Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001 adottato da ASTER – Azienda Sevizi Territoriali Genova S.p.A.

PARTE SPECIALE

ALTRI REATI

Stato delle revisioni

Nr. Rev.	Descrizione modifiche	Data	Approvazione
0	Creazione parte speciale come documento autonomo del Modello di organizzazione, gestione e controllo ex D.lgs. 231/2001	28/06/2023	Consiglio di Amministrazione

INDICE

1. PREMESSA 4
2. FALSITA' IN MONETE, IN CARTA DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO 5
2.1. I reati 5
2.2. I processi sensibili ai fini del decreto 6
2.3. Regole di comportamento 6
3. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO 6
3.1. I reati 6
3.2. I processi sensibili ai fini del decreto 7
3.3. Regole di comportamento 7
4. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE 8
4.1. I reati 8
4.2. I processi sensibili ai fini del decreto 8
4.3. Regole di comportamento 8
5. REATI CONTRO LA PERSONALITÀ INDIVIDUALE 9
5.1. I reati 9
5.2. I processi sensibili ai fini del decreto 10
5.3. Regole di comportamento 10
6. REATI DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE 11
6.1. I reati 11
6.2. I processi sensibili ai fini del decreto 12
6.3. Regole di comportamento 12
7. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI 13
7.1. I reati 13
7.2. I processi sensibili ai fini del decreto 13
7.3. Regole di comportamento 14
8. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO E DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI 14
8.1. I reati 14
8.2. I processi sensibili ai fini del decreto 15
8.3. Regole di comportamento 15

9. REATI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA 16
9.1. I reati 17
9.2. I processi sensibili ai fini del decreto 17
9.3. Regole di comportamento 17
10. REATI DI RAZZISMO E XENOFOBIA 18
10.1. I reati 18
10.2. I processi sensibili ai fini del decreto 18
10.3. Regole di comportamento 18
11. DELITTI CONTRO IL PATRIMONIO CULTURALE E REATI DI RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI**Errore. Il segnalibro non è definito.**
11.1. I reati ..... **Errore. Il segnalibro non è definito.**
11.2. I processi sensibili ai fini del decreto ..... **Errore. Il segnalibro non è definito.**
11.3. Regole di comportamento ..... **Errore. Il segnalibro non è definito.**
12. DELITTI DI CRIMINALITA' ORGANIZZATA 19
12.1. I reati 19
12.2. I processi sensibili ai fini del decreto 19
12.3. Regole di comportamento 19
13. I FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA. **Errore. Il segnalibro non è definito.**
14. I CONTROLLI DELL'ORGANISMO DI VIGILANZA..... **Errore. Il segnalibro non è definito.**

1. PREMESSA

In questa parte speciale del Modello 231 sono illustrate le regole di condotta (o protocolli) volte a prevenire il compimento di reati previsti dal D.Lgs. 231/2001 che non rientrano nelle altre parti speciali del Modello 231.

La scelta di creare una parte speciale denominata "Altri reati" è dovuta al fatto che dall'attività di identificazione e valutazione dei rischi che è stata condotta, sono stati individuati dei reati che, pur presentando una probabilità di accadimento più contenuta rispetto ai reati oggetto di trattazione nelle altre parti speciali, potrebbero comunque potenzialmente essere commessi. La definizione della presente parte speciale risponde all'esigenza di prevenire la commissione dei reati presupposto della responsabilità amministrativa, anche in relazione all'ipotesi di concorso nel reato tra l'agente apicale/dipendente di Aster e soggetti esterni alla società.

Di seguito si riporta l'elencazione delle categorie considerate in questo documento, facendo rinvio all'Allegato 1 del Modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*", per la descrizione del dettato normativo relativo ai diversi reati che rientrano nelle varie categorie. Nello specifico si tratta di:

- falsità in monete, in carta di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- delitti contro l'industria e il commercio;
- reati in materia di violazione del diritto d'autore;
- reati contro la personalità individuale;
- reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- reati informatici e trattamento illecito di dati;
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio, delitti in materia di strumenti di pagamento diversi dai contanti;
- reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- reati di razzismo e xenofobia;
- delitti contro il patrimonio culturale;
- reati di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici;
- delitti di criminalità organizzata.

