

AMSIC s.r.l.

MODELLO ORGANIZZATIVO DI GESTIONE E CONTROLLO, EX D.LGS. 231/2001

PARTE SPECIALE

REV. 00 – 12.10.2024

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 2 di 53

INDICE

1.	RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE.....	6
1.1.	Individuazione del rischio – le attività sensibili	6
1.2.	Ipotesi di reati presupposto verificabili	7
1.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	8
1.4.	Soggetti ed aree coinvolte nella gestione del processo	8
1.5.	Sistema di controllo e gestione del rischio nel processo “rapporti con la PA”	8
1.5.1.	Regole generali	8
1.5.2.	Protocolli specifici.....	9
1.6.	Flussi informativi e attività dell’Organismo di Vigilanza (OdV)	11
2.	GESTIONE DEI FLUSSI MONETARI E FINANZIARI	13
2.1.	Individuazione del rischio – attività sensibili.....	13
2.2.	Ipotesi di reati presupposto verificabili	13
2.3.	Punti critici ed ipotetica modalità di commissione dei reati presupposto.....	14
2.4.	Soggetti ed aree coinvolte nella gestione del processo	14
2.5.	Sistema di controllo relativo al processo di gestione dei flussi monetari e finanziari	14
2.5.1.	Regole generali	14
2.5.2.	Protocolli specifici.....	15
2.6.	Flussi informativi e attività dell’Organismo di Vigilanza.....	16
3.	PROCESSO PER LA GESTIONE AMMINISTRATIVA-CONTABILE E ADEMPIMENTI FISCALI	17
3.1.	Individuazione del rischio – le attività sensibili	17
3.2.	Ipotesi di reato verificabili ai sensi del d .lgs. 231/01.....	17
3.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	18
3.4.	Soggetti ed aree coinvolte nella gestione del processo	19
3.5.	Sistema di controllo e gestione del rischio nel processo “gestione amministrativa-contabile e adempimenti fiscali”	19
3.5.1.	Regole Generali	19
3.5.2.	Protocolli specifici.....	20
3.6.	Flussi informativi ed attività dell’Organismo di Vigilanza.....	21
4.	GESTIONE DEI RAPPORTI CON CONSULENTI E PROFESSIONISTI TERZI	22
4.1.	Individuazione del rischio – attività sensibili.....	22
4.2.	Ipotesi di reato astrattamente verificabili.....	22
4.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	23
4.4.	Soggetti ed aree coinvolte nella gestione del processo	23
4.5.	Sistema di controllo in relazione al processo “rapporti con consulenti e professionisti terzi”	23

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 3 di 53

4.5.1.	Regole generali	23
4.5.2.	Protocolli specifici.....	24
4.6.	Flussi informativi ed attività dell’Organismo di Vigilanza.....	25
5.	GESTIONE CONTRATTI CON SOGGETTI PUBBLICI E PRIVATI	27
5.1.	Individuazione del rischio – attività sensibili.....	27
5.2.	Ipotesi di reato astrattamente verificabili.....	27
5.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	28
5.4.	Soggetti coinvolti nella gestione del processo	29
5.5.	Sistema di controllo relativo al processo di gestione dei contratti con soggetti pubblici e privati	29
5.5.1.	Regole Generali	29
5.5.2.	Protocolli specifici.....	30
5.6.	Flussi informativi ed attività dell’Organismo di Vigilanza.....	32
6.	DONAZIONI, LIBERALITÀ E OMAGGI.....	34
6.1.	Individuazione del rischio – attività sensibili.....	34
6.2.	Ipotesi di reati presupposto verificabili.....	34
6.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	34
6.4.	Soggetti ed aree coinvolte nella gestione del processo	35
6.5.	Sistema di controllo relativo al processo di donazioni, liberalità e omaggi	35
6.5.1.	Regole generali	35
6.5.2.	Protocolli specifici.....	35
6.6.	Flussi informativi ed attività dell’Organismo di Vigilanza.....	36
7.	GESTIONE DEI RIMBORSI SPESE, ANTICIPI E DELLE SPESE DI RAPPRESENTANZA	37
7.1.	Individuazione dei rischi – attività sensibili.....	37
7.2.	ipotesi di reati presupposto verificabili.....	37
7.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	37
7.4.	Soggetti ed aree coinvolte nella gestione del processo	37
7.5.	Sistema di controllo in relazione al processo “gestione dei rimborsi spese e delle spese di rappresentanza”	38
7.5.1.	Regole generali	38
7.5.2.	Protocolli specifici.....	38
7.6.	Flussi informativi ed attività dell’Organismo di Vigilanza.....	38
8.	SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE	39
8.1.	Individuazione dei rischi – attività sensibili.....	39
8.2.	Ipotesi di reato astrattamente verificabili.....	39
8.3.	Punti Critici ed ipotetica modalità di commissione dei reati presupposto	39
8.4.	Soggetti ed aree coinvolte nella gestione del processo	40

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 4 di 53

8.5.	Sistema di controllo relativo al processo di selezione, assunzione e gestione del personale	40
8.5.1.	Regole generali	40
8.5.2.	Protocolli specifici.....	41
8.6.	Flussi informativi e attività dell’Organismo di Vigilanza.....	41
9.	PROCESSO PER LA GESTIONE DELLA SALUTE E SICUREZZA SUI LUOGHI DI LAVORO	42
9.1.	Individuazione del rischio – attività sensibili	42
9.2.	Ipotesi di reato verificabili	42
9.3.	Punti critici ed ipotetica modalità di commissione dei reati presupposto.....	42
9.4.	Soggetti ed aree operative coinvolte nella gestione del processo.....	42
9.5.	Sistema di controllo interno relativo al processo di gestione della salute e sicurezza sui luoghi di lavoro	42
9.5.1.	Regole generali	42
9.5.2.	Protocolli specifici.....	44
9.6.	Flussi informativi e attività dell’Organismo di Vigilanza.....	45
10.	GESTIONE DEL SERVIZIO DI INTERMEDIAZIONE DEI RIFIUTI	46
10.1.	Individuazione del rischio – attività sensibili	46
10.2.	Ipotesi di reati presupposto verificabili	46
10.3.	Punti critici ed ipotetica modalità di commissione dei reati presupposto.....	47
10.4.	Soggetti ed aree operative coinvolte nella gestione del processo.....	47
10.5.	Sistema di controllo relativo al processo per la gestione delle attività di pulizia e raccolta, trasporto, smaltimento e trattamento dei rifiuti	47
10.5.1.	Regole generali	47
10.5.2.	Protocolli specifici.....	48
10.6.	Flussi informativi e attività dell’Organismo di Vigilanza.....	48
11.	GESTIONE DEI SISTEMI INFORMATICI.....	50
11.1.	Individuazione del rischio – attività sensibili	50
11.2.	Ipotesi di reati presupposto verificabili	50
11.3.	Punti critici ed ipotetica modalità di commissione dei reati presupposto.....	50
11.4.	Soggetti ed aree coinvolte nella gestione del processo	51
11.5.	Sistema di controllo relativo al processo di gestione dei sistemi informatici	51
11.5.1.	Regole generali	51
11.5.2.	Protocolli specifici.....	52
11.6.	Flussi informativi e attività dell’Organismo di vigilanza	53

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 5 di 53

TABELLA DELLE REVISIONI E DEGLI AGGIORNAMENTI	
REV. 00 – 12.10.2024	Prima Emissione

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 6 di 53

1. RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Il presente processo ha ad oggetto i rapporti e le occasioni di contatto che si possono instaurare con la PA: Stato ed Enti Locali ed Istituzioni UE, Enti Ispettivi, Enti Previdenziali, Forze dell'ordine, Autorità Giudiziaria ed altri soggetti qualificabili come Pubblici Ufficiali ovvero incaricati di pubblico servizio.

Valutazioni generali in relazione ad i rapporti con la Pubblica Amministrazione

Il processo sensibile individua i profili potenziali di rischio di reato in relazione ai rapporti che la società intrattiene con la Pubblica Amministrazione. Si osserva che ai fini del Modello appartengono alla Pubblica Amministrazione tutti quei soggetti, pubblici o privati, che svolgono una "funzione pubblica" o un "pubblico servizio" ai sensi degli artt. 357 e 358 del Codice Penale.

Per **funzione pubblica** si intende l'esercizio delle attività, disciplinate da norme di diritto pubblico, attinenti alla funzione legislativa, amministrativa e giudiziaria. La funzione pubblica è caratterizzata dall'esercizio del potere autoritativo e del potere certificativo. Colui che "esercita una pubblica funzione legislativa, giudiziaria o amministrativa" è qualificato, ai sensi dell'art. 357 c.p., quale "pubblico ufficiale".

Per **pubblico servizio** si intende, invece, l'esercizio delle attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'Autorità Pubblica o l'esercizio delle attività volte a garantire i diritti fondamentali della persona, quali quello alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione, etc. Il pubblico servizio è un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri autoritativi e certificativi. Colui che "a qualunque titolo presta un pubblico servizio" è qualificato, ai sensi dell'art. 358 c.p., quale "persona incaricata di un pubblico servizio".

1.1. Individuazione del rischio – le attività sensibili

Il processo in esame si articola nelle seguenti attività, che pur non presentando rischi diretti di rilevanza penale, se combinate con le attività direttamente sensibili, possono comportare la realizzazione del reato presupposto e sono quindi funzionali alla condotta illecita.

Ai sensi dell'art. 6 del Decreto, sono state individuate dalla società le attività sensibili nell'ambito delle quali possono essere commessi i reati di cui agli artt. 24 e 25 del Decreto:

- **i rapporti con uffici, organi, funzioni, Enti della P.A.**, nell'ambito di procedimenti amministrativi, **partecipazione a gare pubbliche ed affidamenti**, nonché nell'ambito di **attività di ispezione e controllo** svolte dagli apparati pubblici sull'attività aziendale; si tratta di attività che possono identificarsi in singole Operazioni a Rischio, definite nel tempo ed individuabili separatamente;
- **i rapporti con la P.A. collegati alla specifica attività aziendale**, relativi principalmente alle verifiche e autorizzazioni da parte della P.A., necessarie all'azienda per lo svolgimento della specifica attività aziendale;
- **i rapporti con la P.A. collegati alla richiesta e fruizione di finanziamenti o benefici erogati dallo Stato, la Comunità Europea e altri Enti pubblici locali, nazionali o comunitari.**

Particolare attenzione va prestata nelle seguenti attività:

- **i rapporti con i vari uffici della pubblica amministrazione per l'ottenimento di permessi, concessioni, autorizzazioni iscrizione all'Albo Nazionale dei Gestori Contabili o altri provvedimenti abilitativi;**
- i rapporti con i servizi della pubblica amministrazione di **ispezione e vigilanza** (ambientale, amministrativa, fiscale, previdenziale, sanitaria etc.);
- i rapporti con l'amministrazione della giustizia nell'ambito o in occasione di **procedimenti giudiziari** di natura civile, amministrativa, tributaria e penale, che coinvolgano la società;
- l'avvio e la gestione di procedure per l'ottenimento di **erogazioni o contributi** da parte delle PP.AA. italiane o comunitarie e la gestione dei fondi eventualmente erogati;

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 7 di 53

- la **produzione di documentazione** alla P.A., anche attraverso i mezzi informatici;
- gestione dei rapporti con l'amministrazione della giustizia nell'ambito o in occasione di procedimenti giudiziari di natura giuslavoristica che coinvolgano la società;
- ricerca e sviluppo di nuovi prodotti o soluzioni tecniche (quali ad es. macchinari aziendali sviluppati internamente e destinati ad essere utilizzati in aziende terze);
- la trasmissione di dati in via informatica a soggetti pubblici, ad esempio all'Agenzia delle Entrate o agli Enti previdenziali o assicurativi, o comunque l'elaborazione e la trasmissione di documenti aventi efficacia probatoria.

Nel corso della mappatura delle attività sensibili per i reati contro la Pubblica Amministrazione sono state inoltre evidenziate le seguenti attività strumentali, il cui svolgimento potrebbe, potenzialmente, rappresentare un mezzo per la commissione di un Reato Presupposto contro la Pubblica Amministrazione (ad es. creando fondi da utilizzare per finalità corruttive):

- la selezione ed assunzione di personale dipendente;
- gestione delle risorse finanziarie della società (incassi e pagamenti);
- gestione delle carte di credito corporate, note spese e anticipi;
- gestione di sponsorizzazioni;
- gestione di dotazioni e utilità aziendali (es. computer, telefoni, autovetture etc.);
- gestione dei rapporti con i fornitori ed i clienti

1.2. Ipotesi di reati presupposto verificabili

- Reati di cui all'art. 24 d.lgs 231/01:
 - Art. 316 bis c.p. "malversazione a danno dello stato"
 - art. 316 ter c.p. "indebita percezione di erogazioni a danno dello stato";
 - art. 353 c.p. "turbata libertà degli incanti";
 - art. 353 bis c.p. "Turbata libertà del procedimento di scelta dei contraenti";
 - art. 356 c.p. "frode nelle pubbliche forniture";
 - art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche";
- Reati di cui all'art. 25 d.lgs 231/01:
 - Art. 314 c.p. "peculato";
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
 - Art. 346 bis "traffico di influenze illecite"
- Reati di cui all'art. 24 ter d.lgs 231/01:
 - art. 416 c.p. "associazione per delinquere";
 - art. 416 bis "associazioni di tipo mafioso anche straniere";
 - art. 416 ter "scambio elettorale politico – mafioso";
- Reati di cui all'art. 25 decies d.lgs 231/01:
 - Art 377 bis c.c. "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria"
- Reati tributari di cui all'art. 25 quinquiesdecies
 - Artt. 2 e ss. D. Lgs. 74/2000

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 8 di 53

1.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

La società è esposta al rischio dei reati presupposto sopra indicati nelle seguenti ipotesi:

- a) nell’ambito della partecipazione ad una gara pubblica ovvero nella procedura per ottenere finanziamenti pubblici, prospettare una realtà aziendale difforme da quella reale al fine di ottenere un indebito vantaggio;
- b) accordarsi con il dirigente un Ufficio Pubblico al fine di dare/ricevere/promettere denaro o altra utilità per compiere un atto contrario ai doveri del pubblico ufficiale per ottenere un vantaggio indebito;
- c) utilizzare violenza, minaccia, promesse, regali o altri mezzi fraudolenti per non consentire il regolare svolgimento delle gare pubbliche;
- d) nell’ambito di un accertamento o accesso ispettivo da parte delle Forze dell’Ordine o Enti Ispettivi, dare/promettere denaro o altra utilità al fine di ottenere un vantaggio indebito;
- e) nella gestione di procedimenti giudiziari, dare/promettere utilità al fine di essere favoriti o danneggiare una parte processuale;
- f) associarsi con tre o più persone allo scopo di commettere più delitti (anche contro la PA) utilizzando, eventualmente la forza dell’intimidazione mafiosa;
- g) accettare la promessa di procurare supporti elettorali a soggetti riconducibili ad associazioni mafiose, in cambio di indebita utilità;

1.4. Soggetti ed aree coinvolte nella gestione del processo

Nell’ambito del presente processo sono coinvolti i seguenti soggetti:

- AU
- Area Amministrativa Contabile
- Area Commerciale

1.5. Sistema di controllo e gestione del rischio nel processo “rapporti con la PA”

1.5.1. Regole generali

L’elaborazione del presidio muove, innanzitutto, dalla specifica necessità di sterilizzare le occasioni di commissione di reati corruttivi.

