito e approvate in anticipo lo scopo dei viaggi con tracciabilità e conservazione della documentazione a supporto;
- siano definiti i criteri di accettabilità delle spese di rappresentanza, le quali comunque devono essere "moderate" e chiaramente destinate a facilitare le discussioni di lavoro;

In relazione ai *“reati di omicidio colposo e lesioni gravi o gravissime commessi in violazione delle norme sulla tutela della Salute e Sicurezza sul Lavoro”*, sono previsti i seguenti protocolli di controllo:

- la definizione di ruoli e responsabilità per la gestione degli aspetti relativi alle trasferte del personale lavorativo;
- la definizione di apposite procedure volte alla gestione delle attività di trasferta;
- la definizione ed attuazione di attività formative volte alla gestione del *“rischio Paese”* per il personale coinvolto in trasferte verso Paesi esteri;
- la definizione delle modalità di comunicazione/contatto con i lavoratori che effettuano le proprie prestazioni al di fuori della sede di lavoro (siano essi lavoratori in trasferta o lavoratori trasfertisti) in caso di eventi emergenziali occorsi nel luogo presso cui essi si trovano;
- la definizione delle modalità di gestione e comunicazione alle Autorità competenti delle eventuali situazioni emergenziali occorse ai lavoratori.

## 8. Processo “RESEARCH AND DEVELOPMENT”

### 8.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Research and Development”<sup>6</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione di marchi e brevetti di proprietà, anche tramite terzi.

### 8.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 317 c.p. Concussione
- art. 318 c.p. Corruzione per esercizio della funzione
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio
- art. 319 bis c.p. Circostanze aggravanti
- art. 319 ter c.p. Corruzione in atti giudiziari
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità
- art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p. Pene per il corruttore
- art. 322 c.p. Istigazione alla corruzione
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 640 c.p. Truffa
- art. 640 bis c.p. Truffa aggravata per il conseguimento di erogazioni pubbliche
- art. 346 bis c.p. Traffico di influenze illecite.

#### **Reati societari (art. 25 ter)**

- art. 2629 c.c. Omessa comunicazione del conflitto di interessi
- art. 2635 c.c. Corruzione tra privati
- art. 2635 bis c.c. Istigazione alla corruzione tra privati

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

- art. 515 c.p. Frode nell'esercizio del commercio
- art. 513 bis c.p. Illecita concorrenza con minaccia o violenza
- art. 517-ter c.p. Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale

### 8.3. Standard di controllo

#### 8.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

<sup>6</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A.

### 8.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

- siano individuati i soggetti preposti alla creazione e registrazione di un nuovo marchio o di un nuovo diritto di proprietà industriale, imponendo, ove possibile, una ricerca di anteriorità;
- sia censiti i diritti industriali di proprietà di Brennercom e siano tutelati attraverso un inserimento puntuale di clausole nei contratti con i terzi;
- siano censiti i diritti industriali dei Clienti e dei Fornitori;
- siano censite le clausole di riservatezza;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

## 9. Processo “INFORMATION TECHNOLOGY”

### 9.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Information Technology”<sup>7</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione di accessi logici, account e profili.
- Gestione della sicurezza informatica.
- Gestione dei sistemi hardware e software e dell'acquisizione di licenze software.
- Gestione degli accessi fisici ai siti ove risiedono infrastrutture IT.
- Gestione della smart card per firme digitali.

### 9.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Delitti informatici e trattamento illecito di dati (art. 24 bis)**

- art. 615 ter c.p. Accesso abusivo ad un sistema informatico o telematico;
- art. 615 quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- art. 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- art. 617 quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- art. 617 quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
- art. 635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici;
- art. 635 ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità;
- art. 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;
- art. 1, comma 11, D.L. 21 settembre 2019, n. 105 - Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica.

#### **Reati in materia di diritto d'autore (art. 25 novies):**

- art. 171, legge n.633/1941 comma 1 lett. a) bis 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-bis legge n.633/1941 comma 1 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.

<sup>7</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A

### 9.3. Standard di controllo

#### 9.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

#### 9.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

- siano identificati i ruoli e le responsabilità del personale coinvolto nelle attività;
- siano previsti attori diversi operanti nelle seguenti fasi/attività del processo:
  - creazione di una nuova utenza;
  - creazione, modifica, disattivazione degli account logici;
  - autorizzazione delle richieste;
- siano definiti dei principi generali di identificazione, autenticazione e autorizzazione;
- siano definiti dei flussi autorizzativi per la creazione, modifica e dismissione delle utenze;
- sia consentito l'accesso alle sole risorse informatiche a cui si è autorizzati;
- le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali siano custodite secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;
- siano rispettate le policy aziendali in merito ai dispositivi antintrusione e antivirus;
- siano definiti nei contratti con i fornitori per l'esecuzione di incarichi relativi ad uno o più processi del sistema informatico (sviluppo software, esercizio applicazioni, manutenzioni), i controlli e le misure necessarie per garantire la sicurezza del servizio, verificandone altresì l'attendibilità commerciale e professionale;
- sia mantenuta evidenza, in apposite registrazioni su archivi informatici, dei livelli di autorizzazione all'accesso (alla rete aziendale ed a sistemi di proprietà di Terzi) degli utenti ai fini della tracciabilità degli accessi e delle attività informatiche.
- siano previsti strumenti di riutilizzo di supporti di memoria in condizioni di sicurezza;
- siano previsti e attuati processi e meccanismi che garantiscano la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti;
- sia garantita la protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking;
- siano verificate le competenze, l'esperienza e l'affidabilità necessarie da parte dei soggetti nominati Amministratori di Sistema per assolvere le proprie mansioni;
- siano definiti i compiti in capo agli Amministratori di Sistema e controlli ad hoc sugli accessi effettuati;
- siano descritte le attività di monitoraggio periodico delle utenze finalizzate alla bonifica di quelle utenze non più necessarie (es. per modifiche organizzative, utente che ha lasciato l'azienda, ecc.);
- siano definite le regole per garantire la tracciabilità delle attività svolte, e siano supportate da evidenze formali, dallo scambio di informazioni all'interno dell'azienda per la gestione degli accessi logici, account e profili;
- sia richiesta a ciascun fornitore a cui sono affidati servizi di amministrazione di sistema l'elenco delle persone fisiche preposte come Amministratori di Sistema;
- sia tenuta traccia degli accessi anche degli Amministratori di Sistema ai sistemi che trattano dati personali in un apposito access log, di cui sono garantite l'integrità e l'immodificabilità;
- sia data comunicazione ai terzi del Modello 231, dei cui principi si richiede il rispetto attraverso

opportune clausole contrattuali, qualora le operazioni oggetto della presente attività siano date in outsourcing;

- siano descritte le misure di sicurezza previste per la gestione sicura e corretta della rete e per la manutenzione della stessa;
- sia descritta l'architettura di rete;
- sia prevista la segregazione logica e, laddove possibile, fisica della rete interna e dalle reti esterne, e siano previste idonee misure di sicurezza e firewall che permettano di ridurre l'esposizione ai rischi (es. connessione delle terze parti, Internet);
- sia prevista la separazione delle reti su cui si attestano sistemi di produzione (reti server) dalle reti cui si connettono gli utenti (reti client) e dalle reti amministrative e siano previsti meccanismi di sicurezza volti a limitare l'accesso unicamente al personale dotato di adeguati profili autorizzativi;
- sia previsto il blocco del traffico amministrativo dei dispositivi connessi a Internet, consentendolo soltanto ad un range dedicato di indirizzi interni;
- sia registrato e conservato in un apposito server ogni tentativo di violazione alle regole dei firewall delle liste controllo accessi;
- laddove necessario, siano previste restrizioni d'accesso alle connessioni esterne implementate per la connessione punto-punto con clienti e fornitori, in linea con il principio del minimo privilegio; eventuali nuove connessioni siano formalmente richieste e tracciate mediante uno strumento di ticketing e soggette a formale autorizzazione da parte delle Direzioni preposte;
- i log generati contengano almeno data e ora della connessione e attività svolte;
- sia prevista la connessione in VPN per gli utenti che intendano connettersi da remoto alla rete interna; laddove tecnicamente possibile, l'accesso in VPN avvenga mediante meccanismi di autenticazione basati su strong authentication;
- l'accesso alla connessione alla rete WLAN sia consentito unicamente ai soggetti autorizzati, previa autenticazione mediante l'impiego di un protocollo di sicurezza autorizzato, sicuro e affidabile, al fine di minimizzare il rischio di accesso non autorizzato alle risorse di rete;
- sia previsto il monitoraggio completo delle licenze software:
  - attraverso il passaggio dalla funzione IT di ogni richiesta di installazione di un nuovo software/hardware;
  - attraverso l'acquisizione di strumenti idonei a rilevare l'installazione di software non licenziati;
- sia previsto il monitoraggio completo dei software e hardware installati, attraverso l'acquisizione di uno strumento in grado di rilevare l'installazione di software ed hardware non autorizzati;
- siano comunicate al personale dipendente, al momento dell'assunzione, le istruzioni per l'utilizzo dei pc per l'uso interno alla società;
- sia erogata formazione periodica al personale dipendente su tematiche attinenti all'utilizzo dei software e hardware aziendali;
- sia predisposto un elenco degli hardware e dei software autorizzati a livello aziendale e disponibile a tutto il personale;
- sia predisposto un elenco delle licenze acquistate dalla società e sia reso accessibile a tutto il personale;
- l'accesso ai server sia riservato unicamente al personale autorizzato, previo superamento di una procedura di autenticazione;
- siano monitorate periodicamente le utenze, al fine di individuare e disabilitare le utenze non più necessarie o che non sono utilizzate da un determinato lasso di tempo;
- i server siano collocati in un'area appropriata, dotata di meccanismi per il controllo degli accessi e delle necessarie misure di sicurezza ambientale (es. climatizzazione, rilevatore fumi, impianto antincendio, ...);