In base ai risultati dell'attività di risk assessment condotta (si veda al riguardo il documento del Modello denominato "*Matrice risk assessment 231")* sono state identificate delle categorie di reato che, data l'attività svolta da Aster, la natura dei suoi processi gestionali e i suoi assetti istituzionali e di governance sono state considerate come "astrattamente ipotizzabili", poiché al momento dell'approvazione del modello, non sono state identificate specifiche attività o processi che presentano un'esposizione al rischio di commissione dei reati. Nello specifico le categorie si riferiscono a:

- delitti con finalità di terrorismo e di eversione dell'ordine democratico (ex art. 25-quater D.Lgs. 231/2001);
- pratiche di mutilazioni degli organi genitali femminili (ex art. 25-quater1 D.Lgs. 231/2001);
- abusi di mercato (ex art. 25-*sexies* D.Lgs. n. 231/2001);
- frode in competizioni sportive (ex art. 25-quaterdecies D.Lgs. 231/2001);
- reati di contrabbando (ex art. 25-sexiesdecies, D.Lgs. 231/2001);
- reati transnazionali.

In ogni caso, per evitare il possibile configurarsi di forme di responsabilità amministrativa a carico di ASTER ai Destinatari del Modello è fatto divieto di violare i principi del Codice etico della Società e di attuare comportamenti che possano determinare, anche soltanto in via potenziale, il configurarsi dei reati che rientrano nelle suddette categorie, come illustrato nell'allegato 1 "*Elenco dei reati presupposto della responsabilità amministrativa*".

2. FALSITA' IN MONETE, IN CARTA DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO

2.1. I reati

L'art. 25-*bis* del D.Lgs. 231/2001 considera i seguenti reati presupposto della responsabilità amministrativa:

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

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia all'Allegato 1 al presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

2.2. I processi sensibili ai fini del decreto

In relazione ai reati elencati nel paragrafo precedente, la Società ha individuato i processi sensibili di seguito elencati:

- gestione dei pagamenti e degli incassi in contanti;
- acquisto ed utilizzo di valori bollati;
- realizzazione e vendita di servizi utilizzando marchi ed altri segni di riconoscimento;
- pubblicità e promozione aziendale utilizzando marchi ed altri segni di riconoscimento.

Per un maggior dettaglio dei processi sensibili sopra citati si rinvia al documento del Modello denominato "*Matrice di risk assessement 231*".

2.3. Regole di comportamento

Al fine di evitare di incorrere nella realizzazione dei suddetti reati si prevede il divieto di:

- porre in essere condotte di contraffazione o alterazione di banconote, valori bollati e altri strumenti di pagamento;
- contraffare o alterare marchi ed altri segni di riconoscimento (es. loghi aziendali, segni ornamentali);
- accettare e effettuare pagamenti in contanti soltanto nei casi previsti dalla procedura di tesoreria e nel rispetto dei limiti di importo stabiliti nella procedura medesima;
- partecipare a schemi fraudolenti aventi ad oggetto i reati sopra definiti.

3. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

3.1. I reati

L'art. 25-*bis*1 del D.Lgs. 231/2001 considera i seguenti reati presupposto della responsabilità amministrativa:

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

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia al documento del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

3.2. I processi sensibili ai fini del decreto

La Società ha individuato i processi sensibili di seguito elencati:

- Processi di produzione e vendita del conglomerato bituminoso;
- Controllo di qualità del conglomerato bituminoso (frode nel commercio).

Per un maggior dettaglio dei processi sensibili sopra citati si rinvia al documento del Modello denominato "*Matrice di risk assessement 231*".

3.3. Regole di comportamento

Nell'espletamento della attività aziendali, tutti coloro che operano per conto di ASTER sono tenuti al rispetto delle norme di comportamento di seguito indicate:

1. Nelle operazioni di vendita dei servizi di ASTER e del conglomerato bituminoso è previsto l'obbligo di rispettare rigorosamente nei rapporti con il potenziale acquirente le regole di correttezza commerciale, definite dalle norme di legge a tutela del mercato e dei consumatori operando in ossequio ai principi di trasparenza, buona fede e diligenza professionale;
2. astenersi dal compiere pratiche commerciali scorrette o ingannevoli (compresa l'omissione di informazioni) evitando di fornire informazioni false ai potenziali acquirente/ al fine di indurli ad acquistare i servizi o i prodotti realizzati dalla società;
3. garantire lo svolgimento dei controlli circa la qualità del conglomerato bituminoso secondo le normative in vigore EN 13108-1;
4. qualora dal controllo di cui al punto 3. emerga la scarsa qualità del prodotto, lo stesso non potrà essere utilizzato per l'asfaltatura di strade né per altri utilizzi commerciali.

