MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(Decreto Legislativo n. 231/2001 e s.m.i.)

MEMC ELECTRONIC MATERIALS S.P.A.

PARTE GENERALE

Approvato con delibera del Consiglio di Amministrazione del 26/11/2024

Indice

DEFINIZIONI 3
PREMESSA 5
1. SCOPO DEL DECRETO LEGISLATIVO N. 231/2001 E SUA APPLICAZIONE 5
2. ATTUAZIONE DELL'ART. 6 DEL DECRETO LEGISLATIVO N. 231/2001 7
3. FUNZIONE DEL MODELLO 7
4. DESTINATARI DEL MODELLO 9
5. ETICA E RISPETTO DELLE NORMATIVE 9
6. LE *POLICIES*, GLI STANDARD, LE PROCEDURE ED I RIFERIMENTI DI DERIVAZIONE TAIWANESE 10
7. IL CODICE ETICO 14
8. LE PROCEDURE 15
9. LA FORMAZIONE 16
10. L'ORGANIZZAZIONE AZIENDALE 17
11. L'ATTRIBUZIONE DI POTERI 18
12. LA REVISIONE ESTERNA – L'INTERNAL AUDIT 18
13. I RIFERIMENTI CONTRATTUALI 19
14. FORMAZIONE DEI PROCESSI DECISIONALI 20
15. IL RUOLO SVOLTO DALL'ORGANISMO INDICATO DALL'ART. 6 DEL DECRETO: 21
16. VERIFICHE PERIODICHE DEL MODELLO 25
17. SEGNALAZIONI IN MATERIA DI WHISTLEBLOWING 26
18. SISTEMA DISCIPLINARE 34

DEFINIZIONI

Le seguenti definizioni si riferiscono a tutte le parti del Modello, fatte salve ulteriori eventuali definizioni contenute nella Parte Speciale.

GlobalWafers Co. Ltd: è la società capogruppo, con sede legale in Taiwan, quotata alla borsa valori locale.

GlobalWafers BV: è la società con sede legale in Olanda, appartenente al gruppo GlobalWafers e unica socia di Memc Electronic Materials S.p.A.

Aree a Rischio: le aree di attività della Società nel cui ambito risulta esservi il rischio di commissione dei Reati *ex* D. Lgs. 231/2001 che possono comportare la responsabilità amministrativa in capo alla Società, così come individuate nelle singole sezioni della Parte Speciale del presente Modello e meglio dettagliate nella matrice dei Processi e delle Attività Sensibili, allegata al documento.

CCNL: i Contratti Collettivi Nazionali di Lavoro applicati dalla Società.

Codice Etico: il codice etico adottato dalla Società nel dicembre 2023.

Collaboratori Esterni: i Consulenti, i Partner commerciali ed i Fornitori.

Organismo di Vigilanza (OdV): l'organismo interno di controllo preposto alla vigilanza sul funzionamento e sull'osservanza del Modello, nonché al relativo aggiornamento.

Consulenti: i soggetti che agiscono in nome e/o per conto della Società in forza di un mandato o di altro rapporto contrattuale di collaborazione professionale.

Destinatari: amministratori, sindaci, dirigenti e Dipendenti della Società e Collaboratori Esterni.

Dipendenti: i soggetti aventi un rapporto di lavoro subordinato con la Società, ivi compresi i dirigenti.

D.Lgs. 231/2001 o il Decreto: il D.Lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni.

Ente o Società: è la società Memc Electronic Materials S.p.A. o una sua unità organizzativa.

Fornitori: i fornitori di beni e servizi della Società.

Linee Guida: le Linee Guida adottate da Confindustria in data 7 marzo 2002 e successivi aggiornamenti ed integrazioni, per la predisposizione dei modelli di organizzazione, gestione e controllo ai sensi dell'art. 6, comma terzo, del D. Lgs. 231/2001.

Modello: il modello di organizzazione, gestione e controllo previsto dal D. Lgs. 231/2001.

Organi Sociali: il Consiglio di Amministrazione, il Collegio Sindacale e i loro componenti.

P.A.: la Pubblica Amministrazione e, con riferimento ai reati nei confronti della pubblica amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio.

Partner: le controparti contrattuali con le quali la Società addivenga ad una qualche forma di

collaborazione contrattualmente regolata (associazione temporanea d'impresa, *joint venture*, consorzi, licenza, agenzia, collaborazione in genere), ove destinate a cooperare con la Società nell'ambito delle Attività Sensibili.