- siano analizzate le modalità di richiesta, approvazione ed eventuale revoca dei soggetti autorizzati all'apposizione della firma digitale sui documenti;
- siano comunicate le responsabilità dei soggetti autorizzati all'apposizione della firma digitale sui documenti;
- sia previsto l'utilizzo di sistemi di certificazione (criteri e modalità per la generazione, distribuzione, revoca ed archiviazione delle chiavi digitali come le smart card);
- siano definite le modalità di utilizzo ed invio dei documenti informatici sottoposti a firma digitale;
- siano definite le modalità di gestione delle smart card (o eventuali altri supporti) da parte di soggetti terzi;
- siano definiti i controlli di sicurezza per la protezione delle smart card (o eventuali altri supporti) da possibili modifiche, distruzioni e utilizzi non autorizzati;
- siano definiti dei processi aziendali e dei processi IT, compresi quelli che regolano sviluppo, manutenzione ed esercizio di tali sistemi, al fine di assicurare la conformità a livello di singoli sistemi/infrastrutture ICT/Rete alle prescrizioni adottate dalla Società;
- siano attribuiti i poteri autorizzativi e di firma chiaramente definiti e conosciuti all'interno della Società, in modo coerenti con le responsabilità organizzative;
- sia fatto divieto di alterare in qualsiasi modo, manomettere o modificare autonomamente i sistemi applicativi, le infrastrutture hardware e i dati in uso di proprietà o di Terzi, o manipolarne i dati;
- sia fatto divieto di danneggiare i sistemi informatici di proprietà o di Terzi;
- sia fatto divieto di 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;
- sia fatto divieto di installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- nei contratti con i fornitori per l'esecuzione di incarichi relativi ad uno o più processi del sistema informatico (sviluppo software, esercizio applicazioni, manutenzioni) siano definiti i controlli e le misure necessarie per garantire la sicurezza del servizio, verificandone altresì l'attendibilità commerciale e professionale;
- siano adottate le procedure necessarie per la gestione delle attività di backup delle scritture obbligatorie ed in particolare al fine di:
  - mantenere le copie di backup in luoghi sufficientemente distanti dal sito principale;
  - effettuare test sul ripristino delle scritture contabili obbligatorie;
  - eseguire un'attività di monitoraggio sull'esito dei backup e, qualora vi fossero riscontrate anomalie, vengono prese in carico e risolte tempestivamente;
- siano adottati piani di Disaster Recovery al fine di garantire la continuità dei sistemi informatici utilizzati per la tenuta delle scritture contabili obbligatorie ed in particolare:
  - una periodica attività di aggiornamento di tali piani;
  - una periodica attività di testing di tali piani;
- il sistema amministrativo-contabile sia impostato in modo tale da non consentire la registrazione di scritture contabili nei periodi chiusi;
- sia inserito nel sistema contabile un apposito meccanismo automatico volto ad impedire la duplice registrazione di un documento nel medesimo esercizio.

## 10. Processo “MARKETING COMMUNICATION”

### 10.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Marketing Communication<sup>8</sup>”. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione delle attività di marketing, pubblicità e comunicazione (compresa la gestione dei contenuti).
- Gestione di sponsorizzazioni, omaggi, donazioni ed erogazioni liberali.
- Gestione dei contenuti del sito Internet della Società e dei relativi social network, anche tramite soggetti terzi.

### 10.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 316 bis c.p. Malversazione a danno dello Stato
- art. 317 c.p. Concussione
- art. 318 c.p. Corruzione per l’esercizio della funzione
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità
- art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p. Pene per il corruttore
- art. 322 c.p. Istigazione alla corruzione
- art. 322 bis c.p. Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- art. 346 bis c.p. Traffico di influenze illecite

#### **Reati societari (art. 25 ter)**

- art. 2635 c.c. Corruzione tra privati
- art. 2635 bis c.c. Istigazione alla corruzione tra privati

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

#### **Razzismo e xenofobia (art. 25 terdecies)**

- art. 5 c.2 Legge 167/2017, Razzismo e xenofobia

#### **Reati in materia di diritto d’autore (art. 25 novies)**

- art. 171, legge n.633/1941 comma 1 lett. a) bis 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-bis legge n.633/1941 comma 1 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

<sup>8</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A

contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori.

**Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art. 25 octies)**

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

**Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- art. 378 c.p. Favoreggiamento personale
- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso

**Reati di abuso di mercato (art. 25 sexies)**

- art. 184 TUF Abuso di informazioni privilegiate
- art. 185 TUF Manipolazione del mercato.

### 10.3. Standard di controllo

#### 10.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

#### 10.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

- nelle comunicazioni al mercato sia garantita la veridicità e la correttezza delle informazioni concernenti la Società, in particolare, di quelle destinate a investitori, analisti finanziari, giornalisti o altri rappresentanti dei mezzi di comunicazione;
- la comunicazione esterna verso il mercato e la Consob avvenga attraverso comunicati curati dalle funzioni preposte. Siano vietate comunicazioni esterne verso il mercato e la Consob non preventivamente approvate dall'Amministratore Delegato o da personale dotato di idonei poteri, nel rispetto delle procure in essere;
- sia svolta un'analisi preventiva delle informazioni da comunicare all'esterno in coerenza con gli obiettivi aziendali (ad esempio al fine di verificare che non compromettano le attività commerciali della Società o che non siano soggette a restrizioni);
- sia svolto un monitoraggio delle comunicazioni alla stampa o ad altri mezzi di informazione, al fine prevenire il rischio di diffusione di notizie false o fuorvianti riguardanti, ad esempio, le condizioni della Società;
- sia garantita integrità, imparzialità e indipendenza, non influenzando impropriamente le decisioni dei media e non richiedendo trattamenti di favore; è in ogni caso sia fatto divieto di promettere, erogare o ricevere favori, somme e benefici di qualsivoglia natura;
- l'utilizzo di contenuti multimediali, propri o di terzi, ovvero selezionati tramite banche immagini o prodotti da fornitori contrattualizzati, sia preventivamente autorizzato e sottoposto a verifiche di conformità ai sensi delle vigenti normative in materia di pubblicità;

- sia garantita una chiara definizione delle responsabilità e dell'iter approvativo relativo all'apporto di modifiche alle sezioni del sito;
- siano catalogate in apposito database le opere protette da diritto d'autore acquistate dalla Società ai fini dell'attività comunicativa, sia interna che esterna;
- siano formalmente identificate le funzioni aziendali responsabili e coinvolte nella gestione di sponsorizzazioni, eventi ed iniziative promozionali;
- la concessione di sponsorizzazioni sia coerente con i valori aziendali espressi nel Codice Etico e sia diretta ad accrescere e promuovere l'immagine e la cultura della Società;
- sia garantita segregazione tra chi approva il budget delle sponsorizzazioni e della partecipazione ad iniziative promozionali, chi le richiede e chi le autorizza;
- siano individuati specifici driver per la valutazione della sponsorizzazione (es. immagine dell'impresa, valenza commerciale dell'iniziativa, copertura media, relazioni con il territorio, relazioni con gli stakeholder ecc.);
- sia effettuata una due-diligence sui destinatari/promotori delle iniziative, finalizzata ad accertare la capacità tecnica/economica, che non vi siano condizioni di incompatibilità o conflitto di interessi, anche con riguardo ai rapporti di parentela o alle relazioni di carattere personale o professionale del destinatario;
- l'esecuzione delle iniziative venga formalmente autorizzata da parte di soggetti dotati di idonei poteri e l'inizio della prestazione sia sempre preceduta dalla stipula di un accordo/contratto scritto di sponsorizzazione;
- eventuali spese extra (rispetto al preventivo approvato) siano sottoposte ad autorizzazione e sia effettuato un monitoraggio sui consuntivi di spesa al fine di informare il management di eventuali scostamenti rilevanti;
- siano formalmente identificate le funzioni aziendali responsabili e coinvolte nella gestione di omaggi, donazioni ed erogazioni liberali;
- sia garantita segregazione tra chi approva il budget degli omaggi, donazioni ed erogazioni liberali, chi le richiede e chi le autorizza;
- la concessione di donazioni ed erogazioni liberali sia coerente con i valori aziendali espressi nel Codice Etico;
- venga effettuata una due-diligence sui beneficiari delle donazioni ed erogazioni liberali, finalizzata a verificare il tipo di organizzazione e la finalità per la quale è costituita e ad accertare che non vi siano condizioni di incompatibilità o conflitto di interessi, anche con riguardo ai rapporti di parentela o alle relazioni di carattere personale o professionale del destinatario;
- sia fatto divieto di accettare, ricevere, dare, offrire o promettere - anche indirettamente - denaro, doni, favori, beni, servizi o prestazioni non dovuti, in relazione a rapporti intrattenuti con pubblici ufficiali, incaricati di pubblico servizio, Enti pubblici o privati o loro dipendenti;
- sia preventivamente definita la tipologia e i limiti degli omaggi in ingresso e in uscita concessi, anche, eventualmente, verso esponenti della Pubblica Amministrazione, Società a controllo pubblico, Pubblici Ufficiali, Incaricati di Pubblico Servizio;
- gli omaggi consentiti:
- siano sempre caratterizzati per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad es., la distribuzione di libri d'arte) o la brand image di Brennercom e comunque tali da non poter essere interpretati come finalizzati ad ottenere un trattamento di favore e da non compromettere l'integrità o la reputazione;
- siano rivolti verso soggetti che svolgono ruoli inerenti alle attività aziendali e che rispondono ai requisiti di reputazione e di onorabilità generalmente riconosciuti;
- tengano conto del profilo del soggetto beneficiario, con riguardo alle consuetudini nei rapporti istituzionali o professionali;

- siano effettuati dagli amministratori, dai dirigenti e dai dipendenti in funzione dell'attività svolta e del ruolo ricoperto all'interno della Società;
- tutte le concessioni di utilità siano approvate dai soggetti dotati di idonei poteri, nel rispetto delle procure in essere;
- sia prevista la rilevazione di operazioni ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- siano immediatamente interrotte o, comunque, non eseguite operazioni relative a donazioni, sponsorizzazioni, omaggi e liberalità, che vedano coinvolti come beneficiari, soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- nell'ambito degli accordi contrattuali con Soggetti Terzi sia garantita la presa visione e la conformità ai principi contenuti nel Codice Etico e nel Modello Organizzativo di Brennercom;
- sia garantita la tracciabilità e corretta archiviazione di tutti i passaggi del processo sia a livello di sistema informativo che documentale.