Inoltre, è fatto <u>divieto</u> di:

1. adottare comportamenti in contrasto con i contenuti del Codice Etico adottato dalla Società, nonché con la normativa vigente in materia di promozione e tutela della concorrenza;
2. realizzare qualsiasi forma di attività intimidatoria o vessatoria nei confronti di concorrenti attuali o potenziali, ovvero trasmettere informazioni menzognere in danno di terzi potenziali concorrenti;
3. porre in essere qualsiasi comportamento che non sia improntato a correttezza e lealtà anche nei confronti dei partner e dei clienti e che sia, anche indirettamente, volto ad ottenere in modo illecito una restrizione della concorrenza.

4. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

4.1. I reati

La Legge 99/2009 ha introdotto nel D.Lgs. 231/2001 l'art. 25-*novies* ampliando le tipologie di reati presupposto alle categorie contemplate nella Legge 22 aprile 1941 n. 633 riguardante la "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio".

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia al documento n.7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

4.2. I processi sensibili ai fini del decreto

La Società ha individuato i processi sensibili di seguito elencati:

- la gestione dei sistemi informatici, con particolare riguardo all'acquisto ed il rinnovo delle licenze software;
- l'accesso a banche dati e a qualsiasi materiale coperto dal diritto di autore;
- la gestione dei contenuti del sito internet;
- la predisposizione di materiale pubblicitario.

Per un maggior dettaglio dei processi sensibili sopra citati si rinvia al documento del Modello denominato "*Matrice di risk assessement 231*".

4.3. Regole di comportamento

Nell'espletamento della propria attività, tutti i dipendenti di ASTER sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico:

- devono essere rispettate le norme in materia di diritto d'autore e, in particolare, le disposizioni di legge applicabili con riferimento all'acquisizione, conservazione, utilizzo, riproduzione, duplicazione, elaborazione, diffusione e distribuzione (anche attraverso reti telematiche) di software, banche dati, testi, immagini, video e altro materiale coperto dal diritto d'autore;
- è previsto il divieto di:
    - installare programmi software diversi da quelli messi a disposizione e autorizzati dalla società;
    - scaricare da Internet programmi senza la preventiva autorizzazione della Società;
    - acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
    - installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di underlincensing;

- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
- accedere illegalmente e duplicare banche dati;
- in caso di elaborazione di un programma pubblicitario, garantire che il materiale utilizzato (a titolo esemplificato ma non esaustivo che nel materiale multimediale si richiamano immagini, video, riprese etc.), sia prodotto in proprio sia da terzi, venga verificato prima della loro pubblicazione.

5. REATI CONTRO LA PERSONALITÀ INDIVIDUALE COMPRESE L'INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO

5.1. I reati

La Legge 11 agosto 2003 n. 228 recante "Misure contro la tratta di persone" ha introdotto nel D. Lgs. 231/01, la macroarea di reati "Delitti contro la personalità individuale" alla commissione dei quali la Società può essere perseguita e punita. Tale area di reati è contemplata nell'art. 25-*quinquies* del D. Lgs. 231/01.

Le fattispecie di reato contenute in tale macroarea sono le seguenti:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-bis, comma 1, c.p.)
- Pornografia minorile (art. 600-ter, commi 1 e 2, c.p.)
- Detenzione di materiale pornografico (art. 600-quater c.p.)
- Pornografia virtuale (art. 600-quater.1, c.p.)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Adescamento di minorenni (art. 609 undecies c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.)

Ulteriori modifiche legislative in materia di responsabilità degli enti sono state introdotte dalla Legge n. 7/2006[1], che vieta e punisce le c.d. pratiche di infibulazione, dalla Legge n. 38/2006[2], contenente "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia

[1] Legge 9 gennaio 2006, n. 7, recante *"Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile"*, pubblicata nella Gazzetta Ufficiale n. 14 del 18 gennaio 2006.

