ALLEGATO C.)

SISTEMA INFORMATIVO FUNZIONALE ALLA APPLICAZIONE DELL'ART. 7 D.LGS. 231/2001.

0.3.) Avvertenza.

1.) ISTITUZIONE E GESTIONE DEL SISTEMA.

1.0.) Avvertenza.
Nel prosieguo, per brevità, SASSARI AMBIENTE Società Consortile A.r.l. verrà indicata semplicemente come "Società"
1.1.) La Società istituisce un'articolazione aziendale, denominata "*Segreteria 231*", a cui conferisce il compito di organizzare e gestire un sistema di flussi informativi, aventi ad oggetto il concreto operato dei Soggetti di cui alla lettera b.) dell'art. 5 D.lgs. 231/2001: "*persone sottoposte alla direzione o alla vigilanza*" [N.d.R., di seguito indicati come: "Sottoposti"].

Le informazioni (dati e notizie), contenute in tali flussi, sono indispensabili per il concreto esercizio degli obblighi "*di direzione o vigilanza*", indicati dall'art. 7, comma 1 D.lgs. 231/2001; obblighi incombenti sull'"*organo dirigente*", che per la "Società" è costituito dal Consiglio di Amministrazione [acronimo: CdA].

Tali obblighi – si ricorda - costituiscono una "specificazione" del potere /dovere di direzione e controllo, che l'art. 2086 Cod. civ. pone in capo all'*"Imprenditore*" (e, per richiamo, dell'art. 2380- bis, in capo agli Amministratori di Società commerciali).

1.2.) Il sistema di flussi viene organizzato e gestito con modalità tali da renderlo:

- effettivo, in quanto concretamente attuato;
- efficace, in quanto idoneo a/capace di "scoprire" tempestivamente gli eventi sintomatici, indicatori di rischio di commissione di illeciti o anche di irregolarità costituenti violazione di principi e regole comportamentali aziendali;
- probatorio, in quanto in grado di dimostrare la propria effettività ed efficacia, per il tramite di documenti (cartacei o digitali).

2.) IL SISTEMA.

Si espone una sintesi della "struttura" del sistema.

2.1.) L'IMPOSTAZIONE.

Il sistema è impostato per attestare documentalmente:

- la costante vigilanza del CdA, sulla liceità e regolarità dell'attività aziendale;
- la tempestiva scoperta/intercettazione di situazioni costituenti indici/segnali di rischio, detti: "eventi sintomatici".

Per regolarità si intende la conformità dell'attività lavorativa dei Sottoposti: sia a disposizioni di legge e sia anche ai principi ed alle regole aziendali, contenute nel "Codice Etico" e nel MOG.

Per "evento sintomatico" si intende ogni atto/fatto/situazione che sia ragionevolmente indicativo:

- o della possibile commissione di illeciti, ad opera di Sottoposti
- oppure della violazione del MOG e dei suoi Allegati, da parte di Sottoposti.

Più esplicitamente, il sistema informativo dell'Allegato C.) è strutturato per intercettare anche eventi che non integrano i "reati presupposto" del D. lgs. 231; ma che possono incidere sulla legalità e regolarità dell'attività aziendale.

Ciò in applicazione della previsione contenuta nell'art. 7 D.lgs. 231/2001
"3. Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio".

2.2.) I SOGGETTI.

Il CdA ha individuato i Soggetti (definiti: "Referenti informativi") che, per la loro collocazione nell'organigramma aziendale, sono in grado di:

- verificare la "regolarità" dello svolgimento dell'attività aziendale;
- rilevare l'insorgenza di "eventi sintomatici" (quali sopra definiti).

Ai "Referenti", una volta debitamente istruiti sull'utilizzo del "Sistema", è stato assegnato il compito/mansione lavorativo/a di operare le predette verifica e rilevazione, utilizzando i "Moduli", di cui ai paragrafi successivi.

2.3.) LE INFORMAZIONI

Le informazioni (dati e notizie), che alimenteranno i flussi informativi su cui si articola il sistema sono calibrate sulla funzione, per la quale il sistema viene istituito; che è quella di vigilare sull'operato dei Sottoposti.

Conseguentemente, sono state selezionate (per l'inserimento nei flussi) le informazioni ritenute rilevanti, per la prevenzione del rischio di illiceità o irregolarità.