Reati: le fattispecie di reato alle quali si applica la disciplina prevista dal D. Lgs. 231/2001 sulla responsabilità amministrativa degli enti.

PREMESSA

Il presente documento, adottato con delibera del Consiglio di Amministrazione del 26/11/2024, contiene le linee guida ed i principi generali di adozione descrittivi del Modello e si compone di una “Parte Generale”, nonché di una “Parte Speciale”.

La Parte Generale contiene una sintetica illustrazione del Decreto e dei suoi contenuti, oltre alle regole ed i principi generali del Modello, l’identificazione dell’Organismo di Vigilanza e la definizione dei compiti, poteri e funzioni di tale organismo, la descrizione dei sistemi di segnalazione, sanzionatorio e disciplinare; la definizione di un sistema di comunicazione, informazione e formazione sul Modello, nonché la previsione di verifiche periodiche e dell’aggiornamento del Modello.

La Parte Speciale contiene l’individuazione delle aree ed attività ritenute rilevanti per la Società, nonché la descrizione dei protocolli di controllo preventivi adottati in merito a ciascuna categoria di reato ritenuta rilevante per la Società ai sensi del D. Lgs. 231/2001. Essa comprende anche la “Matrice dei Processi e delle Attività Sensibili”, ovvero l’analisi di rischio concernente i Reati.

1. SCOPO DEL DECRETO LEGISLATIVO N. 231/2001 E SUA APPLICAZIONE

Il D. Lgs. 231/2001, rubricato “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica” ha introdotto per la prima volta in Italia la responsabilità in sede “penale” degli enti per alcuni reati commessi nell’interesse o a vantaggio degli stessi. Le norme ivi contenute identificano come soggetti attivi del reato persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione e il controllo dell’Ente o di una sua unità organizzativa e, infine, persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

I Reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell’Ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche ed integrazioni. Quanto ai Reati cui si applica la disciplina in esame, si tratta attualmente delle seguenti tipologie: (a) reati commessi nei rapporti con la Pubblica Amministrazione e contro il patrimonio dello Stato o di altro Ente Pubblico, (b) reati in tema di falsità in monete, carte di pubblico credito, valori di bollo e in strumenti o segni di riconoscimento, (c) reati in materia societaria (ivi compresi i reati di corruzione tra privati e istigazione alla corruzione tra privati), (d) reati con finalità di terrorismo e di eversione dell’ordine democratico, (e) reati contro la personalità individuale, (f) reati di abuso di informazioni privilegiate e di manipolazione di mercato, (g) delitti commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, (h) ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (i) reati transnazionali, (j) delitti informatici e di trattamento illecito di dati, (k) delitti in materia di

violazione del diritto di autore, (l) delitti contro l'industria e commercio, (m) delitti di criminalità organizzata, (n) delitti contro l'amministrazione della giustizia, (o) reati ambientali, (p) delitti in materia di immigrazione e condizione dello straniero, (q) delitti in tema di razzismo e xenofobia, (r) frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, (s) reati tributari, (t) delitti di contrabbando.

Presupposto essenziale per l'applicazione del Decreto è che gli illeciti siano commessi nell'interesse o a vantaggio delle società o degli enti destinatari della normativa:

a) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli enti o da una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitano, anche di fatto, la gestione e il controllo degli enti medesimi, nonché

b) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra.

È importante notare che, ai fini della configurazione dei reati previsti dal presente Decreto, non è necessario che la Società sia a conoscenza dei fatti compiuti dai soggetti summenzionati né che la Società abbia conseguito un vantaggio patrimoniale. È sufficiente che il reato sia commesso semplicemente a vantaggio o nell'interesse dell'ente; ovviamente l'interesse o il vantaggio dell'ente deve essere valutato *ex ante*.

Le sanzioni previste nell'ipotesi in cui venga commesso uno dei reati indicati nel Decreto sono: la sanzione pecuniaria, le sanzioni interdittive, la confisca e la pubblicazione della sentenza. Tra le sanzioni previste, le più gravi sono costituite dalle pene interdittive quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni o servizi.

Tuttavia, la Società non è responsabile se prova:

- di aver adottato ed implementato idonei modelli di organizzazione, gestione e controllo prima della commissione del reato;
- di aver affidato il compito di vigilare sul funzionamento e sull'osservanza dei modelli ad un organismo dotato di autonomi poteri di iniziativa e controllo;
- che le persone abbiano commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione;
- che non vi sia stata omessa vigilanza da parte dell'organismo preposto.