Infatti, gli illeciti corruttivi mostrano una maggiore pericolosità rispetto alle altre figure delittuose analizzate, dovuta alla tendenziale inafferrabilità-imprevedibilità *ex ante* delle controprestazioni illecite, che rende di fatto più arduo pronosticare le possibili modalità realizzative.

Ciò suggerisce l’opportunità di arretrare il più possibile le operazioni di *risk management*, preferendo invece **misure di allontanamento** dal rischio-illiceità.

A tale scopo, tutti i Destinatari del Modello, come individuati dalla Parte Generale, adottano regole di comportamento conformi ai principi di seguito elencati, nello svolgimento o nell’esecuzione delle operazioni nell’ambito delle attività sensibili e strumentali indicate nel paragrafo precedente, al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione rilevanti per la società e previsti dal Decreto.

In generale, si stabiliscono i seguenti principi di comportamento da rispettare nell’adempimento delle attività sensibili.

È fatto divieto a tutti i Destinatari del Modello di:

- intrattenere rapporti con la Pubblica Amministrazione, in rappresentanza o per conto della società, in mancanza di apposita delega o procura della società stessa;
- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, anche acquisite al di fuori della propria realtà professionale, al

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 9 di 53

fine di influenzarne le decisioni, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del settore, erogazione di contributi/finanziamenti pubblici e/o simili informazioni;

- offrire denaro o altra utilità a Pubblici Ufficiali o incaricati di Pubblico Servizio o organi o funzionari dell’Autorità Giudiziaria, inclusi i familiari degli stessi, al fine di influenzarne la discrezionalità, l’indipendenza di giudizio o per indurli ad assicurare un qualsiasi vantaggio alla società, oppure allo scopo di ottenere specifiche informazioni sugli sviluppi futuri del settore e/o erogazione di contributi/finanziamenti pubblici e/o simili informazioni;
- riconoscere, in favore di fornitori o collaboratori esterni, o loro familiari, che operino nei confronti della Pubblica Amministrazione in nome e per conto della società, compensi indebiti che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- corrispondere e/o proporre la corresponsione e/o chiedere a terzi di proporre la corresponsione o dazione di denaro o altra utilità a un pubblico funzionario dell’Autorità Giudiziaria, o suoi familiari, nel caso in cui la società sia parte di un procedimento giudiziario;
- conferire incarichi professionali, dare o promettere doni, danaro, o altri vantaggi a chi effettua gli accertamenti e le ispezioni, autorità pubbliche ovvero ad organi dell’Autorità Giudiziaria;
- ricorrere a forme di contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze, pubblicità, configurino, invece, forme di doni o regalie verso pubblici funzionari, loro familiari, enti e autorità pubbliche; presentare dichiarazioni, comunicazioni o documenti contenenti informazioni non veritiere, fuorvianti o parziali alla Pubblica Amministrazione, ovvero omettere informazioni, al fine di ottenere provvedimenti favorevoli dalla Pubblica Amministrazione (ad es. per ottenere il rilascio di concessioni o autorizzazioni, finanziamenti pubblici);
- destinare a finalità diverse da quelle per le quali sono stati concessi contributi, sovvenzioni o finanziamenti o altra erogazione dello stesso tipo ottenuti dallo Stato o da altro ente pubblico o dall’Unione Europea.

In particolare, inoltre:

- le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione e realizzazione, nonché di controllo;
- l’Azienda regola la propria politica retributiva e di carriera tenendo in debita considerazione la correttezza e legalità dei comportamenti, penalizzando ogni comportamento che tenda al raggiungimento di obiettivi a discapito del rispetto delle regole aziendali o legali;
- qualsiasi rapporto con funzionari pubblici è corretto, formale ed attento alle molteplici implicazioni che da esso possono derivare;
- l’assunzione di personale dipendente avviene secondo criteri oggettivi di individuazione delle necessità aziendali e delle corrispondenti capacità e titoli individuali, con processo condiviso da più funzioni aziendali che contribuiscono alla scelta dei candidati nel rispetto dei predetti criteri;
- l’opportunità di accesso a finanziamenti e contributi pubblici è individuata sulla base della effettiva presenza di tutti requisiti legali richiesti; una volta ottenuto il beneficio, lo stesso è utilizzato esclusivamente nell’ambito e per le finalità individuati dal provvedimento di erogazione, nel rispetto di tutte le modalità attuative previste, fornendo alla P.A. competente una rendicontazione trasparente, completa e veritiera delle attività finanziate svolte;
- le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Sezione sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella Parte Generale del presente Modello.

1.5.2. Protocolli specifici

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 10 di 53

L’obiettivo della gestione dei rischi individuati nel presente processo sensibile si raggiunge, oltre che con l’osservanza delle regole di portata generale, con l’adempimento di regole più specifiche contenute in mirati protocolli e procedure adottati dalla società.

Le regole contenute nei protocolli e procedure diventano vincolanti per i Destinatari del Modello, i quali sono passibili di sanzione disciplinare in caso di inosservanza.

Di seguito si enunciano i presidi fondamentali da rispettare per eliminare ovvero ridurre il rischio dei reati presupposto individuati nel processo “rapporti con la PA”.

Presidio per ottenimento licenze, concessioni, autorizzazioni, finanziamenti e contributi

- Nella **Fase della Predisposizione Documentale**, l’AU ovvero il dipendente formalmente incaricato predispone i documenti necessari, al fine di garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell’istanza di autorizzazione o fornite in esecuzione degli adempimenti o delle attività di monitoraggio, prevedendo, ove opportuno, specifici controlli
- Nella **Fase della Verifica della Documentazione predisposta**, l’AU ovvero il dipendente formalmente incaricato garantisce effettua un controllo sulla correttezza delle elaborazioni da parte del referente/responsabile di riferimento
- Nella **Fase della Trasmissione della documentazione richiesta e archiviazione della pratica**, l’AU ovvero il dipendente formalmente incaricato di inviare o trasmettere richieste, dati o informazioni, in nome e per conto della società ad enti pubblici se privo di deleghe formali, deve essere individuato e autorizzato tramite delega interna, che deve essere archiviata. La delega deve definire in modo specifico ed inequivocabile i poteri del delegato, il soggetto cui il delegato riporta gerarchicamente ed eventualmente gli altri soggetti ai quali le deleghe sono congiuntamente o disgiuntamente conferite.

Presidio nell’ambito di verifiche e visite ispettive

Nell’ambito di **Verifiche ed ispezioni da parte dell’Ente Pubblico**, gli elementi specifici di controllo si basano su livelli autorizzativi definiti, sulla separazione di ruolo nelle fasi chiave del processo, sulla registrazione e sulla tracciabilità delle attività e sulla valutazione complessiva del processo.

Solamente i soggetti muniti di idonei poteri sono autorizzati a interloquire con i rappresentanti degli Enti autorizzativi e di controllo in occasione di verifiche ispettive.

Eventualmente, ulteriori soggetti possono entrare in contatto con i rappresentanti della P.A. in occasione di visite e ispezioni purché espressamente individuati e autorizzati tramite delega interna, che deve essere archiviata.

La tracciabilità è garantita tramite la registrazione e l’archiviazione degli atti e dei documenti (es. verbale di ispezione, copie della documentazione fornita, etc.) inerenti ogni specifica verifica o ispezione, a cura dei soggetti che hanno assistito alla verifica.

La valutazione complessiva avviene tramite la rendicontazione dell’attività svolta, richiesta dalla società a tutti i soggetti che hanno assistito alla verifica.

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 11 di 53

Al fine di poter effettuare una valutazione complessiva dell'attività svolta, la Società richiede a tutti i soggetti che gestiscono rapporti con la PA, di rendicontare periodicamente in merito alle attività svolte.

Presidio per la gestione degli investimenti e del progetto finanziato con fondi pubblici

La Società deve specificare se vi son soggetti diversi dall'AU per lo svolgimento della seguente attività istruttoria:

- Raccogliere e mettere a disposizione del vertice aziendale tutte le informazioni relative all'investimento o alla spesa da sostenere, attraverso l'ottenimento di fondi pubblici, in modo puntuale, corretto e veritiero
- Archiviare la suddetta documentazione al fine di consentire un'accurata verifica nel tempo
- la presentazione della domanda entro i termini previsti
- la funzione preposta, una volta accertato l'esito del finanziamento ed ottenuti gli estremi della delibera dell'ente preposto alla loro concessione, deve avviare l'investimento o la spesa entro i termini previsti e, eventualmente qualora concesso dal "bando", rinunciare alla domanda presentata su altra fonte di finanziamento agevolata

qualora l'AU incarichi formalmente un dipendente, quest'ultimo deve:

- Attivarsi per ottenere, in itinere, tutte le informazioni tecniche, economiche e finanziarie necessarie
- Informare, periodicamente, l'AU circa l'andamento del progetto in termini di impiego delle risorse finanziarie, stato del progetto, analisi degli eventuali scostamenti, etc.
- deve predisporre la documentazione ed i dati richiesti dall'ente erogatore, secondo la tempistica e modalità previste dal bando

Gestione del progetto finanziato

- Tutti i soggetti diversi dall'AU che, in fase di richiesta e gestione di finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della società, devono essere formalmente autorizzati in tal senso;
- I soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società (es. pratiche di richiesta, istanze, rinnovo delle autorizzazioni, etc.) devono essere formalmente delegati in tal senso (con idonea procura, se trattasi di un dipendente della Società o, nel caso di professionista esterno, tramite espressa previsione nel contratto)
- Qualora sia previsto il coinvolgimento di Società esterne nella predisposizione delle pratiche di richiesta, nella gestione del finanziamento o nella successiva esecuzione di attività connesse con i progetti finanziati, i contratti con tali Società devono contenere apposita dichiarazione di conoscenza del modello organizzativo adottato dal AMSIC e di impegno al suo rispetto.

1.6. Flussi informativi e attività dell'Organismo di Vigilanza (OdV)

In relazione al presente processo sensibile, l'AU ed i dipendenti dovranno informare l'OdV periodicamente attraverso uno specifico report riguardo gli aspetti significativi afferenti alle diverse attività del processo di propria competenza, in particolare per quanto attiene:

- La documentazione relativa alle pratiche inoltrate per l'ottenimento di licenze, autorizzazioni, afferente l'esecuzione di finanziamenti
- Elenco soggetti autorizzati per richiesta e gestione di finanziamenti o contributi alla P.A.
- Elenco società esterne coinvolte nella gestione delle pratiche e successive attività connesse

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 12 di 53

- Esiti di verifiche ed ispezioni da parte gli enti pubblici

La Società, inoltre, ha l’obbligo di comunicare immediatamente all’OdV ogni deroga alle procedure di processo decisa in caso di emergenza oppure di impossibilità temporanea di attuazione, indicando la motivazione ed ogni anomalia significativa riscontrata.

L’Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, delle fasi di ciascun processo che implichi un contatto con la P.A., evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L’Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello, fermo restando il dovere di osservare il divieto di comunicare e/o diffondere le informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste da forze di polizia, dall’autorità giudiziaria, da organismi di sicurezza o da altri soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 13 di 53

2. GESTIONE DEI FLUSSI MONETARI E FINANZIARI

Il processo si riferisce alle attività riguardanti i flussi monetari e/o finanziari in entrata e in uscita aventi l'obiettivo di adempiere le obbligazioni ed incassare i crediti di varia natura della Società.

I flussi monetarie finanziari sono connessi alle attività eseguite dalla Società, quali ad esempio, acquisti di beni, servizi e licenze, oneri finanziari, fiscali e previdenziali, stipendi e salari.