[2] *Legge 6 febbraio 2006, n. 38, contenente "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", pubblicata nella Gazzetta Ufficiale n. 38 del 15 febbraio 2006.*

anche a mezzo Internet" e, infine, dalla Legge di ratifica ed esecuzione della Convenzione di Palermo sulla criminalità organizzata transnazionale del 15 novembre 2000[3].

La Legge 6 febbraio 2006, n. 38, ha modificato l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (rispettivamente, artt. 600-ter e 600-*quater* c.p.), per i quali era già prevista la responsabilità dell'ente ex Decreto 231, includendo anche le ipotesi in cui il materiale pornografico utilizzato rappresenti immagini virtuali di minori (c.d. "pedopornografia virtuale").

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

5.2. I processi sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute a rischio risultano essere le seguenti:

- la gestione del personale con riferimento all'orario di lavoro (compresi gli straordinari), ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria e alle ferie;
- la determinazione delle retribuzioni del personale;
- la gestione degli aspetti attinenti alla salute e sicurezza nei luoghi di lavoro;
- la gestione dei metodi di video sorveglianza;
- la gestione degli accessi ai siti internet ove possano essere contenuto materiale pornografico e pedopornografico;
- la promozione e pubblicità.

5.3. Regole di comportamento

Al fine di evitare il rischio di incorrere nei reati contro la personalità individuale, ASTER non tollera alcuna forma di lavoro irregolare ed è molto attenta al rispetto della normativa in tema di:

- tutela del lavoro minorile e delle donne;
- condizione igienico-sanitarie e di sicurezza;
- diritti sindacali o comunque di associazione e di rappresentanza.

Si indicano qui di seguito i principi che tutti i Soggetti che operano per conto di Aster sono tenuti a rispettare:

- nei processi di assunzione del personale la società opera nel rispetto delle norme giuslavoristiche, degli obiettivi posti dal Comune di Genova, dei regolamenti aziendali e degli accordi sindacali per l'assunzione;

[3] Legge 16 marzo 2006, n. 146, recante *"Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001"*, pubblicata nella Gazzetta Ufficiale dell'11 aprile 2006, n. 85 – Suppl. Ord. n. 91.

- nel corso del rapporto di lavoro è fatto obbligo di rispettare le norme di legge in tema di tutela del lavoro minorile e delle donne, condizioni igienico-sanitarie e di sicurezza, diritti sindacali e di associazione e rappresentanza richiesti dalla normativa del paese in cui essi operano. Deve essere, altresì, verificato il rispetto delle regole di correttezza e di buon comportamento nell'ambiente di lavoro ed in ogni caso deve essere posta particolare attenzione a situazioni lavorative anormali o abnormi;
- le disposizioni in materia di retribuzioni (specifiche per ogni categoria lavorativa), di orari di lavoro, di periodi di riposo, di aspettativa obbligatoria e ferie devono essere definite in conformità con quanto previsto dalla Legge, dai Contratti collettivi di lavoro applicabili e dai contratti integrativi eventualmente sottoscritti dalla Società;
- l'utilizzo di eventuali sistemi di sorveglianza (quali telecamere, impianti audio, ecc.) richiesti da esigenze organizzative e produttive, deve avvenire nel rispetto di quanto previsto dalla Legge, dallo Statuto dei lavoratori e previo accordo con le rappresentanze sindacali oppure tramite altre forme previste dalla normativa vigente;
- ASTER prevede il divieto assoluto per i propri dipendenti di accedere tramite il PC aziendale a siti Internet contenenti materiale relativo alla pornografia minorile e di scaricare o diffondere tale materiale;
- ASTER richiede al personale un corretto utilizzo degli strumenti informatici in proprio possesso rispettando le previsioni contenute nel Regolamento aziendale per l'utilizzo dei sistemi informativi e l'accesso alla rete internet;
- ASTER può effettuare, nel rispetto delle normative vigenti, controlli periodici per verificare il corretto utilizzo dei sistemi informativi aziendali;
- ASTER può bloccare qualsiasi accesso a siti internet o canali social (es. telegram, facebook, instagram etc.) dai computer aziendali, o da remoto in caso di smartworking, ove possano essere contenuti materiali pornografici o pedopornografici;
- la selezione delle controparti destinate a fornire particolari servizi (quali ad esempio le imprese con alta incidenza di manodopera non qualificata), siano essi Partner o Fornitori, deve essere svolta con particolare attenzione per evitare di incorrere nei rischi previsti in questa parte del Modello 231. In particolare, l'affidabilità di tali Partner o Fornitori deve essere valutata, ai fini della prevenzione dei Reati di cui alla presente sezione, anche attraverso specifiche indagini ex ante da svolgersi prima dell'affidamento dell'appalto.