2. ATTUAZIONE DELL'ART. 6 DEL DECRETO LEGISLATIVO N. 231/2001

Con l'adozione del presente documento, si intende adempiere, anche sul piano formale, a quanto espressamente richiesto dall'art. 6 del Decreto in relazione alla prevista "adozione" dei modelli di organizzazione, gestione e controllo.

Nella stesura del documento si è tratto in parte spunto e indicazione dalle Linee Guida di Confindustria.

È necessario in ogni caso precisare che il Modello adottato dalla Società rinvia o si riferisce, in molti casi, ad una molteplicità di fonti e di riferimenti interni aziendali (es. procedure, Codice Etico, schemi e flussi di lavoro, ecc.) il cui testo non verrà riprodotto in questa sede per evidenti ragioni di sintesi e chiarezza espositiva. Tali fonti e riferimenti sono peraltro resi disponibili ai destinatari e reperibili ove necessario.

Il compito di curare, ove necessario, l'aggiornamento del Modello nonché di vigilare sul funzionamento e l'osservanza dello stesso spetta all'Organismo di Vigilanza ("OdV").

Con particolare riguardo all'attività di aggiornamento del Modello, al fine di assicurare la perfetta aderenza dello stesso rispetto a eventuali mutamenti aziendali o normativi che possano comportare un'estensione delle Aree a Rischio, l'OdV, anche attraverso l'ausilio di consulenti esterni, dovrà garantire la massima tempestività nell'attività di integrazione e di revisione dello stesso.

3. FUNZIONE DEL MODELLO

L'adozione del Modello da parte delle imprese non è obbligatoria, ma facoltativa.

Qui di seguito le modalità di redazione del Modello e i suoi scopi:

- individuare le aree di attività a rischio reato;
- verificare e documentare le operazioni a rischio;
- individuare un organo che svolga le funzioni di controllo e vigilanza previste dal Decreto;
- implementare i sistemi di controllo e vigilanza già esistenti all'interno della Società ed eventualmente colmare le lacune degli stessi;
- elaborare, secondo i principi dettati dal Decreto, nuove procedure di controllo per quei rischi non coperti dai sistemi di controllo e vigilanza esistenti;
- diffondere e sensibilizzare a tutti i livelli aziendali le regole di comportamento e le procedure istituite;
- ribadire che tutti i comportamenti illeciti sono condannati dalla Società in quanto contrari alle disposizioni di legge e alle prescrizioni del Codice Etico adottato da MEMC;
- consentire alla Società e conseguentemente all'OdV di intervenire tempestivamente per

prevenire e contrastare la commissione dei reati previsti dal Decreto.

La Società ha inteso adottare ed aggiornare il Modello previsto dal Decreto anche al fine di sensibilizzare tutti coloro che operano in nome e per conto della Società, affinché osservino, nello svolgimento delle proprie attività e mansioni, comportamenti corretti, tali da prevenire il rischio di commissione dei reati previsti dal legislatore.

Gli elementi che caratterizzano il presente Modello sono l'efficacia, la specificità e l'attualità.

L'efficacia

L'efficacia di un modello organizzativo dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da calmierare – o quantomeno ridurre significativamente – l'area di rischio da responsabilità. Tale idoneità è garantita dall'esistenza di meccanismi di controllo preventivo e successivo idonei a identificare le attività sensibili a rischio commissione reati, e segnalare eventuali condotte illecite. L'efficacia di un modello organizzativo, infatti, è anche funzione dell'efficienza degli strumenti idonei a identificare e prevenire la commissione/realizzazione dei reati *ex* D. Lgs. 231/2001.

La specificità

La specificità di un modello organizzativo è uno degli elementi che ne connota l'efficacia.

- È necessaria una specificità connessa alle aree a rischio, così come richiamata dall'art. 6, comma 2, lett. a), del D. Lgs. 231/2001, che impone un censimento delle attività nel cui ambito possono essere commessi i reati.
- È altrettanto necessaria una specificità dei processi di formazione delle decisioni dell'ente e dei processi di attuazione nei settori "sensibili", così come previsto dall'art. 6, comma 2, lett. b), del D. Lgs. 231/2001.

Il Modello deve tener conto delle caratteristiche proprie, delle dimensioni della Società e del tipo di attività svolte, nonché della storia della Società.

L'attualità

Si sottolinea che, per garantire l’efficacia del Modello di Organizzazione Gestione e Controllo adottato dalla Società, è necessaria una verifica nel continuo del funzionamento dello stesso ed un’attività di costante aggiornamento (in relazione ai mutamenti della struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati di cui al D. Lgs. 231/2001).