Il processo per i flussi in uscita si articola nelle seguenti fasi:

- **Richiesta di pagamento**
- **Verifica dei presupposti per disporre il pagamento**
- **Disposizione del pagamento**
- **Verifica dei flussi di cassa in uscita ed archiviazione della documentazione**

Il processo per i flussi in entrata si articola nelle seguenti fasi:

- **Verifica dei presupposti per richiedere il pagamento**
- **Calcolo ed emissione della fattura per le attività svolte**
- **Analisi dei crediti e verifica delle scadenze di incasso**
- **Verifica dei flussi di cassa in ingresso e archiviazione della documentazione**

2.1. Individuazione del rischio – attività sensibili

- Apertura, chiusura e gestione dei conti correnti bancari
- Predisporre bonifici bancari
- Gestione delle operazioni della piccola cassa
- Verifiche di quadratura periodiche
- Effettuare riconciliazioni bancarie
- Registrare le presenze/ferie/malattie del personale dipendente ai fini dell'elaborazione dei salari
- elaborare i cedolini paghe mensili, gli oneri contributi
- archiviazione dei documenti fiscali e registrazione in contabilità

2.2. Ipotesi di reati presupposto verificabili

- Reati di cui all'art. 25 d.lgs 231/01:
 - art. 316 ter c.p. "indebita percezione di erogazioni a danno dello stato";
 - art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche";
- Reati di cui all'art. 25 dlgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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"

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 14 di 53

- Reati di cui all'art. 25 oties.1 d.lgs 231/01 "delitti in materia di strumenti di pagamento diversi dai contanti":
 - Art. 493 ter c.p.: "indebito utilizzo e falsificazione di carte di credito e di pagamento";
 - Art. 493 quater c.p.: "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti";
- Reati di cui all'art. 25 quinquiesdecies "reati tributari":
 - Art. 2 d.lgs 74/00 "dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti";
 - Art. 2 d.lgs 74/00 "dichiarazione infedele";
 - Art. 3 d.lgs 74/00 "dichiarazione fraudolenta mediante altri artifici";
 - Art. 5 d.lgs 74/00 "omessa dichiarazione";
 - Art. 8 d.lgs 74/00 "emissione di fatture o altri documenti per operazioni inesistenti";
 - Art. 10 d.lgs 74/00 "occultamento o distruzione di documenti contabili";
 - Art. 10-quater d.lgs 74/00 "indebita compensazione";
 - Art. 11 d.lgs 74/00 "sottrazione fraudolenta al pagamento di imposte"

2.3. Punti critici ed ipotetica modalità di commissione dei reati presupposto

Nell'esecuzione delle attività sensibili si rilevano i seguenti punti critici:

- Ottenere un finanziamento o altro tipo di erogazione per eseguire un progetto difforme da quello oggetto della richiesta di finanziamento
- Gestire i flussi di denaro in entrata ed in uscita in modo da creare dei fondi neri illeciti, destinati a fini corruttivi;
- "impiegare" (inteso come acquisto, ricezione, occultamento, trasferimento) di denaro, beni o utilità provenienti da delitto;
- Emettere una fattura per un servizio di intermediazione non reso al produttore o detentore del rifiuto
- Pattuire con l'impianto di trattamento un importo "gonfiato" da comunicare al produttore/detentore del rifiuto, in modo da ottenere dal titolare dell'impianto un qualsiasi tipo di vantaggio illecito
- Utilizzare una fattura emessa per un servizio di intermediazione inesistente o parzialmente inesistente per dichiarare costi fittizi nelle dichiarazioni periodiche
- Concedere l'utilizzo di carte di credito a soggetti creditori come forma di remunerazione

2.4. Soggetti ed aree coinvolte nella gestione del processo

Nel presente processo sono coinvolte le seguenti figure:

- AU
- Area Amministrativa Contabile
- Area Commerciale

2.5. Sistema di controllo relativo al processo di gestione dei flussi monetari e finanziari

2.5.1. Regole generali

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 15 di 53

È fatto divieto di:

- effettuare prestazioni in favore di persone (anche familiari), partners o fornitori che non trovino adeguata giustificazione nel contesto del rapporto costituito;
- riconoscere compensi in favore dei collaboratori e consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- ricevere o sollecitare elargizioni in denaro, omaggi, regali o vantaggi di altra natura, nell'ambito dell'esercizio delle proprie funzioni aziendali, ove eccedano le normali pratiche commerciali e di cortesia;
- intrattenere rapporti commerciali o avviare progetti promozionali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- emettere fatture per operazioni inesistenti, sovrappagamenti o sottopagamenti;
- presentare dichiarazioni incomplete o, comunque, non veritiere ad organismi pubblici nazionali, Regionali o comunitari, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- impiegare somme ricevute da organismi pubblici Regionali, nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per finalità diverse da quelle cui erano destinate.

2.5.2. Protocolli specifici

Il sistema di controllo è strutturato sugli elementi qualificanti nelle diverse fasi del processo, tali da definire la tracciabilità degli atti.

Le attività di pagamento e incasso devono essere tempestivamente e correttamente registrate, deve rimanere traccia scritta dei seguenti dati:

- Data di pagamento e/o incasso
- Data valuta, in caso di bonifico
- Tipo pagamento
- Soggetto che effettua il pagamento a favore di AMSIC

Gestione della cassa

La gestione della cassa è assegnata formalmente all'AU. Diversi soggetti possono essere incaricati di compiere operazione di cassa, avendo cura di specificare poteri e attività a questi consentite.

I valori di cassa, composti da contanti, valori bollati ed assegni, devono essere custoditi in una cassetta di sicurezza, sotto la responsabilità della risorsa incaricata.

L'accesso alla cassetta di sicurezza è consentito esclusivamente all'AU e a diverso soggetto incaricato.

I valori di cassa vengono utilizzati dall'AU o da diverso soggetto incaricato per effettuare i pagamenti per le spese postali e le necessità quotidiane presso la sede della Società, nonché per il pagamento di bollettini postali riferiti a sanzioni, pagamenti in contrassegno, etc., prelevando dalla cassa il relativo importo.

Tutte le operazioni di cassa devono essere documentate da appositi giustificativi e sono registrate.

Con cadenza periodica, i movimenti sono registrati nella contabilità ordinaria.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 16 di 53

Gestione dei conti correnti bancari

L'autorizzazione all'apertura o alla chiusura di un conto corrente bancario o postale è di competenza dell'AU.

I conti correnti della Società vengono controllati e visualizzati dall'AU o da soggetti espressamente autorizzati/incaricati.

L'AU o soggetti espressamente autorizzati/incaricati possono compiere movimentazioni finanziarie tramite conto corrente, dopo aver verificato la copertura finanziaria.

La documentazione di supporto relativa ad ogni singola disposizione effettuata deve essere archiviata.

Archiviazione e verifiche di quadratura

La documentazione, completa di ogni dettaglio, dovrà essere archiviata da un soggetto incaricato.

Con cadenza periodica, un soggetto espressamente incaricato effettua delle verifiche di quadratura in relazione alle registrazioni effettuate e ai rendiconti bancari.

In caso di discrasia tra i dati bancari e quelli della Società devono essere effettuati gli approfondimenti e le verifiche del caso.

Presidio di prevenzione rispetto ai reati di riciclaggio

In tutte le fasi del processo, qualora si palesino notizie che evidenzino la potenziale sussistenza di proventi da delitti in azienda, gli importi equipollenti dovranno essere accantonati per evitarne il reimpiego fino a quando non si chiudano i controlli destinati a confermare o meno l'esistenza di dette provviste, previa informativa all'Organismo di Vigilanza.

Gli importi accantonati nella disponibilità della Società potranno essere liberati a seguito delle definizioni e chiusure dei relativi ed eventuali contenziosi.

2.6. Flussi informativi e attività dell'Organismo di Vigilanza

I soggetti coinvolti nella gestione dei rischi del presente processo devono comunicare all'organismo di vigilanza, con periodicità definita, quanto segue:

- Rendiconto mensile dei pagamenti in contanti effettuati oltre il limite legale oppure oltre il limite imposto d eventuali provvedimento emessi dalle Autorità
- Pagamenti ricevuti tramite assegno circolare
- Elenco dei soggetti autorizzati alle movimentazioni monetarie/finanziarie
- Verifiche di quadrature

In ogni caso, l'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 17 di 53

3. PROCESSO PER LA GESTIONE AMMINISTRATIVA-CONTABILE E ADEMPIMENTI FISCALI

Il presente processo sensibile ha ad oggetto le attività di natura amministrativa, sia ordinarie che straordinarie, con particolare riguardo alla corretta tenuta della contabilità ed ai conseguenti adempimenti fiscali.

3.1. Individuazione del rischio – le attività sensibili

Il processo in oggetto si articola nelle seguenti attività sensibili:

- Gestione fatture emesse per servizi resi;
- Gestione fatture da pagare per gli acquisti/spese effettuati;
- Gestione dei pagamenti occasionali e del fondo cassa a disposizione dei dipendenti;
- Pagamenti dei dipendenti e dei professionisti;
- acquisizione, registrazione, elaborazione, valutazione ed illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali;
- gestione della documentazione, archiviazione e conservazione delle informazioni relative all'attività di impresa, anche attraverso i mezzi informatici;
- predisposizione e trasmissione delle dichiarazioni fiscali
- pagamento delle imposte e degli oneri previdenziali e assistenziali

3.2. Ipotesi di reato verificabili ai sensi del d.lgs. 231/01

- Reati di cui all'art. 25 d.lgs 231/01:
 - art. 316 ter c.p. "indebita percezione di erogazioni a danno dello stato";
 - art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche";
- Reati di cui all'art. 25 d.lgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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 di cui all'art. 25 oties.1 d.lgs 231/01 "delitti in materia di strumenti di pagamento diversi dai contanti":
 - Art. 493 ter c.p.: "indebito utilizzo e falsificazione di carte di credito e di pagamento";
 - Art. 493 quater c.p.: "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti";
 - Art. 512 bis c.p. "Trasferimento fraudolento di valori"
- Reati di cui all'art. 25 quinquiesdecies "reati tributari":
 - Art. 2 d.lgs 74/00 "dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti";
 - Art. 2 d.lgs 74/00 "dichiarazione infedele";
 - Art. 3 d.lgs 74/00 "dichiarazione fraudolenta mediante altri artifici";

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 18 di 53

- Art. 5 d.lgs 74/00 “omessa dichiarazione”;
- Art. 8 d.lgs 74/00 “emissione di fatture o altri documenti per operazioni inesistenti”;
- Art. 10 d.lgs 74/00 “occultamento o distruzione di documenti contabili”;
- Art. 10-quater d.lgs 74/00 “indebita compensazione”;
- Art. 11 d.lgs 74/00 “sottrazione fraudolenta al pagamento di imposte”

3.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

Nell'esecuzione delle attività sensibili del presente processo si rilevano i seguenti punti critici:

- a) Rappresentare una realtà aziendale al fine di ottenere indebitamente sovvenzioni e/o finanziamenti pubblici;
- b) Concedere l'utilizzo di carte di credito o altri strumenti di pagamento a soggetti non autorizzati come forma indebita di remunerazione;
- c) Gestire i flussi di denaro in entrata ed in uscita in modo da creare dei fondi neri illeciti, destinati a fini corruttivi;
- d) Omettere di effettuare le dichiarazioni ai fini del pagamento delle imposte entro i termini di legge;
- e) Effettuare pagamenti in difformità a quanto previsto dai contratti di servizi
- f) Effettuare una dichiarazione ai fini del pagamento delle imposte non veritiera, esponendo fatture per operazioni inesistenti, altri artifici ovvero simulando l'alienazione di beni per evitare le procedure di riscossione dell'Erario;
- g) Trasferire fittiziamente a terzi la disponibilità di beni e/o denaro;
- h) nell'ambito della gestione amministrativa-contabile, porre in essere le seguenti condotte idonee a provocare un danno nei confronti dei creditori:
 - esporre nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni idonee ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della società, con l'intenzione di ingannare i soci o il pubblico;
 - omettere, con la stessa intenzione, informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge;
 - ostacolare, mediante occultamento di documenti o altri artifici idonei, lo svolgimento delle attività di controllo attribuite ai soci e agli altri organi sociali;
 - Esporre nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento, in tutto o in parte, con altri mezzi fraudolenti di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.
- i) nell'ambito di acquisti “impiegare” (inteso come acquisto, ricezione, occultamento, trasferimento) di denaro, beni o utilità provenienti da delitto.
- j) al fine di evadere le imposte sui redditi o sul valore aggiunto, compiere atti fraudolenti mediante artifici utili a far apparire una realtà diversa da quella reale; al fine di evadere le imposte sui redditi o sul valore aggiunto, omettere una delle dichiarazioni relative a dette imposte; al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emettere o rilasciare fatture o altri documenti per operazioni inesistenti; occultare o distruggere documenti contabili di cui è obbligatoria la conservazione; utilizzare in compensazione crediti non spettanti non versando le somme dovute; alienare i propri beni al fine di rendere inefficace la procedura di riscossione coattiva.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 19 di 53

3.4. Soggetti ed aree coinvolte nella gestione del processo

I soggetti e le aree coinvolte nella gestione del presente processo sono:

- AU
- Area Amministrativa Contabile
- Area Commerciale

3.5. Sistema di controllo e gestione del rischio nel processo “gestione amministrativa-contabile e adempimenti fiscali”

3.5.1. Regole Generali

L’AU ed i dipendenti ovvero i suoi consulenti nell’ambito delle funzioni ad essi attribuiti hanno l’obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate. In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l’obbligo di:

- porre in essere correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività finalizzate alle dichiarazioni periodiche ai fini delle imposte, alla formazione del bilancio e delle altre comunicazioni sociali, onde fornire una informazione veritiera e completa sulla situazione economica, patrimoniale e finanziaria della società; in particolare è fatto divieto di:
- rappresentare o trasmettere per l’elaborazione delle dichiarazioni periodiche e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi, fuorvianti o, comunque, non rispondenti alla realtà;
- omettere dati o informazioni imposti dalla legge e dai regolamenti sulla situazione economica, patrimoniale e finanziaria;
- rispettare le disposizioni di legge, i principi contabili e le regole aziendali, ponendo la massima attenzione, professionalità ed accuratezza, nella acquisizione, elaborazione, valutazione ed illustrazione dei dati e delle informazioni necessarie alla predisposizione del bilancio e delle altre comunicazioni sociali;

In particolare, è fatto divieto di:

- porre in essere comportamenti che impediscano materialmente, mediante l’occultamento di documenti o l’uso di altri mezzi fraudolenti, o comunque che ostacolino lo svolgimento dell’attività di controllo;
- osservare scrupolosamente le norme a tutela dei creditori e della integrità ed effettività del capitale sociale;
- tenere comportamenti che, mediante il mancato tempestivo aggiornamento della documentazione, la mancata corretta conservazione o l’occultamento dei documenti impediscano alle autorità ed agli organi di vigilanza di effettuare le dovute attività di controllo.

A ciò si aggiunge che la società deve effettuare:

- monitoraggio documentato dei flussi di cassa, di cui dovrà essere garantita la tracciabilità, ed a cui sono abbinate procedure interne aziendali finalizzate a garantire la genuinità e veridicità di quanto rappresentato nelle comunicazioni sociali nonché nelle dichiarazioni fiscali;
- predisporre un’anagrafica fornitori, svolgimento di verifiche sull’operatività dei fornitori, verifiche sui prezzi di acquisto, verifiche delle prestazioni ricevute, congruità delle fatture;
- predisporre un’anagrafica clienti, verifica delle prestazioni effettuate, definizione di procedure di *pricing*;
- verificare operazioni societarie e rispondenza con la realtà, verifica dei soggetti coinvolti, verifica della documentazione a supporto delle operazioni;

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 20 di 53

- individuazione delle funzioni aziendali incaricate della tenuta e verifica delle stesse, verifiche periodiche sulla corretta tenuta delle scritture contabili.

3.5.2. Protocolli specifici

Il presidio specifico è stato effettuato considerando la necessità di sterilizzare le occasioni di commissione di reati presupposto.

I rischi ai quali la società è esposta, infatti, possono essere correttamente ed utilmente mitigati dall'adozione di specifiche procedure interne, che interessano innanzitutto la fase di elaborazione dei documenti fondamentali per la contabilità (es. emissione di fatture).