6. REATI DI IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

6.1. I reati

Il D. Lgs. n. 109/2012 (pubblicato sulla G.U. n. 172 del 25 luglio 2012) ha ampliato ulteriormente il catalogo dei reati che possono generare una responsabilità diretta dell'ente, inserendo nel D. Lgs. 231/2001 l'art. 25-*duodecies*" Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

In sintesi, l'ente che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è soggetto ad una sanzione pecuniaria se i lavoratori occupati sono (circostanza alternative tra di loro):

- in numero superiore a tre;
- minori in età non lavorativa;
- esposti a situazioni di grave pericolo, con riferimento alle prestazioni da svolgere ed alle condizioni di lavoro.

Per un dettaglio del reato sopra citato e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

6.2. I processi sensibili ai fini del decreto

I processi a rischio sono stati individuati nei seguenti:

- selezione e assunzione del personale dipendente;
- gestione degli acquisti.

6.3. Regole di comportamento

È fatto obbligo a tutti i destinatari del Modello di:

- operare in conformità alle disposizioni contenute nel D. Lgs. 286/1998 (testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero) e s.m.i;
- impiegare soltanto lavoratori extracomunitari in possesso di valido permesso di soggiorno;
- richiedere ai lavoratori extracomunitari di esibire il permesso di soggiorno all'atto dell'assunzione e a seguito del rinnovo dello stesso;
- monitorare le scadenze dei permessi di soggiorno dei lavoratori extracomunitari;
- inviare comunicazioni e richiedere documenti ai dipendenti relativamente alle operazioni di rinnovo del permesso di soggiorno;
- archiviare correttamente la documentazione relativa al permesso di soggiorno;
- inviare le comunicazioni agli enti pubblici competenti assicurando che le informazioni trasmesse siano veritiere, complete e basate su idonea documentazione;
- nell'ipotesi di esecuzione di lavori eseguite da imprese in regime di appalto e subappalto nei contratti dovrà essere inserita specifica clausola 231.

È fatto divieto di impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale.

7. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

7.1. I reati

I delitti informatici introdotti nel D. Lgs. 231/2001 con l'art. 24-*bis* sono i seguenti, modificati a seguito della Legge n. 238/2021 avente ad oggetto *"Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020"*:

- Documenti informatici (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
- Intercettazione, impedimento e interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
- Detenzione, diffusione e installazione abusiva d'apparecchiature e di altri mezzi atti a intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informativi o telematici (art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105).

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia all'Allegato 1 al presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

7.2. I processi sensibili ai fini del decreto

In generale, sono individuati come processi a rischio, tutte quelle aree aziendali che, per lo svolgimento della propria attività, utilizzano strumenti informatici, e le funzioni che potrebbero accedere, quanto meno in linea teorica, agli strumenti informatici altrui. Le aree di attività ritenute più specificamente a rischio, individuate in sede di identificazione dei processi sensibili, sono state circoscritte nella "Gestione sistemi informatici e telematici", in cui vi sono ricompresi:

- Collegamento ai sistemi informativi di soggetti terzi;
- Collegamento ad archivi e banche dati per accedere alle quali sono richiesti codici di accesso;

- Gestione dei collegamenti ad internet;
- Gestione dei dispositivi USB.

7.3. Regole di comportamento

È fatto obbligo a carico di tutti i destinatari del Modello di rispettare il regolamento aziendale per l'utilizzo dei sistemi informatici e la rete internet. Più in generale è fatto obbligo di rispettare tutte le norme che disciplinano l'accesso e l'utilizzo dei sistemi e degli applicativi informatici della Società e che contengono principi cui attenersi.