## 11. Processo “LEGAL & CORPORATE AFFAIRS”

### 11.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Legal & Corporate Affairs”<sup>9</sup>. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione di procedimenti giudiziari, arbitrari e stragiudiziali con la P.A. e con soggetti terzi.

### 11.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio;
- art. 319 ter c.p. Corruzione in atti giudiziari;
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità;
- art. 321 c.p. Pene per il corruttore;
- art. 322 c.p. Istigazione alla corruzione;
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 346 bis Traffico di influenze illecite.

#### **Reati Societari (art. 25 ter)**

- art. 2621 c.c. False comunicazioni sociali;
- art. 2622 c.c. False comunicazioni sociali delle società quotate;
- art. 2625 Impedito controllo;
- art. 2626 c.c. Indebita restituzione di conferimenti;
- art. 2628 c.c. Illecite operazioni sulle azioni o quote sociali o della società controllante;
- art. 2629 bis c.c. Omessa comunicazione del conflitto d'interessi;
- art. 2632 c.c. Formazione fittizia del capitale;
- art. 2633 c.c. Indebita ripartizione dei beni sociali da parte dei liquidatori;
- art. 2636 c.c. Illecita influenza sull'assemblea.
- art. 2635 c.c. Corruzione tra privati;
- art. 2635 bis c.c. Istigazione alla corruzione tra privati.

#### **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies)**

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

### 11.3. Standard di controllo

#### 11.3.1. Standard di controllo generali

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e agli standard di controllo generali definiti ed implementati dalla Società che gestisce le attività.

<sup>9</sup> Il processo e le relative attività sensibili sono gestiti in regime di outsourcing e costituiscono oggetto di contratto di service infragruppo con Retelit S.p.A.

### 11.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

- siano definite e condivise con il vertice societario le strategie processuali;
- sia monitorato periodicamente lo status dei contenziosi in corso, in coordinamento con i legali esterni incaricati, anche al fine di monitorare l'effettiva attuazione della strategia processuale condivisa;
- vi sia formale autorizzazione, nel rispetto delle procure in essere, delle proposte transattive;
- sia garantita la tracciabilità delle richieste di informazioni ricevute nel corso del contenzioso e delle persone coinvolte, nonché del processo di valutazione e autorizzazione interna della documentazione consegnata nel corso del contenzioso;
- i compensi, le spese e le attività dei legali esterni incaricati siano rendicontate e monitorate;
- sia possibile evincere, attraverso l'elenco dei provvedimenti e/o notizie provenienti dall'Autorità Giudiziaria, o da qualsiasi altra autorità, lo svolgimento di indagini/accertamenti riguardanti la Società, anche nei confronti di ignoti, per i reati o gli illeciti amministrativi di cui al D. Lgs. 231/01;
- sia reso noto il numero, l'importo totale (€) e la descrizione di eventuali accordi transattivi stragiudiziali stipulati, anche tramite legali esterni, nel periodo di riferimento;
- la selezione di legali esterni avvenga nel rispetto dei criteri di serietà e competenza del professionista;
- il conferimento di incarichi sia formalizzato tramite contratto/lettera di incarico/mandato alle liti;
- l'attività prestata dai legali sia documentata e vi sia l'attestazione dell'effettività della prestazione da essi erogata, prima della liquidazione del compenso;
- sia garantita l'autorizzazione formale, nel rispetto delle deleghe e delle procure in essere, al pagamento degli onorari dei legali esterni;
- siano definite le modalità operative di archiviazione della documentazione ad opera del Responsabile, in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- sia garantita la protocollazione di tutta la documentazione ufficiale relativamente a contenzioso/arbitrato di interesse del Gruppo;
- sia valutata la congruità formale dei flussi documentali e di esperibilità delle azioni funzionali al procedimento, da parte di un legale interno o del presidio legale di riferimento;
- sia data autorizzazione preventiva e formalizzata dei conferimenti degli incarichi professionali solo da parte di Soggetti specificatamente procurati;
- sia valutata, prima del pagamento del corrispettivo al professionista, la congruità della parcella con riferimento alle prestazioni ricevute dalla Società e alle tariffe definite dal contratto/accordo;
- siano definiti specifici flussi di reporting alle competenti funzioni Legali definiti in relazione ad eventi giudiziari di particolare rilevanza;

in caso di accordi transattivi:

- sia verificata l'esistenza di criteri quali/quantitativi per il ricorso ad accordi transattivi in alternativa alla gestione della controversia in sede giudiziale/arbitrale;
- vi sia l'approvazione, da parte dei soggetti dotati di adeguati poteri, a procedere ad un accordo bonario o transattivo in alternativa al procedimento giudiziale;
- in caso di sottoscrizione di accordi transattivi in deroga, sia acquisito formalmente il parere della Funzione Legale competente;
- l'accordo transattivo sia sottoscritto da parte di adeguato livello gerarchico;
- l'articolazione del processo garantisca la segregazione funzionale tra i coloro che agiscono

nell'ambito del processo di gestione del contenzioso;

- sia prevista la predisposizione di uno scadenario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti;
- sia garantita la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate;

## 12. Processo “RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE”

### 12.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative alla gestione dei rapporti con la Pubblica Amministrazione. Tenuto conto della tipologia dei rapporti che Brennercom intrattiene con la Pubblica Amministrazione, le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione delle richieste di informazioni dalla Procura della Repubblica (inclusa la raccolta e la gestione di traffico dati ai fini di giustizia).
- Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione).
- Gestione dei rapporti con la Pubblica Amministrazione per la richiesta e l'ottenimento di informazioni e di diritti di passaggio, licenze, permessi, autorizzazioni per lo sviluppo dell'infrastruttura.
- Gestione dei rapporti con soggetti istituzionali (inclusa la gestione delle relazioni con AGCOM, Ministeri statali, strutture comunitarie) con altri stakeholder (decision e opinion maker) e attività di lobbying.
- Gestione dei rapporti con gli enti competenti in occasione di ispezioni o verifiche di natura fiscale, previdenziale o lavoristica (ad es. Agenzia delle Entrate, Guardia di Finanza, Ispettorato del lavoro, INPS, INAIL, etc.).

### 12.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25):**

- art. 316 bis c.p. Malversazione a danno dello stato
- art. 316 ter c.p. Indebita percezione di erogazioni a danno dello Stato
- art. 317 c.p. Concussione
- art. 318 c.p. Corruzione per l'esercizio della funzione
- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio
- art. 319 bis c.p. Circostanze aggravanti
- art. 319 ter c.p. Corruzione in atti giudiziari
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità
- art. 320 c.p. Corruzione di persona incaricata di un pubblico servizio
- art. 321 c.p. Pene per il corruttore
- art. 322 c.p. Istigazione alla corruzione
- art. 322 bis c.p. Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri
- art. 346 bis Traffico di influenze illecite
- art. 640 c.2 c.p. Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee
- art. 640 bis c.p. Truffa aggravata per il conseguimento di erogazioni pubbliche
- art. 640 ter c.p. Frode informatica se a danno dello Stato o di altro Ente Pubblico

#### **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies)**

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

### 12.3. Standard di controllo

#### 12.3.1. Standard di controllo generali

Come riportato in premessa, gli standard di controllo generali sono applicabili al processo gestione dei rapporti con la Pubblica Amministrazione, in quanto principi guida del sistema di controllo interno e gestione dei rischi. Le seguenti regole di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, e per conto o nell'interesse della Società, intrattengano rapporti con pubblici ufficiali, incaricati di pubblico servizio o, più in generale, con rappresentanti della Pubblica Amministrazione.

#### 12.3.2. Standard di controllo specifici

Nell'ambito del Processo e dell'attività in oggetto, i protocolli implementati dalla Società prevedono che:

**a) Gestione delle richieste di informazioni dalla Procura della Repubblica (inclusa la raccolta e la gestione di traffico dati ai fini di giustizia)**

- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione delle attività operative relative all'esecuzione delle richieste di informazioni dalla Procura della Repubblica;
- siano definiti i ruoli e le responsabilità in relazione di gestione delle attività operative relative all'esecuzione delle richieste di informazioni dalla Procura della Repubblica;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza, con l'obiettivo di facilitare il dialogo su temi di interesse specifico;
- siano definite le modalità di raccolta, verifica e approvazione della documentazione da trasmettere ai pubblici ufficiali o incaricati di pubblico servizio, con il supporto delle funzioni competente;
- siano definite le modalità di trasmissione della documentazione alla Pubblica Amministrazione tali da assicurare la piena tracciabilità e garantire la completa ripercorribilità dell'operazione;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**b) Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione)**

- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione della partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani;
- siano definiti i ruoli e le responsabilità in relazione alla gestione delle attività operative circa la partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- sia identificata la Funzione Competente responsabile di intrattenere rapporti con esponenti della Pubblica Amministrazione sia in fase di predisposizione della proposta di offerta sia in fase di presentazione della stessa;

- siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza;
  - si prevedano le modalità di partecipazione a procedure ad evidenza pubblica, che assicurino che tutti dipendenti operino nel rispetto delle leggi, dei regolamenti vigenti e della corretta pratica commerciale;
  - siano definite le modalità con cui è svolta l'analisi preliminare di fattibilità tecnica ed economica volta a verificare la capacità della Società di eseguire i lavori nei tempi e nelle modalità previste dal bando di gara o dall'invito a partecipare ovvero di subappaltare le attività di esecuzione ad un operatore terzo;
  - si preveda l'autorizzazione formale preventiva da parte del Responsabile di funzione all'utilizzo dei dati e di informazioni destinati ad atti, comunicazioni, attestazioni e richieste di qualunque natura inoltrate o aventi come destinatario la PA;
  - siano definiti i livelli di autorizzazione necessari relativamente a offerte e contratti e gli stessi siano riflessi all'interno dei sistemi informativi in uso al personale;
  - siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.
- c) Gestione dei rapporti con la Pubblica Amministrazione per la richiesta e l'ottenimento di informazioni e di diritti di passaggio, licenze, permessi, autorizzazioni per lo sviluppo dell'infrastruttura**
- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione dei rapporti con la PA volti a richiedere ed ottenere diritti di passaggio, licenze, permessi e autorizzazioni per lo sviluppo dell'infrastruttura;
  - siano definiti i ruoli e le responsabilità in relazione alla gestione delle attività operative circa la richiesta e l'ottenimento di diritti di passaggio, licenze, permessi e autorizzazioni per lo sviluppo dell'infrastruttura;
  - siano definite le modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
  - siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza, con l'obiettivo di facilitare il dialogo su temi di interesse specifico;
  - si prevedano modalità di intrattenimento dei rapporti con la Pubblica Amministrazione che vietino e impediscano, per quanto possibile, ai soggetti incaricati di intrattenere rapporti con la PA di ricercare o instaurare illecitamente relazioni personali di favore, influenza o ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto con la Pubblica Amministrazione;
  - siano definite formalmente le modalità operative di gestione delle attività per la richiesta e l'ottenimento di diritti di passaggio, licenze, permessi e autorizzazioni per lo sviluppo dell'infrastruttura;
  - si preveda l'autorizzazione formale preventiva da parte del Responsabile di funzione circa i moduli e la documentazione da trasmettere alla Pubblica Amministrazione;
  - si prevedano modalità di trasmissione della documentazione alla PA che garantiscano la completezza, correttezza e trasparenza delle informazioni e dei dati eventualmente richiesti, al fine di assolvere agli adempimenti richiesti dalla Pubblica Amministrazione in relazione all'attuazione di adempimenti connessi alle attività aziendali;

- sia definito uno strumento di monitoraggio, anche supportato da evidenze formali, volto a verificare il corretto espletamento degli adempimenti, nonché il monitoraggio delle loro scadenze;
- sia definito uno strumento di monitoraggio, anche supportato da evidenze formali, volto a monitorare le novità normative in tema di gestione delle autorizzazioni e licenze in relazione alle attività aziendali;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**d) Gestione dei rapporti con soggetti istituzionali (inclusa la gestione delle relazioni con AGCOM, Ministeri statali, strutture comunitarie) con altri stakeholder (decision e opinion maker) e attività di lobbying**

- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione dei rapporti con la PA volti al posizionamento della Società presso le istituzioni e all'intrattenimento dei rapporti con gli stakeholder, nonché a svolgere attività di lobbying;
- siano definiti i ruoli e le responsabilità in relazione alla gestione delle attività operative circa la gestione dei rapporti con la PA volti al posizionamento della Società presso le istituzioni e all'intrattenimento dei rapporti con gli stakeholder, nonché a svolgere attività di lobbying;
- siano definite le modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza, con l'obiettivo di facilitare il dialogo su temi di interesse specifico;
- siano definite adeguate modalità di rappresentazione degli interessi aziendali, tali da garantire la fornitura di informazioni complete e rigorose con l'obiettivo di illustrare alla controparte istituzionale gli scopi della Società e le ricadute per i propri azionisti e tutti gli stakeholder, così come i benefici attesi;
- si prevedano modalità di intrattenimento dei rapporti con la Pubblica Amministrazione che vietino e impediscano, per quanto possibile, ai soggetti incaricati di intrattenere rapporti con la PA di ricercare o instaurare illecitamente relazioni personali di favore, influenza o ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto con la Pubblica Amministrazione;
- siano definite le modalità di formalizzazione della reportistica relativa al rapporto intercorso, sia che la stessa sia prodotta dalla Società o da terze parti. La reportistica sia oggetto di condivisione con il Responsabile della funzione;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**e) Gestione dei rapporti con gli enti competenti in occasione di ispezioni o verifiche di natura fiscale, previdenziale o lavoristica (ad es. Agenzia delle Entrate, Guardia di Finanza, Ispettorato del lavoro, INPS, INAIL, etc.)**

- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione dei rapporti con la PA in occasione di ispezioni o verifiche di natura fiscale, previdenziale o lavoristica;

- siano definiti i ruoli e le responsabilità in relazione alla gestione delle attività operative circa la gestione dei rapporti con la PA in occasione di ispezioni o verifiche di natura fiscale, previdenziale o lavoristica;
- siano definite le modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- sia prevista la presenza di soggetti dotati di idonei poteri e competenti in materia durante gli incontri/visite ispettive con la Pubblica Amministrazione. Di detti incontri deve essere tenuta traccia della documentazione richiesta e consegnata al funzionario;
- siano definite le modalità di gestione dei rapporti con la Pubblica Amministrazione e con Autorità/Organismi di Vigilanza che ispirate ai principi integrità, correttezza, trasparenza e collaborazione, evitando comportamenti che possano in qualsiasi modo considerarsi di ostacolo alle attività che tali Autorità sono chiamate a svolgere;
- si prevedano modalità di intrattenimento dei rapporti con la Pubblica Amministrazione che vietino e impediscano, per quanto possibile, ai soggetti incaricati di intrattenere rapporti con la PA di ricercare o instaurare illecitamente relazioni personali di favore, influenza o ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto con la Pubblica Amministrazione;
- siano definite le modalità di gestione delle ispezioni e dei sopralluoghi svolti da Ispettori / Funzionari di Autorità / Organi di controllo;
- si preveda, a valle dell'ispezione svolta, la sottoscrizione del verbale di ispezione, previa verifica del suo contenuto, ad opera della figura aziendale delegata ad interfacciarsi con gli ufficiali della Pubblica Amministrazione nonché dell'ulteriore figura aziendale presente in sede ispettiva;
- siano definite modalità di condivisione del verbale dell'ispezione subita nonché del verbale sottoscritto con la figura dell'Amministratore Delegato;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

## 13. Processo “OPERATIONS: PLATFORM & INFRASTRUCTURE”

### 13.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento al Processo Sensibile “Operations: Platform & Infrastructure”. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Gestione del servizio VOCE con tecnologia Voice Over IP e dei servizi di Unified Communication (ad esempio il Direct Routing).
- Gestione delle attività di delivery dei servizi della divisione P&I e contatto finale con i clienti nelle fasi di installazione, collaudo e verifica prodotto.
- Gestione contrattualistica "ultimo miglio" con provider di servizi Wholesale.
- Gestione dei servizi di housing & colocation (inclusa la sicurezza fisica) all'interno dei Data Center su territorio nazionale ed estero.
- Gestione dell'infrastruttura di rete (broadband / ultrabroadband / rete mista), compreso il coordinamento di terze parti per l'implementazione dell'infrastruttura ed erogazione del servizio di connessione.
- Gestione della Cyber Security e dei servizi di sicurezza informatica (inclusa la gestione delle terze parti necessarie per l'erogazione dei servizi di sicurezza).
- Gestione dei servizi Cloud (inclusi lo storage Cloud e il servizio Multicloud aziendale).
- Gestione attività di scouting fornitori sul mercato (es. individuazione di provider di nuove tecnologie tramite analisi di mercato).
- Gestione dei servizi a supporto del cliente (c.d. "Managed Services").
- Gestione del magazzino.

### 13.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Delitti informatici e trattamento illecito di dati (art. 24 bis)**

- art. 615 ter c.p. Accesso abusivo ad un sistema informatico o telematico;
- art. 615 quater c.p. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- art. 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- art. 617 quater c.p. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- art. 617 quinquies c.p. Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
- art. 635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici;
- art. 635 ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità;
- art. 640 quinquies c.p. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica;
- art. 1, comma 11, D.L. 21 settembre 2019, n. 105 - Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica.

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

**Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso
- art. 12, c. 3, 3-bis, 3-ter e 5, del testo unico di cui al D.Lgs. 25/07/1998, n.286 Disposizioni contro le immigrazioni clandestine

**Reati societari (art. 25 ter)**

- art. 2621 c.c. False comunicazioni sociali
- art. 2621 bis c.c. Fatti di lieve entità
- art. 2622 c.c. False comunicazioni sociali delle società quotate
- art. 2625 c.c. Impedito controllo
- art. 2628 c.c. Illecite operazioni sulle azioni o quote sociali o della società controllante
- art. 2629 c.c. Operazioni in pregiudizio dei creditori
- art. 2629 c.c. Omessa comunicazione del conflitto di interessi
- art. 2632 c.c. Formazione fittizia del capitale
- art. 2635 c.c. Corruzione tra privati
- art. 2635 bis c.c. Istigazione alla corruzione tra privati
- art. 2636 c.c. Illecita influenza sull'assemblea
- art. 2637 c.c. Aggiotaggio
- art. 2638 c.c. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

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

- art. 270 bis c.p. Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
- L. n. 153/2016, art.270 quinquies 1 c.p. Finanziamento di condotte con finalità di terrorismo
- art. 2 Convenzione di New York del 9 dicembre 1999

**Delitti contro la personalità individuale (art. 25 quinquies)**

- art. 603-bis c.p. Intermediazione illecita e sfruttamento del lavoro.

**Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art. 25 octies)**

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

### 13.3. Standard di controllo

#### 13.3.1. Standard di controllo generali

Come riportato in premessa, gli standard di controllo generali sono applicabili al processo "Operations: Platform & Infrastructure", in quanto principi guida del sistema di controllo interno e gestione dei rischi.