L'obiettivo primario, infatti, è poter fare affidamento sulla veridicità dei documenti prodotti, che si mostrano necessari per l'attività di rendicontazione.

Solo successivamente, si interviene a regolarizzare la fase c.d. dichiarativa, ossia quella fase che si sostanzia nelle dichiarazioni periodiche verso l'Erario, bilanci e comunicazioni sociali.

In generale, il rischio che può derivare dalla commissione dei reati presupposto viene gestito attraverso la **segregazione delle funzioni**.

In particolare, la c.d. *segregation of duties* può concretizzarsi sia in senso verticale che orizzontale.

In senso verticale il principio riguarda la necessità di evitare conflitti di interesse, separando le funzioni operative dalle funzioni di controllo: una stratificazione della funzione controllante garantisce il corretto funzionamento dei processi.

In senso orizzontale, invece, la separazione dei compiti implica che bisogna ripartire i ruoli e le responsabilità di un processo fra più soggetti, per evitare che si verifichi un'eccessiva concentrazione delle attività in capo ad un solo operatore.

Presidio sulla formazione del bilancio e delle comunicazioni sociali

- Identificazione dei soggetti incaricati della predisposizione e verifica della documentazione per la redazione del bilancio e chiara definizione delle rispettive funzioni
- Esporre ai soggetti incaricati le norme che definiscano con chiarezza i principi contabili da adottare per **la definizione delle poste di bilancio civilistico e le modalità operative per la loro contabilizzazione**
- Specificare i dati e le notizie da fornire alle funzioni incaricate in relazione alle chiusure annuali e infrannuali (per il bilancio civilistico), con chiara definizione delle modalità e delle tempistiche
- Qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, deve essere previsto che la funzione preposta informi tempestivamente l'Organismo di Vigilanza
- I documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività a rischio sopra indicate, nonché quelli che danno attuazione alle decisioni devono essere archiviati e conservati a cura della funzione competente per l'operazione
- La trasmissione delle informazioni deve essere consentita alle sole persone autorizzate e avvenire attraverso mezzi tecnici che garantiscano la sicurezza dei dati e la riservatezza delle informazioni
- I soggetti incaricati coinvolti nella formazione del bilancio ovvero altre comunicazioni sociali devono redigere una relazione asseverando la veridicità, la coerenza e la completezza delle informazioni trasmesse

Presidio sulla emissione e pagamento delle fatture

- Accertare che gli ordini dei servizi siano effettuati per iscritto o comunque in modo da garantire la tracciabilità del processo

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 21 di 53

- Verificare la corrispondenza quantitativa e qualitativa tra l'ordine ed il servizio di intermediazione
- Nel caso di servizi da rendere alla clientela, prima di emettere la fattura o richiesta di pagamento, accertare quanto svolto
- Tutta la documentazione contabile/fiscale deve essere archiviata in modo corretto ed ordinato ed utilizzata ai fini delle dichiarazioni periodiche

Presidio sulla fase del calcolo delle imposte e sulle dichiarazioni periodiche verso l'Erario

- La funzione incaricata dell'archiviazione della documentazione contabile/fiscale deve redigere una relazione asseverando la veridicità, la coerenza e la completezza dei documenti archiviati, necessari ai soggetti incaricati per il calcolo delle imposte
- Devono essere formalmente incaricati Dipendenti della Società ovvero i Consulenti/Professionisti abilitati alla predisposizione delle dichiarazioni periodiche ai fini del pagamento delle imposte
- Verificare il corretto versamento delle imposte effettuato

3.6. Flussi informativi ed attività dell'Organismo di Vigilanza

In aggiunta ai report periodici da indirizzare all'Organismo di Vigilanza, la società e tutti i Destinatari del Modello sono obbligati a mantenere informato l'Organismo di Vigilanza:

- dati o saldi anomali ed eventuali chiarimenti forniti da consulenti esterni;
- dettagli su cartelle di pagamento o dichiarazioni fiscali irregolari.
- apertura o chiusura di contratti di leasing, finanziamenti o mutui, locazioni;
- esito di verifiche ed ispezioni da parte delle Autorità competenti.

Tutti i Destinatari garantiscono all'Organismo di Vigilanza libero accesso a tutta la documentazione aziendale rilevante.

Le verifiche dell'Odv potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 22 di 53

4. GESTIONE DEI RAPPORTI CON CONSULENTI E PROFESSIONISTI TERZI

Il processo concerne i rapporti con i partners, i consulenti ed i professionisti terzi che collaborano nell'esecuzione dell'attività di redazione giornalistica.

La Società determina e applica criteri per la valutazione, selezione, monitoraggio delle prestazioni, in conformità ai migliori standard professionali.

4.1. Individuazione del rischio – attività sensibili

I rischi del presente processo si individuano nelle seguenti attività:

- gestione degli incarichi conferiti ai consulenti e professionisti terzi
- pagamento dei consulenti e professionisti per l'attività svolta

4.2. Ipotesi di reato astrattamente verificabili

- Reati di cui all'art. 24 d.lgs 231/01:
 - Art. 316 bis c.p. "malversazione a danno dello Stato"
 - Art. 316 ter c.p. "indebita percezione di erogazioni a danno dello Stato"
 - Art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche"
- Reati di cui all'art. 24 ter d. lgs. 231/01:
 - Art. 416 c.p. "associazione per delinquere"
 - Art. 416 bis c.p. "associazioni di tipo mafioso anche straniere"
 - art. 416 ter "scambio elettorale politico – mafioso"
- Reati di cui all'art. 25 dlgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
 - Art. 346 bis c.p. "traffico di influenze illecite"
- Reati di cui all'art. 25 bis.1 d. lgs. 231/01:
 - Art. 513 bis c.p. illecita concorrenza con minaccia o violenza
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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 di cui all'art. 25 octies 1 d.lgs 231/01:
 - Art. 493 ter c.p. "indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti"
 - Art 493 quater c.p. "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"
 - Art 640 ter c.p. "Frode informatica"
- Reati di cui all'art. 25 duodecies dlgs 231/01 "impiego di cittadini di paesi terzi il cui soggiorno è irregolare":
 - Art. 22, comma 12 – bis, d.lgs 25 luglio 1998, n. 286 (T.U. immigrazione);
- Reati di cui all'art. 25 terdecies d. lgs. 231/01 "Razzismo e xenofobia"

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 23 di 53

- Reati di cui all'art. 25 quinquiesdecies d. lgs. 231/01:
 - Art. 2 d.lgs. 74/00 “dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti”
 - Art 3 d.lgs. 74/00 “ delitto di dichiarazione fraudolenta mediante altri artifici”
 - Art. 8 d. lgs. 74/00 “emissione di fatture per operazioni inesistenti”
 - Art. 10 d.lgs 74/00 “occultamento o distruzione di documenti contabili”

4.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

La Società è esposta al rischio dei reati presupposto sopra indicati nelle seguenti ipotesi:

- a) nell’ambito di una procedura per la concessione o erogazione da parte dello Stato, di altri enti pubblici o dalle Comunità europee, di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, eseguire acquisti e/o altre operazioni diverse da quelle per le quali il finanziamento è stato ottenuto;
- b) accordarsi con i consulenti ovvero i professionisti terzi per eseguire una serie indeterminata di illeciti a vantaggio della società (es. reati tributari, reati di corruzione)
- c) attestare falsamente come eseguito l’incarico assegnato ad un professionista
- d) assegnare un incarico ad un professionista solo perché vicino ad associazioni criminali allo scopo di ottenerne protezione
- e) scegliere consulenti e professionisti allo scopo di procurare supporti elettorali a soggetti riconducibili ad associazioni mafiose;
- f) tramite le figure dei professionisti e dei consulenti, dare/ricevere/promettere denaro o altra utilità per compiere un atto contrario ai doveri del pubblico ufficiale per ottenere un vantaggio indebito
- g) gestire operazioni che per caratteristiche, entità o natura o per qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell’attività svolta dal soggetto cui è riferita, inducano a ritenere – in base agli elementi a disposizione ed utilizzando la normale diligenza – che il denaro, i beni o le utilità oggetto delle operazioni medesime possano provenire da delitto;
- h) gestire i rapporti con la concorrenza con violenza minaccia o altre intimidazioni dirette o tramite soggetti terzi;
- i) concedere l’utilizzo di carte di credito o altri sistemi di pagamento diversi dai contanti, abilitando sistemi di prelievo, al fine di mascherare una transazione;
- j) aderire a politiche dei fornitori di tipo razzista o xenofobe o comunque difforni dalle regole del codice etico aziendale;
- k) emettere e/o utilizzare fatture per prestazioni inesistenti o parzialmente inesistenti.

4.4. Soggetti ed aree coinvolte nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento delle seguenti figure:

- AU
- Area Amministrativa Contabile

4.5. Sistema di controllo in relazione al processo “rapporti con consulenti e professionisti terzi”

4.5.1. Regole generali

Tutte le attività sensibili devono essere svolte conformandosi alle leggi vigenti e al codice etico nonché alle procedure aziendali, ai valori e alle regole contenute nel Modello.

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 24 di 53

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza e comunicazione e specificazione dei ruoli, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative, la società dovrà prevedere non solo un controllo di tipo formale sulla regolarità della documentazione del consulente/professionista al momento dell'affidamento dell'incarico, bensì un controllo di tipo concreto nel momento dell'esecuzione delle attività.

Di seguito le regole di portata generale:

- Deve essere effettuata un'adeguata attività selettiva fra i diversi professionisti/operatori di settore
- Devono essere utilizzati idonei dispositivi contrattuali adeguatamente formalizzati
- Prevedere livelli autorizzativi (in coerenza con il sistema di procure e deleghe aziendale) per il conferimento dell'incarico ai consulenti/professionisti e la stipulazione dei contratti
- Prevedere due livelli di controllo diversi per la sottoscrizione del contratto col consulente/professionista e per la certificazione/validazione del servizio reso
- Prestabilire i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e di meccanismi di valutazione complessiva del servizio reso
- Nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la PA, devono essere previsti dei meccanismi di verifica preventiva dell'assenza di contemporanea collaborazione sulla medesima materia con le stesse amministrazioni pubbliche (per esempio mediante autocertificazione del consulente esterno)
- Nei contratti con fornitori e consulenti deve essere 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 dal presente Modello.
- Nei contratti di fornitura, deve essere inserita esplicitamente la "clausola 231" per l'accettazione dei principi e delle regole previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto
- Devono esistere documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati

4.5.2. Protocolli specifici

Il processo sensibile in analisi si articola nella seguenti fasi:

- Conferimento dell'incarico di consulenza/prestazione professionale
- Esecuzione dei servizi
- Pagamento

Gli elementi specifici da controllare nelle fasi/attività del processo sono:

- Due Diligence requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti
- Quale condizione per intrattenere rapporti contrattuali con AMSIC, si deve effettuare una accurata "**due diligence anticorruzione**" preventiva al conferimento dell'incarico. A tal fine possono essere utilizzati i seguenti indici di attenzione:
 - sottoposizione a procedimento per l'applicazione di misure di prevenzione, ai sensi della normativa antimafia;

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 25 di 53

- applicazione di misure cautelari coercitive nell’ambito di un procedimento penale o pronuncia di sentenza di condanna, ancorché non definitiva, compresa quella prevista dall’art. 444 c.p.p., nei confronti di imprenditori, soci, amministratori o dipendenti di imprese, per reati che incidono sull’affidabilità professionale e, tra questi, per i delitti contro la Pubblica Amministrazione, per partecipazione o concorso esterno nei reati associativi, per i delitti di usura, estorsione, ricettazione, riciclaggio, impiego di beni provenienti da delitti e per altre figure delittuose che assumono rilievo nell’ambito della criminalità organizzata;
 - applicazione di misure cautelari nell’ambito di un procedimento penale e pronuncia di sentenza di condanna, ancorché non definitiva, compresa quella emessa su richiesta delle parti, nei confronti di enti, ai sensi del D.lgs. 231/2001, per reati contro la Pubblica Amministrazione, reati contro la persona, reati di riciclaggio e di associazione a delinquere di natura transnazionale, e per altre figure di reato che assumono rilievo nell’ambito della criminalità organizzata;
 - costituzione di enti nei quali figurano, come soci, amministratori o gestori, persone (o prossimi congiunti) che partecipano o abbiano partecipato alle imprese od enti nelle situazioni indicate ai punti precedenti, ovvero manifestamente sprovvisti, per età o formazione, dei requisiti indispensabili per l’esercizio dell’attività imprenditoriale;
 - imprese che siano da ritenere, sulla base di elementi di fatto, costituite soltanto allo scopo di occultare o favorire soggetti appartenenti a gruppi criminali o, comunque, di eludere divieti nello svolgimento di attività imprenditoriali;
 - imprese od enti che risultino privi di rapporti con aziende di credito;
 - intervento, nelle trattative commerciali, di persone od enti privi di legittimazione ad interloquire nelle trattative medesime;
 - mancata esibizione di documenti comprovanti l’iscrizione ad albi, ordini, elenchi, qualora l’iscrizione sia requisito necessario per lo svolgimento dell’attività.
- valutazione di diversi offerenti e comparazione delle relative offerte (sulla base di criteri oggettivi e documentabili); in assenza di tale attività selettiva dare evidenziazione formale delle ragioni della deroga ed esecuzione da parte del responsabile di una valutazione sulla congruità del compenso pattuito (rispetto agli standard di mercato)
 - predisporre ed utilizzare idonei dispositivi contrattuali adeguatamente formalizzati. Per consulenze svolte da soggetti terzi incaricati di rappresentare la società deve essere prevista una specifica “clausola 231” che li vincoli all’osservanza dei principi etico - comportamentali adottati dalla stessa
 - Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

4.6. Flussi informativi ed attività dell’Organismo di Vigilanza

Le funzioni incaricate per la gestione dei rischi del presente processo dovranno, per quanto di propria competenza e con periodicità definita, informare l’Organismo di vigilanza riguardo:

- Piano delle consulenze/incarichi professionali e relativi aggiornamenti
- attività di consulenza e di partership
- Elenco dei rapporti di consulenza e partership in deroga alle regole del Modello

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 26 di 53

Fermo restando il potere discrezionale dell’OdV di attivarsi con specifici controlli in seguito alle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l’OdV effettua periodicamente controlli a campione, sulle attività potenzialmente a rischio del reato di cui alla presente Parte Speciale, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere.

A tal fine all’OdV viene garantito - nel rispetto della normativa vigente, per esempio in tema di privacy - libero accesso a tutta la documentazione aziendale rilevante.