In tal senso l'art. 6 del D. Lgs. 231/2001 prevede che l'organismo di vigilanza, titolare di autonomi poteri d'iniziativa e controllo, abbia la funzione di aggiornare il Modello.

4. DESTINATARI DEL MODELLO

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, membro del collegio sindacale;
- a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società o in una sua unità organizzativa autonoma;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società o di una sua unità organizzativa;
- ai lavoratori subordinati della Società, compresi i Dipendenti, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale;
- a tutti quei soggetti che collaborano con la Società in forza di un rapporto di lavoro parasubordinato, quali collaboratori a progetto, prestatori di lavoro temporaneo, interinali, ecc.;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima;
- a quei soggetti che agiscono nell'interesse della Società, in quanto legati alla stessa da rapporti giuridici contrattuali o da accordi di altra natura, quali, ad esempio, partner in *joint-venture* o soci per la realizzazione o l'acquisizione di un progetto;
- a tutti i soggetti del Gruppo le cui attività/decisioni abbiano un impatto sulla Società.

Il Modello costituisce un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di materiali, servizi e lavori, consulenti, partners con cui MEMC opera.

5. ETICA E RISPETTO DELLE NORMATIVE

MEMC ha posto a fondamento della propria attività il più rigoroso rispetto delle normative e dei principi etico-comportamentali correnti. Tale valore è chiaramente ripreso e confermato in tutti gli standard e le procedure emessi da MEMC e/o dalla Capogruppo nel corso del tempo, a cui tutte le società del Gruppo, inclusa quindi anche MEMC, sono tenute ad attenersi.

Operando in ambito internazionale MEMC, d'altra parte, ha riconosciuto l'importanza fondamentale di operare in assoluta conformità con il contesto normativo locale o nazionale di riferimento, imponendo *policies*, standard e modelli di comportamento molto spesso più restrittivi di quelli imposti dalle varie legislazioni ed adottando uniformemente a livello internazionale procedure, criteri e metodologie di lavoro ritenuti idonei al fine di prevenire o accertare eventuali illeciti commessi dai propri dipendenti o rappresentanti.

Le *policies* adottate dalla Società riguardano: adempimenti doganali, acquisti, produzione, ricerca e sviluppo, commerciale, IT, comunicazione e marketing, personale, sicurezza sul lavoro e ambiente.

Esse sono contenute nel sistema DMS dell'Ente, accessibile soltanto ai Dipendenti mediante l'utilizzo di username e password, ad eccezione del Codice Etico, che è reperibile sul sistema intranet.

Ciascun Dipendente può accedere alle *policies* comuni a tutti e a quelle proprie della sua mansione.

6. LE *POLICIES*, GLI STANDARD, LE PROCEDURE ED I RIFERIMENTI DI DERIVAZIONE TAIWANESE

GlobalWafers Co. Ltd opera sul territorio italiano attraverso l'organizzazione di MEMC, il cui pacchetto azionario è integralmente detenuto dalla Società GlobalWafers B.V., con sede nei Paesi Bassi.

MEMC è diretta destinataria e responsabile dell'applicazione di tutte le *policies*, gli standard e le procedure (di seguito congiuntamente le "policies") emessi nel tempo dalla Capogruppo. MEMC elabora altresì le proprie *policies*. L'adozione delle *policies* deve essere conforme alla Procedura di Funzione dal titolo Amministrazione Sistema DMS.

Tale procedura, contenuta anch'essa nel Sistema DMS, ha lo scopo di riunire le informazioni per il controllo della documentazione *online*, gestita attraverso l'applicativo DMS.

La cogenza di tali documenti e le conseguenze disciplinari legate alla loro violazione sono chiaramente esplicitate a tutti i dipendenti.

Per quanto riguarda la archiviazione delle *policies*, esse sono contenute nel DMS di MEMC. La Procedura di Funzione dal titolo Amministrazione Sistema DMS prevede metodi automatizzati di conoscenza ai destinatari predefiniti.

7. LE AREE DI RISCHIO NELL'AMBITO DELLE ATTIVITA' DI MEMC ELECTRONIC MATERIALS S.P.A.

La Società ha un oggetto sociale ed una organizzazione particolarmente strutturati. Ciò comporta la necessità di monitorare attentamente l'esposizione al potenziale pericolo di commissione di illeciti che abbiano rilievo dal punto di vista del Decreto, con riguardo a tutte le attività della Società. Vi sono, tuttavia, ambiti in cui tale controllo deve essere svolto in modo particolarmente attento.