#### 13.3.2. Standard di controllo specifici

Nell'ambito del Processo e dell'attività in oggetto, i protocolli implementati dalla Società prevedono che:

**a) Gestione del servizio VOCE con tecnologia Voice Over IP e dei servizi di Unified Communication (ad esempio il Direct Routing)**

- siano individuati i soggetti preposti alla gestione delle attività operative del processo di gestione del servizio Voce;

- siano definiti i ruoli e le responsabilità in relazione alle attività di gestione del servizio Voce;
  - siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
  - siano svolte attività periodiche volte a verificare la corretta corrispondenza tra le caratteristiche del servizio erogato e quanto riportato nel relativo materiale tecnico/informativo o comunque su qualsiasi materiale consegnato al cliente o diffuso al pubblico;
  - siano autorizzate dalle figure aziendali preposte eventuali comunicazioni ai clienti in merito a qualità e specifiche del servizio;
  - sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio dei livelli di traffico generato dai clienti, nonché dell'efficacia della piattaforma di core network;
  - sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio circa il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, tramite l'utilizzo di report e trend sugli incidenti;
  - siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.
- b) Gestione delle attività di delivery dei servizi della divisione P&I e contatto finale con i clienti nelle fasi di installazione, collaudo e verifica prodotto**
- siano individuati i soggetti preposti alla gestione delle attività di installazione, collaudo e verifica del prodotto/servizio;
  - siano definiti i ruoli e le responsabilità in relazione alle attività di installazione, collaudo e verifica del prodotto/servizio;
  - siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa delle attività e le stesse siano formalizzate in apposite procedure;
  - siano definiti ed implementati controlli riguardanti i prodotti non conformi, da effettuare con il coinvolgimento del Cliente;
  - siano svolte attività di verifica circa la congruenza fra quanto contrattualizzato, quanto collaudato/attestato e quanto fatturato;
  - siano definite le modalità per lo svolgimento dell'attività di monitoraggio delle attività operative di installazione e collaudo del prodotto presso il cliente;
  - sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio circa il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica che possono verificarsi in caso di installazione e collaudo del prodotto;
  - siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.
- c) Gestione contrattualistica "ultimo miglio" con provider di servizi Wholesale**
- siano individuati i soggetti preposti alla gestione delle attività di contrattualizzazione con provider di servizi Wholesale al fine acquistare una quota del servizio e di ottenere la massima capillarità sul territorio;
  - siano definiti i ruoli e le responsabilità in relazione alle attività di contrattualizzazione con provider di servizi Wholesale;

- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa delle attività e le stesse siano formalizzate in apposite procedure;
- siano svolte attività di verifica circa la coerenza tra il prezzo autorizzato e riportato nei documenti autorizzativi ed il prezzo contrattualizzato con il Cliente;
- siano svolte attività di verifica circa l'accuratezza della gestione della trattativa/offerta commerciale nelle fasi di stipula del contratto di servizio;
- siano svolte attività di verifica circa la congruenza fra quanto contrattualizzato, quanto collaudato/attestato e quanto fatturato;
- siano svolte attività di monitoraggio e controllo circa il rispetto delle regole di condotta e delle performance previste contrattualmente nei rapporti con le terze parti;
- si prevedano modalità di approvazione delle modifiche/integrazioni alle offerte commerciali da parte di soggetti chiaramente identificati all'interno di procedure aziendali e dotati di adeguato livello autorizzativo;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**d) Gestione dei servizi di housing & colocation (inclusa la sicurezza fisica) all'interno dei Data Center su territorio nazionale ed estero**

- siano individuati i soggetti preposti alla gestione dei servizi di housing e colocation previsti all'interno dei Data Center;
- siano definiti i ruoli e le responsabilità in relazione alle attività di gestione dei servizi di housing e colocation all'interno dei Data Center;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa delle attività e le stesse siano formalizzate in apposite procedure;
- siano svolte periodiche verifiche circa la corrispondenza tra le caratteristiche del servizio erogato e quanto riportato nel relativo materiale tecnico/informativo o comunque su qualsiasi materiale consegnato al cliente o diffuso al pubblico;
- si preveda l'autorizzazione formale preventiva da parte di figure aziendali prima di provvedere alla comunicazione ai clienti in merito a qualità e specifiche del servizio sulla base delle procedure aziendali;
- siano definite le modalità con cui viene svolta l'attività di monitoraggio dei livelli di servizio in termini di efficacia delle tecnologie utilizzate e standard di sicurezza;
- sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio circa il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, tramite l'utilizzo di report e trend sugli incidenti;
- sia adottato e attuato uno strumento normativo che definisca i ruoli, responsabilità e modalità di gestione degli accessi di utenti interni ed esterni alle aree dei Data Center e gli obblighi dei medesimi;
- sia adottato uno strumento normativo che definisca ruoli, responsabilità e modalità per l'identificazione e la classificazione degli assets aziendali presenti nei Data Center;
- sia adottato uno strumento normativo che assicuri la correttezza e sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo preveda:
  - il corretto e sicuro funzionamento degli elaboratori di informazioni;
  - la protezione da software pericolosi;
  - la presenza di strumenti per effettuare la tracciatura delle attività eseguite sulle applicazioni,

sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;

- la verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;

- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**e) Gestione dell'infrastruttura di rete (broadband / ultrabroadband / rete mista), compreso il coordinamento di terze parti per l'implementazione dell'infrastruttura ed erogazione del servizio di connessione**

- siano individuati i soggetti preposti alla gestione dell'infrastruttura di rete, al coordinamento di terze parti per l'implementazione dell'infrastruttura e l'erogazione del servizio;
- siano definiti i ruoli e le responsabilità in relazione alle attività di gestione dell'infrastruttura di rete, al coordinamento di terze parti per l'implementazione dell'infrastruttura e l'erogazione del servizio;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa delle attività e le stesse siano formalizzate in apposite procedure;
- si preveda lo svolgimento di un'attività di verifica circa la necessità di realizzare la tratta in modo autonomo o, alternativamente, acquisire le risorse richieste da un fornitore;
- si preveda il rispetto, nelle fasi di implementazione dell'infrastruttura e di erogazione del servizio, dei principi di trasparenza e oggettività nelle attività svolte in coordinamento con terze parti, laddove previsti;
- si prevedano modalità per l'individuazione dell'operatore economico/realizzatore dell'infrastruttura rete che assicurino la ricerca preliminare tra quelli presenti nell'Albo Fornitori e si preveda, solo in caso di mancata rispondenza dei requisiti sia dal punto di vista tecnico che di affidabilità economico-finanziaria delle società già accreditate presso l'Albo, alla ricerca dell'operatore sul mercato;
- siano svolte adeguate attività di verifica circa la capacità tecnica e finanziaria del fornitore e la sua reputazione sul mercato;
- si preveda l'implementazione di controlli di sicurezza al fine di garantire la riservatezza dei dati all'interno della rete e dei dati in transito su reti pubbliche;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**f) Gestione della Cyber Security e dei servizi di sicurezza informatica (inclusa la gestione delle terze parti necessarie per l'erogazione dei servizi di sicurezza)**

- siano individuati i soggetti preposti alla gestione della cybersecurity;
- siano definiti i ruoli e le responsabilità in relazione alle attività di gestione della cybersecurity;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa delle attività e le stesse siano formalizzate in apposite procedure;
- sia prevista l'implementazione di meccanismi di tracciatura degli eventi di sicurezza sulle reti quali, a titolo esemplificativo, tentativi di accessi, accessi anomali per frequenza, modalità, temporalità ed operazioni su sistemi critici;

- sia prevista la predisposizione di uno strumento normativo aziendale che definisce, tra le altre cose, le attività di back up per ogni rete di telecomunicazione, la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;
- siano previste delle procedure formalizzate per l'implementazione e la manutenzione di reti telematiche che ne regolamentano le responsabilità e le modalità operative, la definizione di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate, l'esecuzione di attività periodiche di vulnerability assessment ed ethical hacking;
- gli accessi del personale alle componenti hardware e software sono definiti in base alle reali necessità delle risorse;
- si prevedano modalità di custodia della password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;
- siano definite, approvate, promanate e rispettate le policy aziendali in merito ai dispositivi antintrusione e antivirus;
- si preveda nei contratti con le terze parti necessarie per l'erogazione dei servizi di cybersecurity a clienti o per l'esecuzione di attività di cybersecurity interna, nell'ambito delle attività di sviluppo software, esercizio applicazioni, manutenzioni, la definizione di controlli e misure necessarie per garantire la sicurezza del servizio, verificandone altresì l'attendibilità commerciale e professionale;
- sia garantita la protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking;
- siano verificate le competenze, l'esperienza e l'affidabilità necessarie da parte dei soggetti nominati Amministratori di Sistema per assolvere le proprie mansioni;
- siano descritte le attività di monitoraggio periodico delle utenze finalizzate alla bonifica di quelle utenze non più necessarie (es. per modifiche organizzative, utenze che ha lasciato l'azienda, ecc.);
- siano definite le regole per garantire la tracciabilità delle attività svolte, e siano supportate da evidenze formali, dallo scambio di informazioni all'interno dell'azienda per la gestione degli accessi logici, account e profili;
- sia richiesta a ciascun fornitore a cui sono affidati servizi di amministrazione di sistema l'elenco delle persone fisiche preposte come Amministratori di Sistema;
- sia tenuta traccia degli accessi anche degli Amministratori di Sistema ai sistemi che trattano dati personali in un apposito access log, di cui sono garantite l'integrità e l'immodificabilità;
- sia data comunicazione ai terzi del Modello 231, dei cui principi si richiede il rispetto attraverso opportune clausole contrattuali, qualora le operazioni oggetto della presente attività siano date in outsourcing;
- siano descritte le misure di sicurezza previste per la gestione sicura e corretta della rete e per la manutenzione della stessa;
- sia descritta l'architettura di rete;
- sia prevista la segregazione logica e, laddove possibile, fisica della rete interna e dalle reti esterne, e siano previste idonee misure di sicurezza e firewall che permettano di ridurre l'esposizione ai rischi (es. connessione delle terze parti, Internet);
- sia prevista la separazione delle reti su cui si attestano sistemi di produzione (reti server) dalle reti cui si connettono gli utenti (reti client) e dalle reti amministrative e siano previsti meccanismi di sicurezza volti a limitare l'accesso unicamente al personale dotato di adeguati profili autorizzativi;
- sia previsto il blocco del traffico amministrativo dei dispositivi connessi a Internet, consentendolo soltanto ad un range dedicato di indirizzi interni;
- sia registrato e conservato in un apposito server ogni tentativo di violazione alle regole dei

firewall delle liste controllo accessi;