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 27 di 53

5. GESTIONE CONTRATTI CON SOGGETTI PUBBLICI E PRIVATI

Il presente processo ha ad oggetto i rapporti che AMSIC instaura con soggetti pubblici e privati nello svolgimento delle attività sensibili.

La scelta e l'individuazione dei soggetti con cui intrattenere rapporti commerciali è ispirata a criteri di fiducia, esperienza e capacità del fornitore, nonché in relazione al tipo e qualità del prodotto che lo stesso offre.

La Società determina e applica criteri per la valutazione, selezione, monitoraggio delle prestazioni e per la valutazione dei fornitori, sulla base della loro capacità di fornire prodotti e servizi conformi ai migliori standard professionali.

5.1. Individuazione del rischio – attività sensibili

- Individuazione dell'impianto di smaltimento/trattamento dei rifiuti e richiesta dell'offerta economica per il conferimento dei rifiuti
- Individuazione del trasportatore dei rifiuti
- Predisposizione dell'offerta al produttore/detentore dei rifiuti
- Evasione dell'ordine/esecuzione del contratto

5.2. Ipotesi di reato astrattamente verificabili

- Reati di cui all'art. 24 d.lgs 231/01:
 - Art. 316 bis c.p. "malversazione a danno dello Stato"
 - Art. 316 ter c.p. "indebita percezione di erogazioni a danno dello Stato"
 - art. 353 c.p. "turbata libertà degli incanti";
 - art. 353 bis c.p. "Turbata libertà del procedimento di scelta dei contraenti";
 - art. 356 c.p. "frode nelle pubbliche forniture";
 - Art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche"
- Reati di cui all'art. 24 ter d. lgs. 231/01:
 - Art. 416 c.p. "associazione per delinquere"
 - Art. 416 bis c.p. "associazioni di tipo mafioso anche straniere"
 - art. 416 ter "scambio elettorale politico – mafioso"
- Reati di cui all'art. 25 d.lgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
 - Art. 346 bis c.p. "traffico di influenze illecite"
- Reati di cui all'art. 25 bis1 d.lgs 231/01:
 - art. 513 c.p. "turbata libertà dell'industria o del commercio"
 - art. 513 bis c.p. illecita concorrenza con minaccia o violenza
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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 di cui all'art. 25 octies 1 d.lgs 231/01:

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 28 di 53

- Art. 493 ter c.p. “indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti”
- Art 493 quater c.p. “Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti”
- Art 640 ter c.p. “Frode informatica”
- Art. 512 bis c.p. “trasferimento fraudolento di valori”
- Reati di cui all’art. 25 undecies d.lgs 231/01
 - Art. 452 bis c.p. “Inquinamento ambientale”;
 - Art. 452 quater c.p. “disastro ambientale”
 - Art. 452 quinquies c.p. “delitti colposi contro l’ambiente”
 - Art. 452 sexies c.p. “traffico e abbandono di materiale ad alta radioattività”
 - Art. 452 quaterdecies c.p. “attività organizzate per il traffico illecito di rifiuti”
 - Art. 733 bis c.p. “distruzione o deterioramento di habitat all’interno di un sito protetto”
 - Art, 137, d. lgs. 152/06 “Reati in materia di scarichi di acque reflue
 - Art. 256 D.Lgs. 152/06 “attività di gestione non autorizzata”
 - Art. 258 D.Lgs. D.Lgs. 152/06 “violazione degli obblighi di comunicazione, tenuta dei registri e dei formulari”
 - Art. 259 D.Lgs. 152/06 “traffico illecito di rifiuti”
 - Art. 260 bis D.Lgs. 152/06 “Sistema informatico di controllo della tracciabilità dei rifiuti”
- Reati di cui all’art. 25 terdecies d. lgs. 231/01 “Razzismo e xenofobia”
- Reati di cui all’art. 25 quinquiesdecies d. lgs. 231/01:
 - Art. 2 d.lgs. 74/00 “dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti”
 - Art 3 d.lgs. 74/00 “ delitto di dichiarazione fraudolenta mediante altri artifici”
 - Art. 8 d. lgs. 74/00 “emissione di fatture per operazioni inesistenti”
 - Art. 10 d.lgs 74/00 “occultamento o distruzione di documenti contabili”

5.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

La Società è esposta al rischio dei reati presupposto sopra indicati nelle seguenti ipotesi:

- nell’ambito di una procedura per la concessione o erogazione da parte dello Stato, di altri enti pubblici o dalle Comunità europee, di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, eseguire acquisti e/o altre operazioni diverse (per qualità e quantità) da quelle per le quali il finanziamento è stato ottenuto;
- promettere denaro o altre utilità, ovvero utilizzare minaccia o violenza, per condizionare il contenuto del bando di gara ovvero per escludere altri partecipanti;
- nei confronti delle imprese concorrenti del settore, utilizzare violenza, minaccia o altre intimidazioni dirette o tramite soggetti terzi al fine di ottenere l’incarico per il servizio di intermediazione;
- trasferire fittiziamente la disponibilità o la titolarità di beni della Società a creditori o altri soggetti, qualificando l’operazione come forma di retribuzione, al fine di eludere le norme in materia di misura di prevenzione patrimoniale;
- concedere l’utilizzo di carte di credito o altri sistemi di pagamento diversi dai contanti, abilitando sistemi di prelievo, al fine di mascherare una transazione;
- concludere contratti per il servizio di intermediazione dei rifiuti, senza richiedere preventivamente al produttore/detentore dei rifiuti i documenti attestanti la regolarità della loro attività (es. autorizzazioni, analisi chimiche, compilazione dei FIR, etc.)

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 29 di 53

- nella individuazione degli impianti di trattamento/smaltimento, omettere di richiedere le autorizzazioni necessarie per la gestione del ciclo dei rifiuti;
- nell’ambito dei rapporti con i clienti ricevere beni o utilità di dubbia provenienza lecita;
- accordarsi per sovrappagare una fornitura in modo da esporre nelle dichiarazioni periodiche fiscali dei costi superiori rispetto a quelli reali.

5.4. Soggetti coinvolti nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento delle seguenti figure:

- AU
- Area Amministrativa Contabile
- Area Commerciale

5.5. Sistema di controllo relativo al processo di gestione dei contratti con soggetti pubblici e privati

5.5.1. Regole Generali

L’AU ed i dipendenti di AMSIC nonché i consulenti nell’ambito delle funzioni ad essi attribuiti hanno l’obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l’obbligo di osservare che:

- i dati e le informazioni su clienti, fornitori e consulenti siano completi e aggiornati, in modo da garantire la corretta e tempestiva individuazione dei medesimi e una puntuale valutazione e verifica del loro profilo;
- la Società, ai fini dell’attuazione delle decisioni di impiego delle risorse finanziarie, si avvalga soltanto di intermediari finanziari e bancari sottoposti a una regolamentazione di trasparenza e correttezza conformi alla disciplina dell’Unione Europea.

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di sono oggetto di segnalazione da parte di tutti i dipendenti secondo le modalità previste dal presente Modello.

- è necessario procedere all’identificazione dei soggetti privati con cui si gestiscono rapporti commerciali nei seguenti casi:
 - instaurazione di un rapporto commerciale;
 - quando vi è sospetto che i beni ricevuti siano di provenienza illecita;
 - quando vi sono dubbi sulla veridicità o sull’adeguatezza della documentazione fornita dal cliente, ai fini dello svolgimento del servizio di intermediazione dei rifiuti;
- gestire correttamente l’archivio, istituito presso l’azienda, sul quale dovranno essere registrati e conservati i documenti, i dati identificativi e le altre informazioni relative alle operazioni ed ai rapporti commerciali. La registrazione può avvenire contestualmente all’operazione o in un momento successivo, entro e non oltre 30 giorni dalla data dell’operazione;
- segnalare le operazioni sospette all’unità di informazione finanziaria, anche nel caso in cui le stesse siano rifiutate o comunque non concluse; l’obbligo di effettuare le predette segnalazioni vige per l’intera durata del rapporto con il cliente e non è limitato quindi alle sole fasi d’instaurazione o di chiusura dello stesso (la decisione dei clienti di interrompere un rapporto non rappresenta, di per sé, elemento di sospetto). Le segnalazioni e le comunicazioni devono essere effettuate con la massima tempestività onde

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 30 di 53

consentire all'Uif l'esercizio del potere di sospensione previsto dall'art. 6, comma 6 lett. c) del decreto antiriciclaggio;

- valutare l'attendibilità dei fornitori con modalità che consentano di verificarne la correttezza professionale in un'ottica di prevenzione dei reati considerati nella presente sezione
- Assicurare adeguata formazione ai dipendenti in materia di riciclaggio.

Inoltre, è necessario rispettare le seguenti norme comportamentali:

- Individuare gli impianti di trattamento/smaltimento dei rifiuti, secondo criteri di trasparenza;
- verificare che le richieste arrivino da soggetti autorizzati a concludere contratti in nome e per conto del contraente;
- garantire la tracciabilità delle valutazioni sulle offerte tecniche ed economiche e delle operazioni effettuate
- Deve essere garantito il rispetto dei compiti, ruoli e responsabilità definiti dal l'AU e formalizzato dal **sistema delle deleghe e delle procure**
- deve essere garantito il rispetto dei principi di correttezza a trasparenza e garanzia dell'integrità e della reputazione delle parti nei rapporti intrattenuti con i fornitori
- Deve essere acquisito l'impegno formale da parte dell'affidatario dei lavori, (ad esempio, il Trasportatore) ad uniformarsi alle prescrizioni del Codice Etico ed alle linee di condotta del Modello al fine di sanzionare eventuali comportamenti contrari ai principi etici aziendali

5.5.2. Protocolli specifici

Il sistema di controllo specifico è strutturato sull'analisi delle fasi chiave del processo, nonché sulla tracciabilità degli atti a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati:

Nella fase della contrattazione

- L'attività è gestita dall'AU o dal **Responsabile dell'Area Commerciale**, munito di delega o procura idonea per contrattare in nome e per conto di AMSIC

Nella fase dell'individuazione dell'impianto di trattamento/smaltimento

- occorre verificare la documentazione attestante la regolarità della conduzione dell'impianto
- utilizzare criteri tecnico-economici per la selezione dell'impianto
- utilizzare criteri oggettivi e documentabili per individuare diversi offerenti ed effettuare una comparazione delle offerte
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati recanti la "clausola 231" per adesione ai principi e regole del presente Modello
- Garantire la tracciabilità delle singole fasi del processo (comunicazioni tramite email, documentazione a supporto, archiviazione), per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative
- Verificare che l'accordo per l'erogazione del servizio sia avvenuto a condizioni di mercato

Presidio sul rischio della criminalità organizzata e controllo del territorio

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 31 di 53

Per la Società è imprescindibile strutturare un sistema di controllo specifico sul rischio derivante dall'infiltrazione della criminalità organizzata sul territorio in cui opera.

A tal fine si rende necessaria o, quantomeno, auspicabile, svolgere un'analisi preventiva e continua del territorio o del contesto, rivolta ad individuare e valutare il pericolo che le organizzazioni criminali, localmente insediate, possano condizionare l'attività d'azienda, strumentalizzandola per il conseguimento di vantaggi illeciti.

Al fine di effettuare l'analisi preventiva del territorio, è fondamentale la raccolta del maggior numero possibile di dati e di informazioni utili per la conoscenza degli attori operanti nel territorio.

E' auspicabile a riguardo – ove ne sussistano le condizioni – una interlocuzione con autorità pubbliche e soggetti rappresentativi localmente competenti (prefetti, questori, forze di polizia, sindaci, associazioni industriali, associazioni sindacali di riferimento od eventuali soggetti funzionalmente assimilabili, associazioni volontarie), diretta ad acquisire dati, indicazioni, circostanze rilevanti ai fini della rilevazione degli indici di attenzione o dei criteri di valutazione.

Per effettuare l'analisi preventiva del territorio possono essere presi in considerazione:

- i provvedimenti o documenti giudiziari o di polizia ove disponibili;
- le relazioni periodiche, ove accessibili, di istituzioni pubbliche competenti;
- le rilevazioni degli ispettorati del lavoro;
- le statistiche ISTAT;
- gli studi sociologici e criminologici disponibili o richiesti ad esperti qualificati;
- le rilevazioni ed elaborazioni delle Camere di Commercio, delle associazioni imprenditoriali e sindacali, delle associazioni antiracket, nonché di ogni altro soggetto pubblico o privato svolgente funzioni similari;
- le inchieste e le cronache giornalistiche.

La prevenzione del rischio di infiltrazione criminale comporta una valutazione di affidabilità dei diversi soggetti (persone fisiche od enti) che hanno rapporti con la società.

Pertanto, quale condizione per intrattenere rapporti contrattuali con la società, occorre effettuare una accurata **“due diligence anticorruzione”** preventiva.

A tal fine possono essere utilizzati i seguenti indici di attenzione:

- sottoposizione a procedimento per l'applicazione di misure di prevenzione, ai sensi della normativa antimafia;
- applicazione di misure cautelari coercitive nell'ambito di un procedimento penale o pronuncia di sentenza di condanna, ancorché non definitiva, compresa quella prevista dall'art. 444 c.p.p., nei confronti di imprenditori, soci, amministratori o dipendenti di imprese, per reati che incidono sull'affidabilità professionale e, tra questi, per i delitti contro la Pubblica Amministrazione, per partecipazione o concorso esterno nei reati associativi, per i delitti di usura, estorsione, ricettazione, riciclaggio, impiego di beni provenienti da delitti e per altre figure delittuose che assumono rilievo nell'ambito della criminalità organizzata;
- applicazione di misure cautelari nell'ambito di un procedimento penale e pronuncia di sentenza di condanna, ancorché non definitiva, compresa quella emessa su richiesta delle parti, nei confronti di enti, ai sensi del D.lgs. 231/2001, per reati contro la Pubblica Amministrazione, reati contro la persona, reati di riciclaggio e di associazione a delinquere di natura transnazionale, e per altre figure di reato che assumono rilievo nell'ambito della criminalità organizzata;

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 32 di 53

- costituzione di enti nei quali figurano, come soci, amministratori o gestori, persone (o prossimi congiunti) che partecipano o abbiano partecipato alle imprese od enti nelle situazioni indicate ai punti precedenti, ovvero manifestamente sprovvisi, per età o formazione, dei requisiti indispensabili per l'esercizio dell'attività imprenditoriale;
- imprese che siano da ritenere, sulla base di elementi di fatto, costituite soltanto allo scopo di occultare o favorire soggetti appartenenti a gruppi criminali o, comunque, di eludere divieti nello svolgimento di attività imprenditoriali;
- imprese od enti che risultino privi di rapporti con aziende di credito;
- intervento, nelle trattative commerciali, di persone od enti privi di legittimazione ad interloquire nelle trattative medesime;
- mancata esibizione di documenti comprovanti l'iscrizione ad albi, ordini, elenchi, qualora l'iscrizione sia requisito necessario per lo svolgimento dell'attività.