In particolare, per quanto concerne il rischio di commissione di "reati presupposto", di cui è ragionevole ipotizzare un rischio di commissione da parte dei Sottoposti, ci si è limitati a quelli di cui agli articoli: **24; 24-bis; 25; 25-qiunquies; 25-septies; 25-decies; 25-undecies; 25-quinquiesdecies**.

Ciò, per la ragione che il rischio che i Sottoposti commettano gli altri reati previsti dal "catalogo 231", è da ritenersi **altamente improbabile**.

2.3.) I DUE FLUSSI "INCROCIATI".

Il Sistema si articola su due flussi informativi:

- uno impostato per rilevare gli "Eventi sintomatici" (segnalazioni ad hoc);
- l'altro impostato per accertare sistematicamente la regolarità dell'operato dei Sottoposti (segnalazioni periodiche).

PROCEDURA IES.

Trattasi della procedimentalizzazione di un sistema di segnalazione dell'accadimento di "**eventi sintomatici"** [acronimo: ES]**,** che il Referente Informativo della Struttura aziendale interessata (dall'evento) dovrà inviare di propria iniziativa alla Segreteria 231, nella immediatezza della conoscenza dell'accadimento dell'evento.

La segnalazione avviene tramite il "**MODULO IES"**, che la Segreteria registra aprendo la relativa pratica che successivamente gestisce sino alla chiusura.

PROCEDURA RAM.

Trattasi dei report mensili di vigilanza sulla regolarità dell'andamento dell'attività aziendale, da inviare alla Segreteria 231, dietro interpello di quest'ultima.

La procedura funziona a cadenza mensile e con metodo ad "interpello con risposta obbligata".

La Segreteria 231 interpella mensilmente tutti i Referenti informativi, e questi ultimi rispondono entro un termine fissato volta per volta.
L'interpello avviene con l'invio del "**Modulo RAM**" (Report andamento mensile dell'attività aziendale).
La Segreteria 231 monitora la continuità delle "risposte" e, se del caso, invia "avvisi di sollecito".

In caso di omissioni, o ritardi ingiustificati, la Segreteria 231 informa il CdA, per le conseguenti valutazioni.
La procedura è unica; mentre ad ogni Referente verrà inviato un modulo "personalizzato" sulla tipologia delle attività dei Sottoposti, operanti nella Struttura aziendale di riferimento.

4.) UTILIZZO DELLE INFORMAZIONI.

4.1.) Report mensili.

La Segreteria 231 "colleziona" i reports mensili (ne attesta l'acquisizione, ne opera la classificazione, catalogazione ed archiviazione) e li inoltra al "Controllo Interno" per la valutazione e le eventuali azioni correttive.

4.2.) Segnalazione eventi sintomatici.

4.2.1.) Ricevuto il modulo IES, la Segreteria 231:

- ne dà immediata notizia al Vertice direzionale (tramite inserzione sul "Portale" di cui al successivo paragrafo 5).
- Apre una specifica istruttoria.

4.2.2.) L'istruzione consiste nell'acquisire dati, documenti e altro materiale e nella valutazione della rilevanza vs. irrilevanza, ai fini dell'esercizio del potere/dovere di "Direzione o vigilanza" di cui all'art. 7 comma 1 citato.

4.2.3.) I risultati dell'istruttoria vengono trasmessi al CdA; che ne prende conoscenza e ne opera valutazione (sempre tramite inserzione sul Portale).

Il Cda (sempre tramite portale) invia la propria valutazione all'OdV; al quale compete la decisione finale sull'evento segnalato.

5.) INFORMATIZZAZIONE DEL SISTEMA.

Le attività descritte al precedente paragrafo sono state informatizzate ed avvengono per il tramite di un "Portale 231" dedicato al Sistema.

Il Portale è collocato nella Sezione "Decreto legislativo 231_2001" del Sito istituzionale della Società ed accessibile tramite login "Portale 231".

Se ne illustra sinteticamente il funzionamento.

5.1.) PROCEDURA IES

La Sezione dedicata è titolata "Protocollo".

Ricevuto un MODULO IES, la Segreteria, dopo averne operato registrazione e averne rilasciato ricevuta, carica sul Portale:

- modulo e relativi allegati (se esistenti).
- le attività successive (sia della Segreteria che delle strutture aziendali cointeressate) svolte in relazione all'Evento segnalato.