È fatto espresso divieto di:

- accedere in maniera non autorizzata ai sistemi informativi degli utenti o della Pubblica Amministrazione o di alterarne in qualsiasi modo il funzionamento;
- di intervenire con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico altrui nei casi in cui l'intervento non sia stato autorizzato dal cliente o dalla controparte;
- detenere o diffondere abusivamente di codici di accesso a sistemi informatici o telematici;
- diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere il funzionamento di un sistema informatico o telematico;
- danneggiare informazioni, dati e programmi informatici;
- danneggiare informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

8. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO E DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

8.1. I reati

Il D. Lgs. 21 novembre 2007 n. 231, art. 63, co. 3 ha previsto una nuova forma di responsabilità dell'Ente conseguente alla commissione nel suo interesse o vantaggio degli illeciti amministrativi previsti nell'art 25-*octies*, D. Lgs. 231/01. Inoltre, il D.Lgs. 184/2021, recante l'"*Attuazione della direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio*", all'art. 3, prevede l'introduzione, nel D.Lgs. 231/2001, del nuovo art. 25-*octies*.1, rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*".
In particolare, i reati contemplati nei suddetti articoli sono:

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

- Autoriciclaggio (art. 648-ter.1 c.p.)
- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater)
- Frode informatica nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter)

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

8.2. I processi sensibili ai fini del decreto

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute a rischio, risultano le seguenti:

- gestione incassi;
- gestione pagamenti;
- gestione delle carte di credito, di debito e prepagate;
- tutti i processi sensibili indicati in relazione ai reati tributari.

8.3. Regole di comportamento

Fatto salvo il rispetto della normativa vigente in materia, del Codice Etico della Società e delle procedure aziendali, il sistema di controllo interno della Società finalizzato alla prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio si basa sui seguenti fattori:

- verifica dell'attendibilità commerciale e professionale dei fornitori e *partner* commerciali/finanziari;
- tenuta di un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge in tutte le attività finalizzate alla gestione anagrafica di fornitori/utenti/partner;
- verifica della regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- controlli formali e sostanziali dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie.

Inoltre, tutti i Destinatari del Modello dovranno attenersi ai seguenti principi di condotta:

1) non intrattenere rapporti commerciali 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;

2) non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
3) effettuare un costante monitoraggio dei flussi finanziari aziendali.

Per prevenire tali reati è fatto inoltre divieto di:

- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto nel caso in cui, utilizzando la normale diligenza professionale, sarebbe stato possibile individuare la provenienza illecita di quanto ricevuto. Costituiscono esempi di utilizzo di una normale diligenza professionale la verifica nelle operazioni di acquisto di beni che il prezzo applicato non sia sproporzionato rispetto ai valori medi di mercato, la verifica della regolarità dei pagamenti a fornitori, con riferimento alla piena coincidenza tra destinatari dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- intromettersi nel far acquistare cose provenienti da un qualsiasi delitto;
- sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo nel compimento di atti negoziali oppure in altre operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa;
- impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto nel caso in cui utilizzando la normale diligenza professionale sarebbe stato possibile individuare la provenienza illecita di quanto ricevuto.

Con particolare riferimento alle attività con valenza diretta ai fini tributari si rinvia ai principi di comportamento contenuti nella "*Parte speciale reati tributari*" di cui al presente Modello.

Relativamente alla prevenzione dei "Delitti in materia di strumenti di pagamento diversi dai contanti", devono essere applicati i seguenti presidi:

- la Società predilige l'utilizzo di strumenti di pagamento diversi dai contanti di tipo ricaricabile;
- lo strumento di pagamento viene preferibilmente ricaricato al momento in cui deve essere sostenuta una specifica spesa;
- la spesa deve essere autorizzata dal Responsabile dell'Ufficio a cui è imputabile la spesa stessa;
- tutti i pagamenti effettuati con strumenti di pagamento diversi dai contanti devono essere rendicontati e deve essere prodotta documentazione a giustificazione della spesa;
- periodicamente vengono monitorate le operazioni eseguite con strumenti di pagamento diversi dai contati per verificare eventuali anomalie;
- ASTER può effettuare, nel rispetto delle normative vigenti, controlli periodici per verificare il corretto utilizzo dei sistemi informatici aziendali.

9. REATI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

9.1. I reati

L'art. 25-*decies* del D. Lgs. 231/2001 prevede il reato di induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria, previsto dall'art. 377-*bis* c.p., che punisce, salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha facoltà di non rispondere.