Selezione dei fornitori

L'obiettivo di prevenire il pericolo di infiltrazioni criminali deve essere perseguito utilizzando il massimo numero possibile di fonti informative, sia al momento della selezione o del primo contatto con i fornitori significativi, sia nella valutazione delle successive condotte.

AMSIC esclude e/o interrompe i rapporti commerciali con fornitori che versino nelle condizioni previste dall'art. 94, D. Lgs. 36/2023.

Selezione dei clienti (produttori e detentori dei rifiuti) e degli impianti

Devono essere acquisite tutte le informazioni accessibili relative ai clienti ed agli impianti di trattamento/smaltimento, da utilizzare, oltre che per la normale valutazione di tipo commerciale, anche per la verifica di possibili rapporti con soggetti ed attività riconducibili ad organizzazioni criminali.

L'acquisizione e la raccolta di informazioni relative ai clienti significativi devono essere effettuate sia nell'avvio che durante lo svolgimento del rapporto.

Le forniture ai clienti devono essere immediatamente sospese qualora risultino concreti elementi di rischio di infiltrazione criminale, oppure del verificarsi, in assenza di giustificazioni economiche o imprenditoriali, di:

- mutamenti repentini o reiterati nella compagine sociale o negli organi sociali;
- mutamenti significativi del settore di attività;
- mutamenti repentini riguardo alle dimensioni dell'attività, al patrimonio, alle richieste di forniture.

Per i clienti e per gli impianti di trattamento/smaltimento dei rifiuti si applicano, in quanto compatibili, gli strumenti di presidio già previsti per i fornitori.

Selezione dei clienti "pubblici"

Per quanto riguarda i clienti pubblici (Comuni, Province, Consorzi, Enti pubblici ecc.), nonché Partiti politici, tenendo conto della loro natura e funzione istituzionale, la Società acquisirà tutte le informazioni accessibili per la verifica di possibili rapporti di questi ultimi con soggetti ovvero con attività riconducibili ad organizzazioni criminali.

Qualora siano accertati dalle Autorità concreti elementi di rischio di infiltrazione criminale riferibili ad un cliente pubblico, AMSIC si atterrà alle indicazioni delle autorità competenti, istituite e/o nominate per legge (commissari, ecc).

5.6. Flussi informativi ed attività dell'Organismo di Vigilanza

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 33 di 53

Le funzioni incaricate per la gestione dei rischi del presente processo dovranno, per quanto di propria competenza e con periodicità definita, informare l'Organismo di vigilanza riguardo:

- Elenco delle verifiche sulle condizioni dei fornitori e dei clienti risultate critiche per la sussistenza di episodi di infiltrazione mafiosa ovvero delle condizioni previste dall'art. 94, d. lgs. 36/2023.

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli in seguito alle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'OdV effettua periodicamente controlli a campione, sulle attività potenzialmente a rischio del reato di cui alla presente Parte Speciale, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere.

A tal fine all'OdV viene garantito - nel rispetto della normativa vigente, per esempio in tema di privacy - libero accesso a tutta la documentazione aziendale rilevante.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 34 di 53

6. DONAZIONI, LIBERALITÀ E OMAGGI

Il presente processo ha ad oggetto le attività ed i rischi riconducibili alle donazioni, liberalità e omaggi ricevuti dalla società ovvero effettuati a beneficio di soggetti terzi.

6.1. Individuazione del rischio – attività sensibili

Il presente processo concerne le seguenti attività:

- donazioni ricevute/effettuate a favore di soggetti terzi
- L'assunzione di iniziative di carattere umanitario e culturale, sociale e sportivo, quali interventi concreti per creare un valore aggiunto agli stakeholder in termini etici, civili e morali

Il processo si articola nelle seguenti fasi:

- Individuazione e formalizzazione delle iniziative a scopo benefico
- Gestione della contabilità relativa alle iniziative a scopo benefico
- Definizione dello scopo da raggiungere tramite le donazioni, liberalità e omaggi ricevuti/effettuati

6.2. Ipotesi di reati presupposto verificabili

- Reati di cui all'art. 24 d.lgs 231/01:
 - Art. 640 bis c.p. "truffa aggravata per il conseguimento di erogazioni pubbliche"
- Reati di cui all'art. 25 d.lgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
 - Art. 346 bis "traffico di influenze illecite"
- Reati di cui all'art. 24 ter d. lgs. 231/01:
 - Art. 416 c.p. "associazione per delinquere"
 - Art. 416 bis c.p. "associazioni di tipo mafioso anche straniere"
 - ART. 416 ter c.p. "scambio elettorale politico mafioso"
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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 di cui all'art. 25 quinquiesdecies d. lgs. 231/01:
 - Art. 8 d.lgs. 74/00 "emissione di fatture o altri documenti per operazioni inesistenti"

6.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

La società è esposta al rischio dei reati presupposto sopra indicati nelle seguenti ipotesi:

- ottenere finanziamenti pubblici falsamente destinati a pubblicità e sponsorizzazioni
- concedere/ricevere finanziamenti sotto forma di donazioni a/da soggetti vicini ad associazioni malavitose
- utilizzare la liberalità come il prezzo della corruzione e di qualsiasi vantaggio indebito
- utilizzare fondi delittuosi per le sponsorizzazioni

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 35 di 53

- concedere liberalità con strumenti illeciti di pagamento non consentiti dalla legge.
- emettere fatture per prestazioni inesistenti o parzialmente inesistenti

6.4. Soggetti ed aree coinvolte nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento delle seguenti figure:

- AU
- Area Amministrativa Contabile
- Area Commerciale

6.5. Sistema di controllo relativo al processo di donazioni, liberalità e omaggi

6.5.1. Regole generali

Le principali indicazioni comportamentali da osservare sono:

- Autorizzazione formalizzata dall’AU o da soggetto dipendente da questi incaricato a conferire utilità
- Gli omaggi consentiti devono essere utilità d’uso di modico valore: a tal fine l’AU definisce la soglia del valore non superiore ad euro 150,00 per gli omaggi destinati a soggetti appartenenti alla Pubblica Amministrazione
- Prevedere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, validati dal superiore gerarchico e archiviati
- Disporre report periodici sulle spese per la concessione di utilità, con motivazioni e nominativi / beneficiari, inviati al livello gerarchico superiore e archiviati
- Non possono essere erogati regali o benefici di qualsiasi natura a soggetti appartenenti alla Pubblica Amministrazione se finalizzati ad influenzarli nell’espletamento dei loro doveri d’ufficio e/o a trarre indebito vantaggio
- Deve essere verificata la regolarità dei pagamenti per donazioni, sponsorizzazioni o liberalità con riferimento alla piena coincidenza dei destinatari dei pagamenti con le controparti effettivamente coinvolte
- Sono immediatamente interrotte o, comunque, non è data esecuzione ad 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.

6.5.2. Protocolli specifici

Il sistema di controllo si basa sulla definizione dei criteri per l’individuazione delle modalità di godimento delle liberalità.

In particolare, gli elementi specifici di controllo sono:

- Nel caso di ricezione di liberalità di valore superiore ad euro 150,00, acquisire documentazione che ne attesti l’origine lecita
- Nel caso di ricezione/elargizione a terzi di liberalità di valore superiore ad euro 150,00, definire il progetto di godimento futuro e le modalità di utilizzo della liberalità ricevuta (es. investimenti, acquisti di macchinari, altre spese)

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 36 di 53

- Tracciabilità delle singole fasi del progetto per consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte

6.6. Flussi informativi ed attività dell'Organismo di Vigilanza

L'organismo di vigilanza deve ricevere dall'AU o da altro soggetto delegato con periodicità definita, un report contenente gli aggiornamenti su eventuali progetti di liberalità effettuati.

All'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione afferente le attività del presente processo.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 37 di 53

7. GESTIONE DEI RIMBORSI SPESE, ANTICIPI E DELLE SPESE DI RAPPRESENTANZA

Il presente processo ha ad oggetto la gestione e contabilizzazione dei rimborsi spese, anticipi e delle spese di rappresentanza, dalle cui possono individuarsi i seguenti rischi.

7.1. Individuazione dei rischi – attività sensibili

- gestione dei costi di inerenza
- spese di trasferta
- spese di rappresentanza
- assegnazione e utilizzo carte di credito

7.2. ipotesi di reati presupposto verificabili

- Reati di cui all'art. 24 ter d. lgs. 231/01:
 - Art. 416 c.p. "associazione per delinquere"
 - Art. 416 bis c.p. "associazioni di tipo mafioso anche straniere"
 - Art. 416 ter c.p. "scambio elettorale politico mafioso"
- Reati di cui all'art. 25 dlgs 231/01:
 - art. 318 c.p. "corruzione per l'esercizio della funzione";
 - art. 319 c.p. "corruzione per un atto contrario ai doveri d'ufficio";
 - art. 319 ter c.p. "corruzione in atti giudiziari";
 - art. 319 quater c.p. "induzione indebita a dare o promettere utilità";
 - Art. 322 c.p. "istigazione alla corruzione";
- Reati di cui all'art. 25 octies 1 d.lgs 231/01:
 - Art. 493 ter c.p. "indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti"
 - Art 493 quater c.p. "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"
- Reati di cui all'art. 25 quinquiesdecies d. lgs. 231/01:
 - Art. 11 d.lgs. 74/00 "sottrazione fraudolenta al pagamento delle imposte"

7.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

- offrire vantaggi a soggetti vicini ad associazioni criminose in occasione di eventi, pasti, viaggi
- utilizzare il costo, apparentemente di "inerenza", per dare o offrire qualcosa ad un pubblico ufficiale, ad un sindaco o altro organo sociale per ottenere un vantaggio indebito e in violazione degli obblighi di fedeltà
- utilizzare di carte di credito aziendali o altri strumenti di pagamento non essendo formalmente autorizzato
- simulare costi o vendite di beni o parte del patrimonio per sottrarre garanzie alla riscossione dei tributi.

7.4. Soggetti ed aree coinvolte nella gestione del processo

Nell'ambito del presente processo sono coinvolti i seguenti soggetti ed aree:

- AU
- Area Amministrativa Contabile

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 38 di 53

– Area Commerciale

7.5. Sistema di controllo in relazione al processo “gestione dei rimborsi spese e delle spese di rappresentanza”

7.5.1. Regole generali

Si riportano le principali regole generali del sistema di controllo:

- Non devono essere ammessi anticipi o rimborsi delle spese sostenute direttamente dai soggetti esterni, in particolare da rappresentanti della Pubblica Amministrazione che beneficiano di ospitalità
- La gestione dei rimborsi spese deve avvenire in accordo con la normativa, anche fiscale, applicabile
- I processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti
- Nello svolgimento di attività di servizio devono essere sempre ricercate le soluzioni più convenienti, sia in termini di economicità che di efficienza operativa
- Il sostenimento di spese di rappresentanza deve soddisfare il concetto di “opportunità” della spesa, in linea pertanto con gli obiettivi aziendali

7.5.2. Protocolli specifici

Il sistema di controllo specifico si combina con presidi già considerati per diversi processi sensibili (es. rapporti con la pubblica amministrazione).

Ciò che rileva in questa sede è regolarizzare l'utilizzo delle carte di credito e di altri strumenti di pagamento.

A tale scopo:

- L'AU effettua direttamente i pagamenti e tutte le altre operazioni tramite conto/corrente, carte di credito o altri strumenti pagamento;
- eventuali soggetti terzi incaricati di gestire i pagamenti per conto della società ed altre operazioni tramite, conto/corrente, carte di credito o altri strumenti di pagamento devono essere esplicitamente autorizzati con delega
- l'autorizzazione deve contenere un limite di manovra, ossia deve essere specificata l'operazione autorizzata e l'importo
- il soggetto incaricato dovrà archiviare apposita documentazione da cui si evincono i costi effettivamente sostenuti
- i costi possono essere contabilizzati previa verifica del rispetto del principio di inerenza

7.6. Flussi informativi ed attività dell'Organismo di Vigilanza

I soggetti incaricati della rendicontazione ovvero che possono autorizzare e verificare il corretto uso dei metodi di pagamento consentito al personale della società devono comunicare all'Organismo di Vigilanza, con periodicità definita, quanto segue:

- Elenco soggetti autorizzati all'uso di carte di credito e strumenti di pagamento della società
- Budget previsto per rimborsi spese, anticipi e spese di rappresentanza
- Elenco consuntivo per rimborsi spese, anticipi e spese di rappresentanza

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 39 di 53

8. SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE

Il processo di selezione e assunzione del personale è costituito da tutte le attività necessarie alla costituzione del rapporto di lavoro tra la società e una persona fisica.