Il sistema attribuisce, in automatico, data e numero progressivo di registrazione di protocollo.

All'atto dell'attribuzione del numero di protocollo, il Sistema invia in automatico mail ai Soggetti, individuati quali Destinatari e quindi abilitati all'accesso, per informarli.

Il "Protocollo" rimane aperto e la Segreteria carica tutti i documenti che pervengano successivamente.

A questo punto esistono due possibili evoluzioni.

i.) La Segreteria, valutato l'ES, se ritiene che abbia dei seguiti e che questi ultimi non siano imminenti; opera una "Valutazione provvisoria".

In tal caso il Protocollo rimane "aperto" in attesa dei seguiti.

Anche del caricamento della "Valutazione provvisoria" viene data informazione in automatico.

ii.) Diversamente, se la Segreteria ritiene che l'ES non abbia evoluzioni successive esprime la "Valutazione definitiva"

La valutazione comprende: identificazione dell'ES, l'indicazione del Referente, gli estremi di registrazione (generale e speciale), una sintetica descrizione, le indicazione delle attività svolte e una "valutazione".

La valutazione comprende: la potenziale rilevanza dell'ES ai fini del D.lgs 231; eventuali considerazioni sulla casistica generale in cui si colloca l'ES e un "commento".

Al caricamento della "Valutazione definitiva" il Portale, in automatico, invia una mail al Presidente del C.d.A. e, per conoscenza, all'O.d.V.

Con la "Valutazione definitiva" il compito della Segreteria si conclude.

i.i.i.) Il C.d.A., esaminata la "Valutazione definitiva":

- se la condivide, la "approva" e, in questo caso, il Sistema informa l'O.d.V. dell'approvazione;

- se non la condivide, informa la Segreteria, esponendo le ragioni della mancata approvazione e richiedendo un supplemento di istruttoria.

Nel secondo caso, il Protocollo si riapre per il caricamento delle attività successive.

i.v.) All'O.d.V compete la decisione finale, ai fini della responsabilità ex D.lgs. 231/2001.

Conseguentemente l'OdV:

- decide la "archiviazione" della segnalazione;
- oppure richiede un supplemento di istruttoria.

5.2.) ALTRE SEZIONI.

IL Portale comprende anche le altre "Sezioni", che vanno a descriversi.

5.2.1.) MODULI RAM.

La Sezione dedicata è titolata "Archiviazione RAM".

La Segreteria, una volta ricevuti i MODULI RAM" e averli trasmessi al "Controllo interno", li carica sulla apposita sezione del Portale; in modo da consentirne la conoscenza ai Soggetti abilitati alla consultazione.

5.2.2.) RELAZIONI DELLA SEGRETERIA.

In questa Sezione la Segreteria carica le proprie "Relazioni mensili" e la "Relazione annuale" sul funzionamento del Sistema.

5.2.3.) RELAZIONI DEL C.d.A.

In questa il CdA carica le proprie "Relazioni", quali previste dal MOG.

5.2.4.) RELAZIONI O.d.V.

Sezione dedicata alle "Relazioni" dell'Organismo di Vigilanza.

APPENDICE DI CHIARIMENTI

Al fine di prevenire ed evitare possibili interpretazioni equivoche od errate del presente Allegato, si forniscono alcune considerazioni di chiarimento e precisazione.

A.) COESISTENZA ED INTERAZIONE DI DUE TIPOLOGIE DI FLUSSI INFORMATIVI.

Il MOG di NOME SOCIETA' è "unico"; nel senso che "copre" il rischio di commissione di reati: sia da parte degli Apicali, che da parte dei Sottoposti ed è impostato sull'art. 6 D.lgs. 231/2001 [N.d.r. articolo che concerne il rischio di commissione dei reati-presupposto, ad opera degli Apicali (e non anche dei Sottoposti)].

Stante tale impostazione il MOG della Società prevede e disciplina i flussi informativi, quali previsti dall'art. 6, comma 2 lettera d.) del D.lgs. 231/2001; ossia: flussi di informazioni rivolti unicamente verso **l'OdV.**

Ne consegue che il MOG non prevede e, quindi, non disciplina/procedimentalizza flussi informativi, il cui destinatario sia l'"*organo dirigente*" [che, nel caso della Società ,è il Consiglio di amministrazione (acronimo: CdA)].