Per un dettaglio del reato sopra citati e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

9.2. I processi sensibili ai fini del decreto

Attraverso l'attività di risk assessment condotta le attività sensibili individuate nell'ambito delle quali potenzialmente potrebbe essere commesso il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria previsto dall'art. 25-*decies* del D. Lgs. 231/2001 sono:

- gestione dei contenziosi giudiziali e stragiudiziali e procedimenti arbitrali che riguardano la Società o un suo rappresentante nell'esercizio delle attività aziendali.

9.3. Regole di comportamento

Per le operazioni riguardanti la gestione dei rapporti con soggetti che nell'ambito di un procedimento giudiziario hanno facoltà di non rispondere, la seguente parte speciale prevede che:

- tutti i destinatari del Modello adottino prassi e comportamenti che siano rispettosi del Codice etico e del Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001;
- che tutti i destinatari del Modello provvedano a fornire in modo chiaro, veritiero e corretto tutte le informazioni richieste all'Autorità giudiziaria nei procedimenti che coinvolgono la Società o suoi esponenti aziendali per attività svolte nell'ambito del loro incarico;
- l'Organismo di Vigilanza venga informato dall'Amministratore di eventuali procedimenti penali su reati compresi nel D. Lgs. 231/2001.

È fatto divieto di indurre un dipendente, collaboratore o altro soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria anche se da tale comportamento potrebbe derivare un (apparente ma, di fatto, inesistente per le responsabilità conseguenti) vantaggio (illecito) per la Società.

10. REATI DI RAZZISMO E XENOFOBIA

10.1. I reati

La presente Parte Speciale si riferisce ai reati di razzismo e xenofobia richiamati dalle disposizioni di cui all'art. 25-terdecies del D. Lgs. 231/2001.

Per un dettaglio del reato sopra citati e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

10.2. I processi sensibili ai fini del decreto

Considerate le attività svolte da ASTER la probabilità di accadimento dei suddetti reati è considerata remota poiché la propaganda politica e le forme di discriminazione religiosa e razziale sono assolutamente vietate e condannate sia dalle regole contenute nel Codice Etico che dai principi e dalle linee guida inclusi nel presente Modello. Inoltre, allo stato attuale appare alquanto improbabile che il personale di ASTER compia attività di propaganda ovvero di istigazione o di incitamento ai crimini di genocidio o contro l'umanità allo scopo di generare un vantaggio a favore della società.
In un'ottica prudenziale, non potendo escludere a priori condotte illecite che possano integrare le suddette fattispecie dei reati, si è proceduto a svolgere un'attività di risk assessment.
Dall'analisi svolta si ritiene che in relazione al reato sopra esplicitato l'area che presenta un'esposizione al rischio seppur remota risultano essere quelle relativa alla gestione delle sponsorizzazioni, delle donazioni e la locazione "attiva" di fabbricati, automezzi e altri beni aziendali.

10.3. Regole di comportamento

La presente parte speciale prevede, nell'espletamento delle attività considerate a rischio, l'espresso divieto per gli esponenti aziendali ed i collaboratori esterni di:

- nel corso dell'attività aziendale promuovere, costituire, organizzare o dirigere associazioni che si propongono il compimento di atti di razzismo e xenofobia;
- fornire, direttamente o indirettamente, tramite sponsorizzazioni o donazioni le risorse monetarie a favore di soggetti che intendano porre in essere reati di razzismo e xenofobia;
- operare in contrasto con le regole contenute nel Codice Etico per quanto riguarda le attività di pubblicità e di sponsorizzazione;
- assumere o assegnare commesse o effettuare qualsivoglia operazione commerciale e/o finanziaria, sia in via diretta, che per il tramite di interposta persona, che abbia come scopo quello di concorrere al compimento di atti di razzismo e xenofobia.

11. DELITTI DI CRIMINALITA' ORGANIZZATA

11.1. I reati

La Legge 94/2009 ha introdotto l'art. 24-*ter* ampliando il novero dei reati presupposto includendo c.d. delitti di criminalità organizzata.