- laddove necessario, siano previste restrizioni d'accesso alle connessioni esterne implementate per la connessione punto-punto con clienti e fornitori, in linea con il principio del minimo privilegio; eventuali nuove connessioni siano formalmente richieste e tracciate mediante uno strumento di ticketing e soggette a formale autorizzazione da parte delle Direzioni preposte;
- i log generati contengano almeno data e ora della connessione e attività svolte;
- sia prevista la connessione in VPN per gli utenti che intendano connettersi da remoto alla rete interna; laddove tecnicamente possibile, l'accesso in VPN avvenga mediante meccanismi di autenticazione basati su strong authentication;
- l'accesso alla connessione alla rete WLAN sia consentito unicamente ai soggetti autorizzati, previa autenticazione mediante l'impiego di un protocollo di sicurezza autorizzato, sicuro e affidabile, al fine di minimizzare il rischio di accesso non autorizzato alle risorse di rete;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**g) Gestione dei servizi Cloud (inclusi lo storage Cloud e il servizio multicloud aziendale)**

- siano individuati i soggetti preposti alla gestione delle attività operative del processo di gestione dei servizi Cloud;
- siano definiti i ruoli e le responsabilità in relazione alle attività di gestione dei servizi Cloud;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano svolte attività di monitoraggio da parte del Responsabile di funzione volte a garantire i livelli di servizio e qualità attesi;
- siano svolte attività periodiche volte a verificare la corretta corrispondenza tra le caratteristiche del servizio erogato e quanto riportato nel relativo materiale tecnico/informativo o comunque su qualsiasi materiale consegnato al cliente o diffuso al pubblico;
- siano autorizzate dalle figure aziendali preposte eventuali comunicazioni ai clienti in merito a qualità e specifiche del servizio;
- sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio dei livelli di operatività delle piattaforme, nonché dell'efficacia del servizio Cloud;
- sia adottato e attuato uno strumento che definisca adeguate modalità per il monitoraggio circa il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, tramite l'utilizzo di report e trend sugli incidenti;
- la documentazione prodotta in relazione alle attività di controllo svolte sia archiviata al fine di garantire la tracciabilità del processo;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**h) Gestione attività di scouting fornitori sul mercato (es. individuazione di provider di nuove tecnologie tramite analisi di mercato)**

- siano individuati i soggetti preposti alla gestione delle attività di scouting fornitori sul mercato e di valutazione degli stessi e delle relative tecnologie;
- siano definiti i ruoli e le responsabilità in relazione alle attività di scouting fornitori sul mercato e di valutazione degli stessi e delle relative tecnologie;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi

referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;

- siano definite le modalità di ricerca di potenziali partner commerciali, sia in modo attivo, ricercando gli stessi su internet o attraverso altri canali che in modo passivo, ricevendo richieste di incontro e partecipando ad attività illustrative e dimostrative delle tecnologie proposte (ad esempio, attività di “Proof of Concept”);
- siano definiti criteri oggettivi e trasparenti per l’individuazione e la valutazione svolta circa potenziali partner commerciali e le relative tecnologie proposte;
- siano definite le modalità di comunicazione ad altre funzioni aziendali circa i partner commerciali individuati e le motivazioni sottostanti alle scelte effettuate;
- sia prevista la separazione di funzioni tra coloro che individuano potenziali partners commerciali, coloro che ne controllano l’operato e coloro che registrano le fatture in contabilità e provvedono alla liquidazione dei corrispettivi;
- siano definite le modalità di gestione delle eccezioni al processo standard;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l’attuazione dell’operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell’intero processo e di agevolare eventuali controlli successivi.

**i) Gestione dei servizi a supporto del cliente (c.d. “Managed services”)**

- siano individuati i soggetti preposti alla gestione dei servizi a supporto del cliente (c.d. “Managed Services”);
- siano definiti i ruoli e le responsabilità in relazione alle attività di supporto al cliente (c.d. “Managed Services”);
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano previste le modalità con cui viene erogato di un servizio di assistenza, anche in modalità remota (teleassistenza), a fronte di problematiche circa il servizio erogato;
- siano definite le modalità di gestione e formalizzazione degli interventi svolti negli ambiti di incident & problem management e change management;
- siano definiti adeguati livelli autorizzativi nell’ambito delle attività di supporto al cliente circa la gestione di incident & problem management e change management e gli stessi siano riflessi all’interno dei sistemi informativi in uso al personale della Società;
- sia definito un adeguato sistema di reporting verso il Responsabile della Funzione coinvolta contenente informazioni in merito alla gestione dell’attività svolta, evidenza dei Key Performance Indicator di riferimento e i livelli di servizio contrattualizzati con i clienti (SLA);
- si preveda adeguata segregazione tra coloro che effettuano le attività di gestione operativa nell’ambito dell’incident & problem management e change management e coloro che autorizzano la condivisione delle risultanze di tali attività con i clienti;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l’attuazione dell’operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell’intero processo e di agevolare eventuali controlli successive.

**j) Gestione del magazzino**

- siano individuati i soggetti preposti alla gestione del magazzino;
- siano definiti i ruoli e le responsabilità in relazione all’attività di gestione del magazzino;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi

referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;

- siano definite le modalità per garantire la tracciabilità dei flussi logistici in entrata e in uscita dei magazzini;
- siano definite le modalità di verifica circa la corrispondenza tra ordinato e ricevuto in fase di ricevimento fisico di materiale;
- siano definite le modalità di gestione del magazzino attraverso:
  - soglie di tolleranza che impediscano di effettuare una entrata merce non giustificata da un ordine, per quantitativi superiori diversi a quelli ordinati o superiori eccedenti alle soglie di tolleranza ed eventualmente preimpostate;
  - l'impossibilità di modificare le impostazioni di sistema da parte dei soggetti deputati alla registrazione dell'entrata merci;
  - l'inserimento obbligatorio della data di ricezione al fine del salvataggio dell'entrata merce;
  - la valorizzazione automatica del magazzino e dei relativi scarichi secondo i principi contabili di riferimento;
  - la definizione di un processo formale di attestazione dell'entrata merce e/o dell'avvenuta prestazione/servizio;
  - la verifica della corrispondenza quali/quantitativa tra venduto e spedito in fase di spedizione del materiale da parte del personale addetto;
- sia previsto un sistema di registrazione e monitoraggio della merce spedita ma non ancora arrivata a destinazione;
- sia definito un processo di certificazione dell'avvenuta consegna fisica del prodotto al cliente (es. firma e timbro del foglio di consegna ad evidenza dell'avvenuta delivery);
- sia definita l'attività di monitoraggio dei prelievi e dei consumi di beni e materiali effettuati nelle attività operative interne agli stabilimenti;
- sia definito e predisposto un inventario periodico volto a verificare la corrispondenza della quantità contabile di magazzino con la quantità fisica effettiva in giacenza, che tenga in considerazione la tipologia di bene;
- siano definiti i criteri e le modalità per apportare eventuali rettifiche inventariali con approvazione da parte di personale dotato i adeguati poteri autorizzativi;
- siano individuate le modalità di approvazione e gestione degli inventari, ed eventuali indagini nel caso di mancata corrispondenza tra contabilità e giacenza fisica effettiva nei magazzini;
- siano definite attività di monitoraggio continuo / periodico delle rettifiche inventariali, relativamente al volume e alla significatività delle stesse;
- sia definito un processo di valorizzazione fiscale ai fini del rispetto della metodologia di calcolo del reddito d'impresa delle rimanenze di magazzino;
- nel caso di beni presso terzi, sia garantita l'applicazione delle stesse regole operative e degli stessi criteri gestionali, oltre alla completa e corretta tenuta delle evidenze contabili prescritte dalle norme tributarie nonché di quelle rese necessarie dalla struttura organizzativa;
- sia garantita la segregazione delle funzioni tra chi inserisce i dati di input a sistema, chi effettua le verifiche inventariali periodiche e chi verifica e approva la correttezza degli inventari;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

## 14. Processo “VENDITE”

### 14.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Vendite”. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Vendite dirette alla Pubblica Amministrazione (PAC, PAL, Regioni e altri enti pubblici) mediante la partecipazione a gare e assegnazioni dirette (incluse le assegnazioni MEPA).
- Vendite indirette: Gestione delle attività di vendita di servizi tramite agenzie e procacciatori d'affari e partner commerciali.
- Gestione delle attività di vendita.

### 14.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 319 c.p. Corruzione per un atto contrario ai doveri di ufficio;
- art. 319 ter c.p. Corruzione in atti giudiziari;
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità;
- art. 321 c.p. Pene per il corruttore;
- art. 322 c.p. Istigazione alla corruzione;
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 346 bis Traffico di influenze illecite.

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

#### **Reati transnazionali (art. 10, L. 146/2006):**

- art. 377 bis c.p. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso

#### **Reati Societari (art. 25 ter)**

- art. 2621 c.c. False comunicazioni sociali;
- art. 2622 c.c. False comunicazioni sociali delle società quotate;
- art. 2625 Impedito controllo;
- art. 2629 bis c.c. Omessa comunicazione del conflitto d'interessi;
- art. 2632 c.c. Formazione fittizia del capitale;
- art. 2633 c.c. Indebita ripartizione dei beni sociali da parte dei liquidatori;
- art. 2636 c.c. Illecita influenza sull'assemblea.
- art. 2635 c.c. Corruzione tra privati;
- art. 2635 bis c.c. Istigazione alla corruzione tra privati.