Si ricorda come il CdA (impersonando l'istituto giuridico dell' Imprenditore) sia comunque titolare del dovere/potere di direzione e controllo sull'operato dei "Collaboratori", previsto dall'art. 2086 Cod. civ e dall'art. 7 comma 1 D.lgs. 231/2001. Potere che espleta (o dovere che assolve) attraverso gli strumenti del cd. "controllo di gestione" / "controllo interno" (internal audit).
Una componente essenziale ed imprescindibile di tali controlli sono i flussi informativi sull'andamento della gestione aziendale; il che significa: sul concreto operato dei Sottoposti.

Viene quindi ad integrarsi una **coesistenza**, all'interno di uno stesso Ente, di due flussi informativi; che sono diversi, per oggetto e Destinatario.
I flussi previsti dall'art. 6 lettera d.), aventi:

- quale oggetto "*il funzionamento e l'osservanza dei modelli*",
- quale Destinatario il solo OdV.

I flussi propri del controllo interno, aventi:

- quale oggetto la gestione aziendale (scilicet: l'operato dei Sottoposti)
- quale Destinatario il solo CdA.

Come anticipato, il MOG della Società prevede, disciplina / procedimentalizza solo i flussi, aventi quali Destinatario l'OdV; mentre i flussi propri del controllo interno non sono previsti e procedimentalizzati.

Eppure tali flussi interagiscono con il sistema di Compliance 231; in quanto costituisco la fonte dei dati che implementano i flussi, procedimentalizzati dal MOG

Tali coesistenza ed interazione potrebbero indurre il dubbio di essere fonte di disfunzioni o sovrapposizioni pregiudizievoli al funzionamento sua del controllo di gestione che della Compliance 231.

Tale dubbio, pur possibile, sarebbe infondato; come va a dimostrarsi.

Tale coesistenza è **fisiologica** ed è esplicitamente prevista e "spiegata" nelle Linee Guida Confindustria (Ed. 2021, pagina 90); ciò, nei termini che integralmente si riportano: "*Con particolare riferimento ai flussi informativi periodici provenienti dal management, se prevedono l'obbligo di comunicare gli esiti di controlli già effettuati e non la trasmissione di informazioni o documenti da controllare, tali flussi periodici fanno chiarezza* ***sui diversi ruoli in materia di prevenzione.*** *Infatti se ben definiti i flussi informativi precisano che il management* ***deve esercitare l'azione di controllo****, mentre l'OdV – quale meccanismo di Assurance –* ***deve valutare i controlli effettuati dal management***".

Chiarita la diversità di ruoli, le Guide Lines prevedono il **coordinamento** dei due flussi informativi: "*Pur nel rispetto dei rispettivi ruoli nel sistema dei controlli interni, sarebbe poi auspicabile, anche in ottica di superamento della separazione e duplicazione delle verifiche, nonché del rischio di corto circuito informativo, uno scambio di flussi informativi tra funzione internal audit e l'OdV sulle risultanze delle rispettive attività di verifica che abbiano una rilevanza comune ai fini 231"* (Linee guida, pag. 90).

Quanto esposto previene il dubbio di un possibile "conflitto" tra il presente Allegato C.) e le parti del MOG della società, che trattano dei flussi informativi verso,

B.) RAPPORTI CON IL REGIME WHISTEBLOWING.

Analogo dubbio si pone in merito a interferenze: tra il presente Allegato C.) e il sistema del Whisteblowing, previsto dal MOG della Società Occorre chiarire i rapporti tra

- le informazioni sugli eventi sintomatici (IES) del presente Allegato C;
- le segnalazioni, in regime di Whisteblowing.

Ad un esame superficiale parrebbe ricorrere una sovrapposizione.
Tale apparenza è fallace, in quanto IES e segnalazione WB hanno Attori e condizioni di utilizzo diverse.

B.1.) Le IES:

i. avvengono ad opera dei **soli** "Referenti informativi";
ii. costituiscono un'**obbligazione lavorativa** (cfr. art. 2104 secondo comma c.c.);
iii. comprendono eventi che appaiono rischiosi, **indipendentemente** dal loro avveramento o possibile avveramento;
iv. riguardano la **regolarità** dell'attività aziendale e non la sola commissione di illeciti;
v. hanno come Destinatario il **CdA**;
vi. sono regolate da una procedura aziendale (il presente Allegato C) e conseguentemente sono **svincolate** dal regime "tutelativo", previsto dal D.lgs. 24/2023.