Le fattispecie di reato contenute nell'art. 24-*ter* sono le seguenti:

- Associazione per delinquere, anche finalizzata a commettere delitti di riduzione o mantenimento in schiavitù, tratta di persone, acquisto o alienazione di schiavi, violazione delle disposizioni sull'immigrazione clandestina (art. 416 e 416 co.6 c.p.);
- associazione di tipo mafioso anche straniere (art. 416 bis c.p.);
- delitti commessi al fine di agevolare l'attività di associazioni mafiose;
- scambio elettorale politico mafioso (art. 416 ter c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DPR n. 309);
- sequestro di persona a scopo di estorsione (art. 630 c.p.);
- illegale fabbricazione, introduzione nello stato, messa in vendita, cessione, detenzione e porto in luogo pubblico di armi da guerra o esplosivi o di armi clandestine nonché di più comuni armi da sparo (art. 407 c.p.p.)

Per un dettaglio dei reati sopra citati e delle sanzioni 231 applicabili si rinvia al documento n. 7 del presente modello denominato "*Elenco dei reati presupposto della responsabilità amministrativa*".

11.2. I processi sensibili ai fini del decreto

Le attività sensibili individuate in relazione ai reati previsti dall'art. 24-ter del D.Lgs. 231/2001 riguardano:

- gestione appalti;
- gestione rapporti con consulenti (a titolo esemplificativo ma non esaustivo Avvocati, Dottori Commercialisti, Intermediari Finanziari etc) al fine di creare un'associazione finalizzata all'ottenimento di vantaggi tributari o di qualsivoglia altra natura;
- assunzione personale;
- gestione delle donazioni, sponsorizzazione e liberalità.

11.3. Regole di comportamento

Nell'espletamento della propria attività, tutti i dipendenti di ASTER sono tenuti al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico.

Per prevenire il rischio di commissione dei reati previsti nell'art. 24-*ter* del D. Lgs. 231/2001 è necessario:

- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuto o sospettato lo svolgimento di attività illecite con riferimento alle fattispecie di reato di cui all'art. 24-*ter*;
- tenere un comportamento corretto, trasparente e collaborativo nel rispetto delle norme di legge e delle procedure interne nello svolgimento delle attività afferenti le attività sensibili;
- verificare l'esistenza di requisiti che attestino l'onorabilità e la liceità di condotta dei fornitori, appaltatori, consulenti, agenti, partner commerciali coinvolti nelle attività sensibili sia in sede di instaurazione, sia in sede di svolgimento del rapporto con gli stessi;
- non riconoscere, in favore dei collaboratori, consulenti, appaltatori, agenti e fornitori, compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alla prassi vigente nel settore di attività interessato;
- assicurare che gli accordi con consulenti siano formalizzati mediante redazione di un contratto/lettera d'incarico, debitamente autorizzato da soggetti muniti di idonei poteri e che riporti indicazione del compenso pattuito, del dettaglio dell'eventuale prestazione di servizi da effettuare e di eventuali *deliverable* da produrre in relazione all'attività svolta (nel caso in cui la prestazione stessa lo preveda);
- verificare l'effettiva erogazione della fornitura/adempimento della prestazione oggetto del rapporto contrattuale e degli eventuali stati di avanzamento;
- assicurare la corretta esistenza ed archiviazione di tutta la documentazione prodotta nell'ambito del processo di approvvigionamento di beni e servizi;
- effettuare tutte le attività di determinazione delle imposte dirette ed indirette nel rispetto delle procedure dell'Azienda e alla normativa vigente e alle circolari, istruzioni e risoluzioni emanate dalle Autorità pubbliche competenti (Agenzia delle Entrate, Ministero delle Finanze ecc.);
- assicurare che la selezione del personale avvenga sulla base di principi che garantiscano una valutazione dei candidati effettuata nel rispetto dei principi sanciti nel Codice Etico e che sia garantita la tracciabilità del processo di selezione mediante l'utilizzo di apposita documentazione nelle diverse fasi del processo;
- gestire le attività di assegnazione dei beni aziendali in ossequio alle policy/procedure aziendali in materia;
- verificare preliminarmente l'onorabilità dei soggetti, enti, associazioni, destinatari di donazioni e atti di liberalità, nonché di sponsorizzazione, mediante la raccolta di informazioni preliminari e/o richiesta di documentazione attestante l'esistenza dei requisiti di onorabilità in capo agli stessi;
- garantire che il valore, la natura e lo scopo del regalo/liberalità abbiano chiari scopi umanitari, di beneficienza, culturali, artistici e di ricerca scientifica e siano considerati legali ed eticamente corretti.