#### **Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art. 25 octies)**

- art. 648 c.p. Ricettazione

- art. 648 bis c.p. Riciclaggio
- art. 648 ter c.p. Impiego di denaro beni o utilità di provenienza illecita
- art. 648 ter 1 c.p. Autoriciclaggio

**Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies)**

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

**Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 duodecies)**

- art. 22, c. 12 D. Lgs 25/07/1998, n. 286 Impiego di lavoratori irregolari

**Reati tributari (art. 25 quinquiesdecies)**

- art 2 D. Lgs 74/2000 Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti
- art. 3 D. Lgs 74/2000 Dichiarazione fraudolenta mediante altri artifici
- art. 4 D. Lgs 74/2000 Dichiarazione infedele
- art. 5 D. Lgs 74/2000 Omessa dichiarazione
- art. 8 D. Lgs 74/2000 Emissione di fatture o altri documenti per operazioni inesistenti
- art. 10 D. Lgs 74/2000 Occultamento o distruzione di documenti contabili
- art. 10 quater D. Lgs 74/2000 Indebita compensazione
- art. 11 D. Lgs 74/2000 Sottrazione fraudolenta al pagamento di imposte

### 14.3. Standard di controllo

#### 14.3.1. Standard di controllo generali

Come riportato in premessa, gli standard di controllo generali sono applicabili al processo Legal & Corporate Affairs, in quanto principi guida del sistema di controllo interno e gestione dei rischi.

#### 14.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

**a) Vendite dirette alla Pubblica Amministrazione (PAC, PAL, Regioni e altri enti pubblici) mediante la partecipazione a gare e assegnazioni dirette (incluse le assegnazioni MEPA)**

- siano individuati i soggetti preposti all'attività di vendita di servizi alla Pubblica Amministrazione;
- siano definiti i ruoli e le responsabilità in relazione all'attività di vendita di servizi alla Pubblica Amministrazione;
- siano definite le modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza;
- si prevedano le modalità di partecipazione a procedure ad evidenza pubblica, che assicurino che tutti dipendenti operino nel rispetto delle leggi, dei regolamenti vigenti e della corretta pratica commerciale;
- sia verificata in ordine alla completezza, veridicità e tempestività la documentazione inviata alla Pubblica Amministrazione;
- siano definiti i livelli di autorizzazione necessari ai fini dell'approvazione del prezzo e degli eventuali sconti e gli stessi siano riflessi all'interno dei sistemi informativi in uso al personale;
- siano definite le modalità di raccolta delle informazioni del cliente e il loro inserimento nel sistema amministrativo contabile (e.g. nome cliente; indirizzo: via, località, paese, regione;

partita IVA; conto di riconciliazione);

- si preveda che le richieste di apertura, integrazione, modifica o cancellazione di un'anagrafica cliente prevengano dalle funzioni aziendali opportunamente individuate e processate da soggetti formalmente incaricati;
- si preveda che le richieste di apertura/integrazione/modifica di una anagrafica siano supportate da idonea documentazione ufficiale ricevuta dal cliente stesso e sia verificata l'esistenza della partita IVA;
- siano preventivamente identificati i soggetti responsabili della predisposizione della proposta di offerta;
- si preveda l'esistenza di segregazione delle funzioni tra i soggetti che predispongono la proposta di offerta e chi effettua la verifica della stessa e tra i soggetti responsabili della negoziazione dei contratti e della loro esecuzione (regolamentando l'intervento di tutte le funzioni coinvolte, anche a livello di Gruppo);
- si preveda che ogni attività di vendita sia supportata da un contratto di vendita/offerta (in cui sono dettagliate le condizioni di vendita, caratteristiche del prodotto/servizio, ecc.) firmato da soggetti dotati di idonei poteri;
- si preveda la verifica di coerenza tra i prezzi concordati in sede di trattativa commerciale con i prezzi di riferimento definiti preventivamente;
- sia prevista l'approvazione formale della proposta d'ordine, previa verifica a sistema della correttezza della stessa;
- sia definito l'iter di verifica ed approvazione delle richieste di modifiche d'ordine avanzate dai clienti;
- sia previsto l'inserimento nei contratti con terze parti, inclusi i clienti e business partner, di apposite clausole di anticorruzione, ove possibile;
- si preveda l'attività di monitoraggio periodico della corretta esecuzione dei contratti, supportato da evidenze formali;
- si preveda, all'interno del sistema informativo (Customer Relationship Management) la formalizzazione in apposite schede di evidenza di tutti i rapporti intercorsi con la Pubblica Amministrazione, come ad esempio e-mail e telefonate;
- sia definito, nell'ambito delle vendite con la PA, un sistema di reporting verso il Responsabile della Funzione coinvolta contenente informazioni in merito ai clienti o potenziali clienti incontrati e all'esito degli incontri;
- siano definiti, nell'ambito delle vendite con la PA, gli incontri periodici con il Responsabile della Funzione coinvolta al fine di condividere le informazioni in merito ai clienti o potenziali clienti incontrati, all'esito degli incontri e ad eventuali situazioni da attenzionare;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

**b) Vendite indirette: Gestione della attività di vendita di servizi tramite agenzie e procuratori d'affari e partner commerciali**

- siano individuati i soggetti preposti alla gestione delle attività di vendita tramite agenzie, procuratori d'affari e partner commerciali;
- siano definiti i ruoli e le responsabilità in relazione all'attività di vendita tramite agenzie, procuratori d'affari e partner commerciali;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;

- siano definite modalità operative per la selezione e qualifica dei partner commerciali, utilizzando gli strumenti di qualificazione che prevedano opportuni parametri di valutazione qualitativa in termini di affidabilità tecnica, finanziaria, commerciale e reputazionale;
- siano preventivamente svolti accertamenti idonei a verificare l'identità, la sede e la natura giuridica della controparte dell'operazione e ne sia acquisito, per le persone fisiche, il casellario giudiziale o una relativa autocertificazione;
- siano definite periodiche attività di aggiornamento (almeno una volta all'anno) delle informazioni raccolte in fase iniziale di impostazione del rapporto con agenzie, procacciatori d'affari o partner commerciali;
- siano definite le modalità per lo svolgimento dell'analisi preliminare, supportata da evidenze formali, degli elementi della richiesta di presentazione di un'offerta da parte del cliente individuato da agenzia, procacciatori d'affari o partner commerciali, finalizzata a valutare la possibilità di avviare o meno l'elaborazione di una proposta di offerta;
- siano definite le modalità di raccolta delle informazioni del cliente e il loro inserimento nel sistema amministrativo contabile (e.g. nome cliente; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione);
- si preveda che le richieste di apertura, integrazione, modifica o cancellazione di un'anagrafica cliente prevengano dalle funzioni aziendali opportunamente individuate e processate da soggetti formalmente incaricati;
- si preveda che le richieste di apertura/integrazione/modifica di una anagrafica siano supportate da idonea documentazione ufficiale ricevuta dal cliente stesso e sia verificata l'esistenza della partita IVA
- Si preveda, nella fase di "Contrattualizzazione dell'agenzia, procacciatore d'affari e partner commerciali", l'utilizzo sistematico di accordi scritti, secondo standard contrattuali redatti dalla funzione Legal o testi da questi approvati e si preveda all'interno di tali contratti:
  - la definizione dei prezzi medi di mercato applicati al servizio di acquisto;
  - una specifica clausola che vincoli dell'agenzia, procacciatore d'affari e partner commerciali all'osservanza dei principi etico-comportamentali adottati dalla Società. La mancata osservanza di tale clausola, da sottoscrivere espressamente, dovrà essere indicata come possibile causa di scioglimento del rapporto contrattuale;
  - l'esclusione dell'utilizzo di clausole ambigue che possano indurre a comportamenti non conformi ai principi etico-comportamentali quali, ad esempio, il riferimento all'adozione di generici provvedimenti atti a superare le criticità nelle procedure autorizzative;
- siano preventivamente identificati i soggetti responsabili della predisposizione della proposta di offerta al cliente;
- si preveda l'esistenza di segregazione delle funzioni tra i soggetti che predispongono la proposta di offerta e chi effettua la verifica della stessa e tra i soggetti responsabili della negoziazione dei contratti e della loro esecuzione (regolamentando l'intervento di tutte le funzioni coinvolte, anche a livello di Gruppo);
- si preveda che ogni attività di vendita sia supportata da un contratto di vendita/offerta (in cui sono dettagliate le condizioni di vendita, caratteristiche del prodotto/servizio, ecc.) firmato da soggetti dotati di idonei poteri;
- si preveda la verifica di coerenza tra i prezzi concordati in sede di trattativa commerciale con i prezzi di riferimento definiti preventivamente;
- sia prevista l'approvazione formale della proposta d'ordine, previa verifica a sistema della correttezza della stessa;
- sia definito l'iter di verifica ed approvazione delle richieste di modifiche d'ordine avanzate dai clienti;

- sia previsto l'inserimento nei contratti con terze parti, inclusi i clienti e business partner, di apposite clausole di anticorruzione, ove possibile;
- si preveda l'attività di monitoraggio periodico della corretta esecuzione dei contratti, supportato da evidenze formali;
- si preveda lo svolgimento di verifiche su clienti individuati da agenzie, procacciatori d'affari e partner commerciali volto a garantire che gli stessi non siano sottoposti a sanzioni a livello internazionale (economic sanctions) che possano precludere il mantenimento dei rapporti commerciali con la Società;
- siano definite le modalità e le tempistiche per lo svolgimento dell'attività di monitoraggio e controllo sull'operato di agenzie, procacciatori d'affari e partner commerciali al fine di valutarne la correttezza delle condotte commerciali rispetto alle policy della Società;
- siano definiti in modo chiaro e trasparente i criteri di attribuzione degli incentivi e delle provvigioni spettanti agli agenti e non siano basati solo sul parametro del maggior venduto, ma anche, a titolo esemplificativo e non esaustivo, sulla fidelizzazione dei clienti, sull'assenza di reclami rispetto all'operato, sul numero di clienti in portafoglio, ecc.;
- si preveda la corrispondenza di provvigioni ad agenti in misura congrua rispetto alla natura e al valore delle transazioni concluse;
- siano previste modalità di pagamento in favore di dealer e di agenti che garantiscano la piena tracciabilità (ad esempio tramite bonifico bancario);
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