Il processo si articola nelle seguenti fasi:

- **Acquisizione e gestione dei curricula-vitae**
- **Selezione**
- **Formulazione dell’offerta ed assunzione**

8.1. Individuazione dei rischi – attività sensibili

- colloqui per nuove assunzioni
- valutazioni del curriculum.
- attività di scouting

8.2. Ipotesi di reato astrattamente verificabili

- Reati di cui all’art. 24 ter d.lgs 231/01:
 - art. 416 c.p. “associazione per delinquere”
 - art. 416 bis c.p. “associazione mafiosa”
 - art. 416 ter c.p. “scambio elettorale politico – mafioso”
- Reati di cui all’art. 25 duodecies dlgs 231/01 “impiego di cittadini di paesi terzi il cui soggiorno è irregolare”;
- Reati di cui all’art. 25 dlgs 231/01:
 - art. 318 c.p. “corruzione per l’esercizio della funzione”;
 - art. 319 c.p. “corruzione per un atto contrario ai doveri d’ufficio”;
 - art 319 ter c.p. “corruzione in atti giudiziari”;
 - art. 319 quater c.p. “induzione indebita a dare o promettere utilità”;
 - Art. 322 c.p. “istigazione alla corruzione”;
- Reati di cui all’art. 25 quinquies d.lgs 231/01:
 - Art. 603 bis c.p. “intermediazione illecita e sfruttamento del lavoro”
- Reati di cui all’art. 25 octies 1 d.lgs 231/01:
 - Art. 493 ter c.p. “indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti”
 - Art 493 quater c.p. “Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti”

8.3. Punti Critici ed ipotetica modalità di commissione dei reati presupposto

- Assumere persone vicine ad associazioni criminali, o indicati da dalle stesse associazioni, al fine di ottenere un vantaggio indebito;
- accettare la promessa di procurare supporti elettorali a soggetti riconducibili ad associazioni mafiose, in cambio di indebita utilità;
- nell’ambito di una procedura di assunzione del personale, impiegare un soggetto privo del permesso di soggiorno o con permesso scaduto e mai rinnovato;

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 40 di 53

- d) ricevere/accettare la promessa di denaro o altra utilità per esercitare le proprie funzioni/poteri in cambio dell'assunzione del candidato;
- e) ricevere/accettare la promessa di denaro o altra utilità per non compiere/ritardare un atto del proprio ufficio in cambio dell'assunzione del candidato;
- f) nella gestione di procedimenti giudiziari, dare/promettere utilità al fine di essere favoriti o danneggiare una parte processuale;
- g) nell'ambito di una procedura di assunzione, concludere contratti con imprese che utilizzano personale d'opera non qualificato provenienti da paesi extra UE;
- h) Nell'ambito di una procedura di assunzione del personale reclutare/impiegare/assumere o utilizzare manodopera sottoponendo i lavoratori a condizioni di sfruttamento e approfittando del loro stato di bisogno.

8.4. Soggetti ed aree coinvolte nella gestione del processo

Nell'ambito del presente processo sono coinvolti i seguenti soggetti ed aree:

- AU
- Area Amministrativa Contabile

8.5. Sistema di controllo relativo al processo di selezione, assunzione e gestione del personale

8.5.1. Regole generali

Il presente sistema di controllo è stato strutturato, in parte, recependo regole già predisposte per la gestione del rischio previsto per altri processi sensibili, ed è stato integrato dalle seguenti:

- Divieto di offrire l'assunzione del dipendente (intesa come utilità) ad un pubblico ufficiale od incaricato di pubblico servizio in cambio di un vantaggio illecito;
- utilizzare, nella gestione dei rapporti con la Pubblica Amministrazione, eventuali percorsi preferenziali o conoscenze personali, anche acquisite al di fuori della propria realtà professionale, al fine di influenzarne le decisioni;
- divieto di riconoscere l'assunzione del dipendente in cambio di favori illeciti di fornitori o collaboratori esterni, o loro familiari;
- conferire incarichi professionali, dare o promettere doni, danaro, o altri vantaggi in cambio dell'assunzione;
- in fase di assunzione, sia ottenuta dal candidato copia del regolare permesso di soggiorno e ne sia verificata la scadenza al fine di monitorarne la validità durante il prosieguo del rapporto di lavoro;
- la documentazione sia conservata, ad opera della funzione aziendale competente, 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;
- sia verificata la sussistenza dei requisiti normativi di regolarità della controparte tramite la consegna della documentazione prevista dalla legge (ad es. documento unico di regolarità contributiva – DURC);
- la società garantisce che l'assunzione del personale, anche straniero, avvenga sulla base di regolari contratti di lavoro, e nel rispetto della normativa vigente in materia.

Si ritiene, inoltre, che i principi contenuti nel Codice Etico costituiscano un valido strumento per prevenire la modalità di commissione dei delitti valutati nel presente processo.

Tutti i destinatari del Modello, quindi, al fine di evitare condotte che possano integrare tale delitto, adottano prassi e comportamenti che siano rispettosi del Codice Etico.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 41 di 53

Le deroghe, le violazioni o il sospetto di violazioni delle norme che disciplinano le attività a rischio di reato di cui alla presente Parte Speciale sono oggetto di segnalazione da parte di tutti i dipendenti e degli organi sociali secondo le modalità previste nella Parte Generale del Modello.

8.5.2. Protocolli specifici

Il sistema di controllo imprescindibile per instaurare un rapporto di lavoro con la Società è una accurata “**due diligence anticorruzione**” preventiva.

A tal fine per la partecipazione alle procedure di selezione, deve essere autocertificato dai candidati di:

- non aver mai aver subito condanne, né di avere subito procedimenti, né di avere in corso procedimenti per i seguenti reati: associazione a delinquere (art. 416 c.p.), associazione per delinquere di tipo mafioso (art. 416 - bis c.p.), scambio elettorale politico mafioso (art. 416 - ter c.p.), ricettazione (art. 648 c.p.), riciclaggio (art. 648 - bis c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648 - ter c.p.);
- non essere in alcun modo collegato né collegabile ad organizzazioni criminali e pertanto, di non essere e di non poter costituire causa o strumento di tentativi di infiltrazione criminale all'interno della società;
- non avere riportato condanne penali passate in giudicato che possano influire sulla moralità professionale del ruolo posto in selezione (saranno equiparati i provvedimenti emanati ex art. 444 c.p.p. – c.d. sentenze di patteggiamento – nonché decreti penali di condanna definitivi; il divieto non opera quando il reato è stato depenalizzato ovvero quando è intervenuta la riabilitazione ovvero quando il reato è stato dichiarato estinto dopo la condanna ovvero in caso di revoca della condanna medesima). Il candidato dovrà indicare le eventuali condanne penali riportate e passate in giudicato al fine di consentire alla commissione di valutarne l'incidenza ai fini della sussistenza o meno della causa ostativa;
- non essere stato interdetto/a dai pubblici uffici, nonché destituito/a o dispensato/a ovvero licenziato/a dall'impiego c/o una Pubblica Amministrazione o una società pubblica (con esclusione dell'ipotesi di cessazione del rapporto di lavoro per giustificato motivo oggettivo);
- non avere alcuna condizione personale di incompatibilità rispetto alle regole ed ai principi contenuti nel Codice Etico aziendale e del Modello 231 di cui dichiara di aver preso visione e di accettare.

8.6. Flussi informativi e attività dell'Organismo di Vigilanza

Le funzioni responsabili della selezione ed assunzione del personale devono informare l'Organismo di Vigilanza, con periodicità predefinita, su:

- Assunzioni effettuate in deroga ai criteri stabiliti dalla società
- Attività di formazione ed informazione dei neo assunti sul Modello 231

In ogni caso, l'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 42 di 53

9. PROCESSO PER LA GESTIONE DELLA SALUTE E SICUREZZA SUI LUOGHI DI LAVORO

Il processo ha ad oggetto tutte le attività concernenti il rispetto degli obblighi normativi previsti per garantire l'integrità della salute e della sicurezza dei dipendenti sui luoghi di lavoro.

9.1. Individuazione del rischio – attività sensibili

- Osservanza degli adempimenti previsti dal d.lgs. 81/2008 in materia di tutela della salute e della sicurezza sui luoghi di lavoro

9.2. Ipotesi di reato verificabili

- Reati di cui all'art. 25 – septies d.lgs 231/01: "omicidio o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute o sicurezza sul lavoro"
 - Art. 589 c.p. "omicidio colposo";
 - Art. 590 c.p. "lesioni personali colpose".

9.3. Punti critici ed ipotetica modalità di commissione dei reati presupposto

In relazione al presente processo, si rilevano i seguenti punti critici e modalità ipotetiche di commissione degli illeciti:

- a) effettuare i lavori omettendo una valutazione aggiornata dei rischi (DVR)
- b) effettuare i lavori omettendo una valutazione aggiornata dei rischi da lavoro interferenziale, nelle ipotesi di collaborazione con imprese terze
- c) non eseguire la formazione dei lavoratori dipendenti
- d) non accertare le capacità soggettive dei dipendenti incaricati di eseguire i lavori
- e) non accertare i requisiti tecnico-strutturali dei macchinari e delle attrezzature della cantina e del magazzino
- f) omettere la necessaria manutenzione dei macchinari e delle attrezzature
- g) non effettuare la sorveglianza sanitaria e le visite periodiche del personale
- h) non prevedere l'uso di DPI ove necessario.

9.4. Soggetti ed aree operative coinvolte nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento dei seguenti soggetti ed aree:

- AU

9.5. Sistema di controllo interno relativo al processo di gestione della salute e sicurezza sui luoghi di lavoro

9.5.1. Regole generali

Il sistema di controllo si articola in modo da garantire la tracciabilità in tutte le attività del presente processo.

I principali elementi di controllo, pertanto, sono:

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 43 di 53

- tracciabilità delle singole attività (verbalizzazione delle decisioni, intestazione/formalizzazione dei documenti e modalità/tempistiche di archiviazione)
- verifica della corrispondenza delle dichiarazioni/certificazioni presentate con la documentazione tecnica di supporto
- archiviazione dei flussi documentali fra le funzioni della società interessate e gli organi della Pubblica Amministrazione deputati al rilascio di autorizzazioni e/o di certificazione attestante la conformità alle prescrizioni di legge, o deputati all'effettuazione di ispezioni e verifiche.

In generale, come previsto dall'art. 30 del D.Lgs. 81/08, la società deve garantire il rispetto delle normative in tema di tutela della salute dei lavoratori, di tutela dell'ambiente, nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, anche attraverso:

- una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere;
- la programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione e condizioni lavorative e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro;
- il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro;
- l'eliminazione/riduzione al minimo dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte;
- la sostituzione di ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso;
- il controllo e l'aggiornamento delle metodologie di lavoro;
- il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici;
- attività di informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, dei dirigenti e dei preposti sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro;
- la partecipazione e consultazione dei lavoratori e dei loro rappresentanti;
- la programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione del codice etico e di buone prassi;
- la formalizzazione di istruzioni adeguate ai lavoratori;
- l'uso di segnali di avvertimento e sicurezza;
- la regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti;
- la definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato.

Le misure relative alla sicurezza non devono in nessun caso comportare oneri finanziari per i lavoratori.

Nella scelta dei fornitori di beni o servizi devono essere privilegiati l'affidabilità del fornitore e la sua capacità di assolvere correttamente alle obbligazioni assunte, oltre al rapporto qualità/prezzo del bene o della prestazione offerta.

È fatto espresso divieto di:

- modificare o disattivare, senza autorizzazione i dispositivi di protezione individuali o collettivi;
- modificare o togliere, senza autorizzazione, i dispositivi di sicurezza o di segnalazione o di controllo;
- fabbricare, acquistare, noleggiare e utilizzare impianti, macchine, attrezzature o altri mezzi tecnici, inclusi dispositivi di protezione individuali e collettivi, non adeguati o non rispondenti alle disposizioni vigenti in materia di sicurezza;
- accedere ad aree di lavoro a cui non si è autorizzati;
- svolgere di propria iniziativa operazioni che non siano di competenza o che possano compromettere la sicurezza propria o di altri lavoratori.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 44 di 53

Inoltre, il Datore di Lavoro deve svolgere i seguenti compiti:

- nominare il Medico Competente (MC) scegliendolo in base ai titoli e ai requisiti previsti per legge;
- comunicare il nominativo del Medico Competente al Responsabile Servizio Prevenzione e Protezione (RSPP), al Responsabile dei Lavoratori per la Sicurezza (RLS), all’OdV;
- disporre l’attuazione di tutte le misure eventualmente indicate dal Medico Competente;
- inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria.

9.5.2. Protocolli specifici

Il sistema di controllo specifico è improntato sul rispetto delle prescrizioni del d. lgs. 81/2008 in materia di salute e sicurezza dei lavoratori sul luogo di lavoro.

Rispetto di standard tecnico-strutturali normati, relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici.

Il Datore di Lavoro, congiuntamente al RSPP, deve svolgere i seguenti compiti:

- individuare tutte le attrezzature e gli impianti utilizzati in azienda e i relativi standard di sicurezza previsti dalla normativa vigente e dalle indicazioni fornite dai fabbricanti;
- individuare gli standard tecnico strutturali dei luoghi di lavoro, in particolare, il sistema antincendio, la salubrità dell’ambiente e quelli relativi al pronto soccorso;
- disporre l’utilizzo limitato di agenti chimici, fisici e biologici e, predisporre tabelle indicanti i limiti e le modalità di utilizzo per ciascuno di essi, nonché modalità di smaltimento;
- redigere il documento di individuazione degli standard tecnico-strutturali di legge da allegare alla valutazione dei rischi e da comunicare all’OdV;
- assicurare la vigilanza costante dei suddetti limiti attraverso la regolare manutenzione di ambienti, attrezzature, impianti, in conformità e con le tempistiche individuate nel documento per la sicurezza ed altresì attraverso sopralluoghi sugli ambienti di lavoro secondo la procedura già adottata dalla società;
- redigere il verbale del controllo periodico eseguito e previsto al punto che precede.

Adozione delle misure di prevenzione e protezione

Il Datore di Lavoro deve svolgere i seguenti compiti:

- monitorare l’attività svolta dai preposti con delega di funzioni conferita ai sensi dell’art. 16, d. lgs. 81/2008;
- nominare il responsabile per la prevenzione e protezione RSPP, in possesso di requisiti professionali richiesti dalla legge e organizzare il servizio all’interno dell’azienda anche con collaboratori esterni;
- trasmettere copia della nomina del RSPP al rappresentante dei lavoratori, al Medico Competente, all’OdV;

L’ RSPP, dopo la nomina deve:

- individuare i fattori di rischio, procedere alla valutazione dei rischi e alla individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro per quanto sia di sua competenza;
- elaborare le misure preventive e protettive e il sistema di controllo delle medesime;
- elaborare le procedure di sicurezza per le varie attività aziendali;
- redigere e conservare tutti i documenti previsti dalle leggi in materia di sicurezza con riferimento ai fattori di rischio, alle misure di prevenzione e alle procedure e trasmetterli al datore di lavoro ai fini della valutazione dei rischi, all’OdV e al rappresentante dei lavoratori;

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 45 di 53

- proporre programmi di formazione e informazione dei lavoratori;
- partecipare alle consultazioni in materia di tutela e sicurezza sul lavoro e alle riunioni periodiche di sicurezza;
- fornire informazioni ai lavoratori circa le misure di prevenzione e protezione.