In particolare, la Società svolge le proprie attività verso una clientela composta da soggetti operanti in particolar modo in ambito privato. In ambito pubblico, MEMC stipula convenzioni con Università per questioni legate alla formazione (borse di studio) e alla ricerca e sviluppo, e dialoga con la P.A. per questioni relative a progetti strategici, volti all'ottenimento di finanziamenti. La Società interagisce con la P.A. anche come utente o fruitore dei servizi resi dalla stessa Pubblica Amministrazione.

Il fatto di dover interagire con rappresentanti di Enti, Autorità o Organismi pubblici costituisce senz'altro un fattore tipico e peculiare di rischio, soprattutto per quanto concerne l'accadimento di possibili fenomeni corruttivi. La nuova disciplina legislativa ha imposto in ogni caso una rivisitazione più ampia ed analitica degli ambiti di attività e dei processi aziendali che potrebbero costituire, almeno in linea teorica, presupposto per la commissione degli illeciti previsti dal Decreto.

Alla luce della struttura particolarmente articolata delle attività e dei processi della Società, è stata elaborata per tipologia di reato, attraverso un'approfondita analisi del contesto aziendale, la "Matrice dei Processi e delle Attività Sensibili" nel cui ambito esiste il rischio di commissione delle diverse fattispecie di illecito previste dal decreto.

Il risultato di tale concreta elaborazione, effettuata attraverso un'attenta analisi dell'attività sociale, delle *policies* e procedure aziendali, della documentazione societaria rilevante, e con l'apporto di Esponenti Aziendali che rivestono "funzioni chiave" all'interno della Società, si è inevitabilmente concentrato sui rischi di commissione di illecito che sono apparsi più significativi rispetto alla specifica realtà di MEMC. Il risultato dell'analisi sopra descritta viene trasposto nelle sezioni della Parte Speciale, alle quali si fa quindi rinvio per la specifica trattazione delle singole fattispecie di illecito, nonché nella "Matrice dei Processi e delle Attività Sensibili" allegata al Modello.

Nell'ambito di detta Matrice, sono state identificate le aree di attività "sensibili" alla commissione dei reati, vale a dire le attività nel cui ambito possono ipoteticamente crearsi le occasioni per la realizzazione dei comportamenti illeciti previsti dal Decreto.

L’analisi ha interessato:

- i reati di cui agli artt. 24 e 25 del Decreto (reati contro la pubblica amministrazione, contro il patrimonio commessi a danno dello Stato o di altro Ente pubblico);
- i reati di cui all’art. 25-ter del Decreto (c.d. reati societari), tra cui il reato di “corruzione tra privati” e di “istigazione alla corruzione tra privati” di cui alla lettera s- bis del medesimo articolo;
- i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro di cui all’art. 25-septies del Decreto;
- i delitti informatici e di trattamento illecito di dati di cui all’art. 24-bis del Decreto;
- i delitti di criminalità organizzata di cui all’art. 24-ter del Decreto;
- le falsità in monete in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento di cui all’art. 25-bis del Decreto;
- i delitti contro l’industria ed il commercio di cui all’art. 25-bis.1 del Decreto;
- i delitti in materia di violazione del diritto d’autore di cui all’art. 25-nonies del Decreto;
- i delitti contro l’amministrazione della giustizia di cui all’art. 25–decies del Decreto;
- i reati ambientali di cui all’art. 25-undecies del Decreto;
- i reati in materia di immigrazione e condizione dello straniero di cui all’art. 25- duodecies del Decreto;
- i reati contro la personalità individuale di cui all’art. 25 – quinquies del Decreto;
- i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio di cui all’art. 25-octies del Decreto;
- i delitti in tema di razzismo e xenofobia di cui all’art 25 – terdecies del Decreto;
- i reati tributari di cui all’art. 25 - quinquiesdecies del Decreto;
- i delitti di contrabbando di cui all’art. 25 – sexiesdecies del Decreto.

Dopo una valutazione preliminare sono stati esclusi dall’analisi di dettaglio i reati di terrorismo di cui all’art. 25-quater del Decreto, nonché i reati di abuso di informazioni privilegiate e di manipolazione di mercato di cui all’art 25-sexies ed i reati transnazionali, in quanto, pur non potendosi escludere del tutto la loro astratta verificabilità, la loro realizzazione in concreto è improbabile, sia in considerazione della realtà operativa della Società, sia in considerazione degli elementi necessari alla realizzazione dei reati in questione (con particolare riferimento per alcuni di essi all’elemento psicologico del reato).