B.2.) Le segnalazioni WB:

i. avvengono ad opera di tutti i Soggetti, indicati dall'art. 3 D.lgs. 24/2023
ii. **non** costituiscono un'obbligazione lavorativa, ma una facoltà del Segnalante;
iii. comprendono atti/fatti/situazioni che appaiono al WB o come **accaduti**, oppure come di probabile accadimento;
iv. riguardano la commissione **degli illeciti** indicati dal D.lgs. 24/2023 o le violazioni del MOG;
v. hanno come Destinatario l'**OdV**;
vi. sono regolate dal **regime** dettato dal D.lgs. 24/2023, come attuato dal MOG della Società.

B.3.) L'unica interferenza che potrebbe porsi è quella riferita ai "Referenti informativi", nel caso in cui Essi vengano a conoscenza di un atto/fatto/situazione, rientrante nell'ambito di operatività dell'art. 1 D.lgs. 24/2023.
In tal caso si pone il problema se i "Referenti" debbano operare una IES oppure una segnalazione WB?
A più attento esame tale interferenza non si pone.

I Referenti informativi sono tenuti a operare una IES.
Trattandosi di un'obbligazione lavorativa ex art. 2104 comma 2); è automatico che l'obbligo prevalga sulla facoltà.

La funzione del sistema WB è quella di "difendere l'integrità" dell'Ente, segnalando la commissione (reale o solo potenziale) di una serie di illeciti a Chi ha il potere di prevenire e contrastare tale commissione.
Orbene, il CdA è il titolare di tale potere; che costituisce anche un dovere (cfr. art. 7 comma 1 D.lgs. 231/2001).
Conseguentemente la IES assolve alla identica funzione della segnalazione WB; pur essendo esclusa dal regime "protettivo" del D.lgs. 24/2023.

B.4.) Esiste un unico caso in cui il Referente informativo deve optare per una segnalazione WB.
Il caso è quello che l'evento riguardi un illecito commesso, o di possibile commissione, da parte di un Soggetto appartenente al CdA.
In questo caso, per ovvie ragioni, il Referente informativo opererà unicamente una segnalazione WB.

C.) INDEBOLIMENTO VS. RAFFORZAMENTO.

Da ultimo, ma non ultimo va prevenuta una possibile critica.

Limitare il sistema informativo ex art. 7, disciplinato dal presente Allegato C.), solo ad alcuni reati-presupposto potrebbe apparire come un "indebolimento" del sistema di "Compliance 231" della Società.

Si tratterebbe di una falsa apparenza.

Il MOG la Società è "unico" nel senso che previene il rischio di commissione di reati: sia da parte degli Apicali, che da parte dei Sottoposti.

Il MOG della Società è impostato sull'art. 6 D.lgs. 213/2001, che concerne il rischio di commissione dei reati-presupposto, ad opera di Apicali; mentre quello relativo ai Sottoposti è regolato dall'articolo 7.

L'unificazione dei due rischi in un unico MOG, impostato sull'art. 6, produce il duplice effetto:

a) di estendere ai Sottoposti un sistema preventivo, che il Legislatore ha disposto per i soli Apicali;
b) di non prevedere e regolare un sistema specifico, rivolto al rischio reati ad opera dei Sottoposti, che il Legislatore ha pur considerato nell'art. 7.

Stante l'effetto sub a.), il rischio della commissione di un reato, diverso da quelli contemplati nel presente Allegato, da parte di un Sottoposto, risulta comunque coperto dalle misure preventive, previste dal MOG.

Il che esclude che la adozione di un sistema preventivo, impostato sull'art. 7 produca un indebolimento nel sistema preventivo del MOG della Società.

Per contro, l'adozione di un sistema, impostato sull'art. 7, "rafforza" il MOG unico, integrandolo e completandolo, con misure preventive specifiche "dedicate" al rischio della commissione di reati da parte di Sottoposti.

Più esplicitamente: la inserzione, tra le misure previste dal MOG della Società di un'ulteriore misura "specifica" dedicata ai soli Sottoposti e riferita solo ad alcuni reati costituisce un completamento e quindi un rafforzamento del sistema preventivo ex D.lgs. 231 della Società