9.6. Flussi informativi e attività dell’Organismo di Vigilanza

Il Datore di Lavoro, l’RSPP ed eventuali altri Preposti informano l’Organismo di Vigilanza con periodicità definita o comunque al verificarsi di eventi significativi:

- In caso di incidenti avvenuti ai danni dei lavoratori nell’esecuzione delle attività aziendali
- Dell’avvenuto aggiornamento del DVR, avendo cura di trasmetterne una copia
- Dei programmi di formazione ed informazione del personale sui rischi derivanti dall’esecuzione delle attività aziendali

In ogni caso, l’Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L’Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 46 di 53

10. GESTIONE DEL SERVIZIO DI INTERMEDIAZIONE DEI RIFIUTI

Il presente processo ha ad oggetto le attività sensibili che rappresentano il *core business* aziendale, concernente l'attività di intermediazione senza detenzione di rifiuti pericolosi e non pericolosi.

L'analisi di alcune attività preliminari è stata effettuata nell'ambito degli altri processi sensibili, sopra esaminati.

Quanto al presente processo, invece, verrà effettuata una analisi specifica relativa alle attività svolte da AMSIC per l'intermediazione dei rifiuti.

10.1. Individuazione dei rischio – attività sensibili

In relazione al presente processo, si rilevano le seguenti attività sensibili:

- Valutazione dei rifiuti del produttore/detentore
- Individuazione della migliore collocazione dei rifiuti presso discariche o impianti di trattamento/smaltimento
- Proposta dell'offerta al produttore/detentore del rifiuto
- Verifica dei documenti per il ritiro e trasporto dei rifiuti
- Tenuta della documentazione obbligatoria
- Eventuale individuazione di soggetti terzi per il trasporto di rifiuti speciali non pericolosi e pericolosi

10.2. Ipotesi di reati presupposto verificabili

- Reati di cui all'art. 24 ter d.lgs 231/01:
 - art. 416 c.p. "associazione per delinquere"
 - art. 416 bis c.p. "associazione mafiosa"
 - art. 416 ter "scambio elettorale politico mafioso"
- Reati di cui all'art. 25 octies d.lgs 231/01:
 - 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 di cui all'art. 25 undecies d.lgs 231/01
 - Art. 452 bis c.p. "Inquinamento ambientale";
 - Art. 452 quater c.p. "disastro ambientale"
 - Art. 452 quinquies c.p. "delitti colposi contro l'ambiente"
 - Art. 452 sexies c.p. "traffico e abbandono di materiale ad alta radioattività"
 - Art. 452 quaterdecies c.p. "attività organizzate per il traffico illecito di rifiuti"
 - Art. 733 bis c.p. "distruzione o deterioramento di habitat all'interno di un sito protetto"
 - Art. 137, d. lgs. 152/06 "Reati in materia di scarichi di acque reflue"
 - Art. 256 D.Lgs. 152/06 "attività di gestione non autorizzata"
 - Art. 258 D.Lgs. D.Lgs. 152/06 "violazione degli obblighi di comunicazione, tenuta dei registri e dei formulari"
 - Art. 259 D.Lgs. 152/06 "traffico illecito di rifiuti"
 - Art. 260 bis D.Lgs. 152/06 "Sistema informatico di controllo della tracciabilità dei rifiuti"
- Reati di cui all'art. 25 quinquiesdecies d.lgs. 231/01
 - Art. 2 D.Lgs. 74/00 "dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto"

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 47 di 53

- Art. 3 D.Lgs. 74/00 “dichiarazione fraudolenta mediante altri artifici”
- Art. 4 D.Lgs. 74/00 “dichiarazione infedele”
- Art. 8 D.Lgs. 74/00 “emissione di fatture o altri documenti per operazioni inesistenti”
- Reati di cui all’art. 25 sexiesdecies d. lgs. 231/01 - contrabbando

10.3. Punti critici ed ipotetica modalità di commissione dei reati presupposto

In relazione al presente processo, si rilevano i seguenti punti critici e modalità ipotetiche di commissione degli illeciti:

- Associarsi con tre o più persone al fine di compiere una serie indeterminata di illeciti a vantaggio della Società
- Omettere di acquisire la documentazione necessaria dagli impianti di trattamento, dal produttore/detentore e dal trasportatore
- Intermediare rifiuti provenienti da aree di stoccaggio non autorizzate
- Proporre ed eseguire un conferimento di rifiuti presso un impianto non autorizzato
- Non provvedere alla corretta tenuta dei registri e dei formulari
- Sovrastimare il pagamento dovuto e contabilizzare un costo superiore a quello effettivo

10.4. Soggetti ed aree operative coinvolte nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento dei seguenti soggetti ed aree:

- AU
- Area Amministrativa Contabile
- Area Commerciale

10.5. Sistema di controllo relativo al processo per la gestione delle attività di pulizia e raccolta, trasporto, smaltimento e trattamento dei rifiuti

10.5.1. Regole generali

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico adottati dalla Società, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento e controllo:

- Devono essere richieste e preventivamente acquisite tutte le autorizzazioni, nonché devono essere effettuate le comunicazioni o le iscrizioni ambientali necessarie per lo svolgimento della propria attività
- Devono essere valutati i potenziali rischi a tutela dell’ambiente interessato
- Si devono rispettare scrupolosamente tutte le prescrizioni contenute negli atti autorizzativi ricevuti
- Deve essere accertata l’avvenuta caratterizzazione dei rifiuti con attribuzione del codice CER
- Deve essere costantemente vigilata la corretta gestione dei rifiuti segnalando eventuali irregolarità alle Autorità competenti al fine di porre in essere le conseguenti azioni di tipo amministrativo e contrattuale oltre che le eventuali azioni di tipo legale.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 48 di 53

10.5.2. Protocolli specifici

Per il conferimento dei rifiuti presso le imprese autorizzate e quindi prima della fase di smaltimento e recupero dei rifiuti, deve essere verificata la regolare compilazione del **modulo di omologa**.

In particolare deve essere verificata:

- L'analisi chimica per la caratterizzazione del rifiuto
- La data di validità dell'autorizzazione
- La tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero
- La localizzazione dell'impianto di smaltimento e o recupero
- Il metodo di trattamento o recupero
- La possibilità di acquisire un campione di rifiuto
- Acquisire delle foto del carico di rifiuti

In fase di esecuzione delle attività di trasporto di rifiuti agli impianti autorizzati deve essere verificata:

- La data di validità dell'autorizzazione
- La tipologia e la targa del mezzo
- I codici CER autorizzati

La società è obbligata alla corretta tenuta della dei registri di carico e scarico e pertanto deve provvedere a:

- Vidimazione dei registri di carico e scarico
- Compilazione dei registri entro 10 giorni lavorativi dalla relativa transazione
- conservazione di una copia del formulario emessa dal produttore (anche detta "quinta copia");
- invio del MUD entro data stabilita dalla normativa;
- conservazione del registro integrato e dei relativi formulari per 5 anni dalla data della registrazione.

10.6. Flussi informativi e attività dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli sulle attività sensibili individuate nel presente capitolo, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

Le verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso

I soggetti incaricati della gestione delle attività sensibili, devono comunicare all'Organismo di vigilanza, con periodicità definita, le seguenti informazioni:

- Autorizzazioni relative alla gestione dei rifiuti
- Informazioni sull'affidamento dello smaltimento dei rifiuti ad imprese autorizzate

In ogni caso, l'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 49 di 53

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 50 di 53

11. GESTIONE DEI SISTEMI INFORMATICI

Con riferimento alla possibile commissione dei reati presupposto nell'ambito del processo in oggetto, sebbene la società non operi direttamente nel settore economico e professionale dell'informatica e della telematica, sussiste un rischio di accadimento delle fattispecie illecite indicate, con riferimento alle attività di gestione ed utilizzo delle reti e degli apparati informatici impiegati per lo svolgimento di qualsiasi attività riconducibile all'azienda.

11.1. Individuazione del rischio – attività sensibili

In relazione al presente processo, si rilevano i seguenti attività sensibili:

- utilizzo di computer, tablet, sistemi informatici
- gestione della sicurezza fisica degli asset IT
- gestione della sicurezza logica degli applicativi informatici utilizzati

11.2. Ipotesi di reati presupposto verificabili

- Reati di cui all'Art. 24 bis d.lgs 231/01 "delitti informatici e trattamento illecito dei dati":
 - Art. 615 ter c.p. "accesso abusivo ad un sistema informatico o telematico";
 - Art. 617 quater c.p. "intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche";
 - Art. 635 bis c.p. "danneggiamento di informazioni, dati e programmi informatici";
 - Art. 635 quater c.p. "danneggiamento di sistemi informatici o telematici";
- Reati di cui all'art. 25 octies.1 d.lgs 231/01 "delitti in materia di strumenti di pagamento diversi dai contanti":
 - Art. 493 quater c.p.: "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti"
 - Art. 640 ter "Frode informatica"

11.3. Punti critici ed ipotetica modalità di commissione dei reati presupposto

In relazione al presente processo, si rilevano i seguenti punti critici e modalità ipotetiche di commissione degli illeciti:

- Alterare il funzionamento di un sistema informatico o telematico, procurando a sé un ingiusto profitto con danno dello Stato o di un ente pubblico;
- Nell'ambito dello svolgimento di attività lavorativa, introdursi abusivamente in un sistema informatico o telematico protetto da password o mantenersi contro la volontà di chi ha il diritto di esclusione dallo stesso (esempio: posta elettronica privata);
- Nell'ambito dello svolgimento di attività lavorativa, intercettare, impedisce o interrompe fraudolentemente comunicazioni relative ad un sistema informatico o telematico;
- Nell'ambito dello svolgimento di attività lavorativa, distruggere, deteriorare, cancellare, alterare o sopprimere (o commettere un atto diretto a porre in essere tali comportamenti) informazioni, dati o programmi informatici altrui;
- Accedere tramite sistemi informatici a strumenti di pagamento non previsti dalla società.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 51 di 53

11.4. Soggetti ed aree coinvolte nella gestione del processo

Le attività inerenti al processo in oggetto prevedono il coinvolgimento dei seguenti soggetti ed aree:

- AU
- Area Amministrativa Contabile
- Area Commerciale

11.5. Sistema di controllo relativo al processo di gestione dei sistemi informatici

11.5.1. Regole generali

- L'utilizzo di specifiche tecniche di crittografia per la protezione e/o trasmissione delle informazioni deve essere regolamentato in una procedura formalizzata in cui siano definite le modalità operative e le responsabilità dei soggetti coinvolti nel processo di gestione.
- Deve essere implementato un sistema di gestione delle chiavi a sostegno dell'uso delle tecniche crittografiche per la generazione, distribuzione, revoca ed archiviazione delle chiavi.
- Devono esser predisposti ed opportunamente documentati di controlli per la protezione delle chiavi da possibili modifiche, distruzioni, utilizzi non autorizzati.
- Devono essere formalizzate le procedure che regolamentano la gestione dell'utilizzo della firma digitale nei documenti, disciplinandone responsabilità, livelli autorizzativi, regole di adozione di sistemi di certificazione, eventuale utilizzo ed invio dei documenti, modalità di archiviazione e distruzione degli stessi.
- La procedura di archiviazione, produzione e manutenzione di un documento informatico deve essere redatta e diffusa a tutti i soggetti che sono coinvolti nel processo di gestione di un documento informatico.

Inoltre, allo scopo di garantire l'integrità e la sicurezza dell'intranet aziendale:

- è vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili così come analizzate nel Documento di Valutazione dei Rischi (DVR);
- è vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle sopra riportate;
- è vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti, se non previa autorizzazione dell'AU o del titolare della postazione;
- è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;

AMSIC	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 52 di 53

- è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- è vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- è vietato lo spamming come pure ogni azione di risposta allo spam;
- è obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

11.5.2. Protocolli specifici

Gestione degli accessi

Il sistema di accesso deve essere idoneo a controllare che l'utilizzo delle risorse da parte degli utenti nonché l'accesso alla rete si esplicino attraverso la verifica e la gestione dei diritti d'accesso.

A tale scopo AMSIC verifica che:

Attivazione

- prima della creazione di un'utenza, che la stessa non sia già stata precedentemente assegnata/disabilitata/rimossa e che uno stesso codice identificativo personale non venga assegnato, neppure in tempi diversi, a persone diverse;
- che sia predisposto l'utilizzo di specifiche tecniche di crittografia per la protezione e/o trasmissione delle informazioni sensibili;
- la Società definisce le modalità operative e le responsabilità dei soggetti coinvolti nel processo di gestione, specificando il tipo di codice assegnato a ciascun individuo;
- la Società sviluppa un sistema di gestione delle chiavi a sostegno dell'uso delle tecniche crittografiche per la generazione, distribuzione, revoca ed archiviazione delle chiavi;
- devono esser predisposti ed opportunamente documentati di controlli per la protezione delle chiavi da possibili modifiche, distruzioni, utilizzi non autorizzati.

Disattivazione

Nel caso in cui un soggetto precedentemente autorizzato perda il diritto di accesso ad alcuni o a tutti i sistemi informatici, la società si occupa della disattivazione dei codici utente associati

Modalità di utilizzo del PC e installazione di software sui sistemi operativi

L'utilizzo del PC deve essere conforme alle prescrizioni impartite al momento della formazione.

La formazione è volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy.

A tale proposito, la società indica esplicitamente il corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni.

AMSIK	MOGC – D.Lgs. 8 giugno 2001 n. 231	REV. 00 – 12.10.2024
	PARTE SPECIALE	Pag. 53 di 53

Contestualmente all'assegnazione del pc e/o dell'indirizzo mail, la Società consegna elenco delle norme per l'utilizzo dei Personal Computer aziendali, della posta elettronica e in generale di documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico.

Al fine di garantire la sicurezza dei software aziendali, i soggetti assegnatari di PC aziendali o posta elettronica aziendali comunicano tempestivamente eventuali vulnerabilità rinvenute al Responsabile incaricato.

La società elabora un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei log-on e log-off).

Trasferimento dati: riservatezza e networking

I dati ricevuti e da trasferire vengono elaborati in maniera tempestiva dai destinatari e limitatamente allo scopo della funzione.

Le informazioni sensibili vengono protette durante i processi di raccolta e di conservazione dalla società, in modo da impedirne la lettura a terzi soggetti non autorizzati, anche tramite accesso fortuito alla rete.

I dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come "dati riservati".

11.6. Flussi informativi e attività dell'Organismo di vigilanza

Le funzioni incaricate della gestione delle apparecchiature informatiche devono comunicare all'Organismo di vigilanza, con periodicità definita, le seguenti informazioni:

- Elenco soggetti autorizzati alla detenzione ed all'uso di credenziali di accesso ai profili informatici aziendali

In ogni caso, l'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.