### **c) Gestione delle attività di vendita**

- siano individuati i soggetti preposti alla gestione delle attività di vendita;
- siano definiti i ruoli e le responsabilità in relazione all'attività di vendita;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano definite le modalità per lo svolgimento dell'analisi preliminare, supportata da evidenze formali, degli elementi della richiesta di presentazione di un'offerta da parte del cliente, finalizzata a valutare la possibilità di avviare o meno l'elaborazione di una proposta di offerta;
- siano definite le modalità di raccolta delle informazioni del cliente e il loro inserimento nel sistema amministrativo contabile (e.g. nome cliente; indirizzo: via, località, paese, regione; partita IVA; conto di riconciliazione);
- si preveda che le richieste di apertura, integrazione, modifica o cancellazione di un'anagrafica cliente prevengano dalle funzioni aziendali opportunamente individuate e processate da soggetti formalmente incaricati;
- si preveda che le richieste di apertura/integrazione/modifica di una anagrafica siano supportate da idonea documentazione ufficiale ricevuta dal cliente stesso e sia verificata l'esistenza della partita IVA;
- si preveda di effettuare la scelta e valutazione della controparte sulla base di requisiti predeterminati dalla Società, definiti sulla base del profilo economico-patrimoniale ed etico-giuridico;
- siano preventivamente identificati i soggetti responsabili della predisposizione della proposta di offerta;
- si preveda l'esistenza di segregazione delle funzioni tra i soggetti che predispongono la proposta di offerta e chi effettua la verifica della stessa e tra i soggetti responsabili della negoziazione dei

contratti e della loro esecuzione (regolamentando l'intervento di tutte le funzioni coinvolte, anche a livello di Gruppo);

- si preveda che ogni attività di vendita sia supportata da un contratto di vendita/offerta (in cui sono dettagliate le condizioni di vendita, caratteristiche del prodotto/servizio, ecc.) firmato da soggetti dotati di idonei poteri;
- si preveda la verifica di coerenza tra i prezzi concordati in sede di trattativa commerciale con i prezzi di riferimento definiti preventivamente;
- sia prevista l'approvazione formale della proposta d'ordine, previa verifica a sistema della correttezza della stessa;
- sia definito l'iter di verifica ed approvazione delle richieste di modifiche d'ordine avanzate dai clienti;
- sia previsto l'inserimento nei contratti con terze parti, inclusi i clienti e-business partner, di apposite clausole di anticorruzione, ove possibile;
- si preveda l'attività di monitoraggio periodico della corretta esecuzione dei contratti, supportato da evidenze formali;
- si preveda lo svolgimento di verifiche su clienti/terze parti volto a garantire che gli stessi non siano sottoposti a sanzioni a livello internazionale (economic sanctions) che possano precludere il mantenimento dei rapporti commerciali con la Società;
- La Società ha previsto un sistema di reporting verso il Responsabile della Funzione coinvolta contenente informazioni in merito ai clienti o potenziali clienti incontrati, esito degli incontri e principali problematiche emerse;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

## 15. Processo “BUSINESS OPERATION & DEVELOPMENT”

### 15.1. Le attività sensibili rilevanti

Nella presente sezione sono esplicitati i principi di comportamento, nonché gli strumenti di controllo volti a prevenire la commissione dei reati previsti dal Decreto con riferimento alle attività sensibili relative al Processo Sensibile “Business Operation & Development”. Le attività sensibili che sono state ritenute più specificamente a rischio sono le seguenti:

- Definizione della componente tecnica degli elementi di offerta, inclusa l'individuazione e selezione di eventuali partner ("service integrator") e di quantificazione dei costi
- Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione).

### 15.2. Reati applicabili

In relazione alle attività sensibili di cui al paragrafo precedente, i reati considerati potenzialmente realizzabili sono i seguenti:

#### **Reati con la Pubblica Amministrazione (art. 24 e 25)**

- art. 356 c.p. Frode nelle pubbliche forniture
- art. 317 c.p. Concussione
- art. 318 c.p. Corruzione per l'esercizio della funzione
- art. 319 quater c.p. Induzione indebita a dare o promettere utilità;
- art. 20 c.p. Corruzione di persona incaricata di un pubblico servizio;
- art. 321 c.p. Pene per il corruttore;
- art. 322 c.p. Istigazione alla corruzione;
- art. 322 bis c.p. Peculato, concussione, induzione indebita a 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. 346 bis Traffico di influenze illecite.

#### **Reati di criminalità organizzata (art. 24 ter):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso anche straniere

#### **Reati transnazionali (art. 10, L. 146/2006):**

- art. 416 c.p. Associazione per delinquere
- art. 416 bis c.p. Associazioni di tipo mafioso

#### **Reati Societari (art. 25 ter)**

- art. 2621 c.c. False comunicazioni sociali;
- art 2625 Impedito controllo;
- art. 2626 c.c. Indebita restituzione di conferimenti;
- art. 2629 bis c.c. Omessa comunicazione del conflitto d'interessi;
- art. 2632 c.c. Formazione fittizia del capitale;
- art. 2633 c.c. Indebita ripartizione dei beni sociali da parte dei liquidatori;
- art. 2635 c.c. Corruzione tra privati;
- art. 2635 bis c.c. Istigazione alla corruzione tra privati.

#### **Delitti contro la personalità individuale (art. 25 quinquies):**

- art 603 c.p. Intermediazione illecita e sfruttamento del lavoro

### 15.3. Standard di controllo

#### 15.3.1. Standard di controllo generali

Come riportato in premessa, gli standard di controllo generali sono applicabili al processo Legal & Corporate Affairs, in quanto principi guida del sistema di controllo interno e gestione dei rischi.

#### 15.3.2. Standard di controllo specifici

Il Processo e le attività in oggetto, svolti operativamente dalla Capogruppo Retelit S.p.A., sono regolati da specifici accordi intercompany che prevedono una gestione operativa allineata alle best practices e ai seguenti protocolli di controllo, implementati dalla Società che gestisce le attività:

##### **a) Definizione della componente tecnica degli elementi di offerta, inclusa l'individuazione e selezione di eventuali partner ("service integrator") e di quantificazione dei costi**

- siano individuati i soggetti preposti alla gestione delle attività di definizione della componente tecnica degli elementi di offerta;
- siano definiti i ruoli e le responsabilità in relazione all'attività di definizione della componente tecnica degli elementi di offerta;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite procedure;
- siano individuati i referenti di progetto/commissa incaricati dell'analisi tecnica in funzione dei requisiti professionali, tecnici e delle esperienze maturate;
- siano definite le modalità standard con cui il personale della funzione svolge le attività di stima e quantificazione dei costi per la realizzazione dei progetti;
- siano definite, in caso di collaborazioni con partner esterni alla Società (ad esempio "service integrator") le modalità e i criteri per la verifica preventiva dei presupposti di carattere strategico, tecnico-economico e finanziario nonché dell'attuabilità dell'operazione;
- siano previste modalità di selezione dei partner sulla base di criteri oggettivi che tengano conto degli aspetti tecnici necessari per la definizione della componente tecnica e degli aspetti economico-finanziari necessari per garantire la solidità economico-finanziaria della controparte;
- siano definite le modalità con cui il personale formalizza la scelta del partner all'interno dei sistemi informativi (ad esempio, nel Customer Relationship Management);
- sia definito un processo strutturato per le attività di definizione della componente tecnica di offerta, suddiviso per specifiche fasi rilevanti, per ognuna delle quali sia prevista la predisposizione di specifica documentazione, flussi informativi verso gli organi gerarchici superiori ed eventualmente l'autorizzazione degli stessi per il passaggio alla fase successiva;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

##### **b) Partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani per l'esecuzione di forniture o altre operazioni similari (incluse le procedure di gara del Mercato elettronico della Pubblica Amministrazione)**

- siano individuate le funzioni e i soggetti incaricati di avere rapporti con i pubblici ufficiali o incaricati di pubblico servizio, nonché le funzioni e i soggetti preposti alla gestione della partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani;
- siano definiti i ruoli e le responsabilità in relazione alla gestione delle attività operative circa la partecipazione a procedure di gara, o di negoziazione diretta, indette da enti pubblici italiani;
- siano definite modalità operative interne, funzioni coinvolte e flussi informativi tra i diversi referenti coinvolti nella gestione operativa del servizio e le stesse siano formalizzate in apposite

procedure;

- sia identificata la Funzione Competente responsabile di intrattenere rapporti con esponenti della Pubblica Amministrazione sia in fase di predisposizione della proposta di offerta sia in fase di presentazione della stessa;
- siano definite le modalità di gestione dei rapporti con le Istituzioni nazionali e locali nonché con altri enti pubblici, improntate alla trasparenza, alla lealtà e alla correttezza;
- si prevedano le modalità di partecipazione a procedure ad evidenza pubblica, che assicurino che tutti dipendenti operino nel rispetto delle leggi, dei regolamenti vigenti e della corretta pratica commerciale;
- siano definite le modalità con cui è svolta l'analisi preliminare di fattibilità tecnica ed economica volta a verificare la capacità della Società di eseguire i lavori nei tempi e nelle modalità previste dal bando di gara o dall'invito a partecipare ovvero di subappaltare le attività di esecuzione ad un operatore terzo;
- si preveda l'autorizzazione formale preventiva da parte del Responsabile di funzione all'utilizzo dei dati e di informazioni destinati ad atti, comunicazioni, attestazioni e richieste di qualunque natura inoltrate o aventi come destinatario la PA;
- siano definiti i livelli di autorizzazione necessari relativamente a offerte e contratti e gli stessi siano riflessi all'interno dei sistemi informativi in uso al personale;
- siano definite modalità per la conservazione della documentazione ad opera del Responsabile interno per l'attuazione dell'operazione, in un apposito archivio, con modalità tali da impedire la modifica successiva, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.