Per quanto attiene al reato di associazione a delinquere *ex* art. 416 c.p., l'analisi si è concentrata sui profili di riconducibilità di detta fattispecie ai reati presi in considerazione nell'ambito della mappatura dei processi e delle attività sensibili. In sostanza, pur non potendosi escludere il richiamo dell'associazione a delinquere anche per fattispecie differenti rispetto a quelle oggetto di mappatura, l'analisi svolta ha considerato, nel rispetto dei principi espressi dagli artt. 2 e 3 del D. Lgs. 231/2001, i profili propri delle attività tipiche della realtà operativa della Società.

Per quanto attiene al reato di "autoriciclaggio", l'analisi, alla luce del rigoroso rispetto dei principi espressi dagli artt. 2 e 3 del D. Lgs. 231/2001, con particolare riferimento alla tassatività delle fattispecie presupposto, è stata condotta secondo due profili:

- considerando il reato di autoriciclaggio come modalità con cui potrebbero essere impiegati, sostituiti o trasferiti, nell'ambito dell'attività economico-imprenditoriale della Società, il denaro, i beni o altre utilità provenienti da reati non colposi che già costituiscono fattispecie presupposto ai fini del D. Lgs. 231/2001 oggetto di mappatura nell'analisi del rischio. In concreto, il reato di autoriciclaggio può essere considerato in tal senso come reato potenzialmente "conseguente" alle fattispecie presupposto di natura non-colposa già identificate in mappatura. Secondo questo profilo, i protocolli di controllo del reato "fonte" dell'autoriciclaggio, con esclusivo riferimento alle categorie di reato che rientrano nell'elenco delle fattispecie presupposto ai sensi del D. Lgs. 231/2001, sono quelli stabiliti nella parte speciale del modello per ogni macrocategoria di reato;
- considerando, inoltre, l'autoriciclaggio con attenzione al momento consumativo del reato stesso, con particolare riferimento alla clausola modale della norma che evidenzia, affinché si realizzi il reato di autoriciclaggio, la necessità di condotte volte ad ostacolare concretamente l'identificazione della provenienza delittuosa del denaro, beni o altre utilità derivanti dalla commissione di un qualsiasi delitto non colposo (quindi anche di quelli non oggetto di mappatura). Secondo questo profilo le analisi si sono concentrate sulla tracciabilità dei flussi finanziari e di tesoreria, essendo questi i processi in cui è concretamente ipotizzabile la condotta di ostacolo concreto all'identificazione della provenienza delittuosa, con particolare ma non esclusivo riferimento ai flussi connessi a operazioni di natura non ordinaria, quali ad esempio operazioni di aumento di capitale, anche mediante conferimento, di finanziamento da parte di soci, ecc.

Con riguardo ai reati tributari di cui all'art. 25-quinquiesdecies del Decreto, si rileva che sono stati ritenuti potenzialmente rilevanti tutti i reati indicati dalla norma:

- dichiarazione fraudolenta mediante fatture per operazioni inesistenti, previsto dall'art. 2 del D. Lgs. 74/2000;
- dichiarazione fraudolenta mediante altri artifici, previsto dall'art. 3 D. Lgs. 74/2000;
- emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'art. 8 D. Lgs. 74/2000;

- occultamento o distruzione di documenti contabili, previsto dall'art. 10 D. Lgs. 74/2000;
- sottrazione fraudolenta al pagamento di imposte, previsto dall'art. 11 D. Lgs. 74/2000.

Inoltre, in attuazione della c.d. "Direttiva PIF", sono stati introdotti anche i reati di:

- dichiarazione infedele, reato previsto dall'art. 4 D. Lgs. n. 74/2000;
- omessa dichiarazione, previsto dall'art. 5 D. Lgs. n. 74/2000;
- indebita compensazione previsto dall'art. 10-quater D. Lgs. n. 74/2000;

i quali rientrano nel perimetro di applicazione del D. Lgs. 231/2001 solo quando l'infedeltà dichiarativa riguardi l'IVA (è, quindi, escluso l'omologo reato previsto per le imposte sui redditi) e la condotta criminosa realizzi congiuntamente tutte le condizioni previste dal D. Lgs. n. 75/2020, quanto alle soglie di rilevanza (IVA evasa superiore ad euro 10 milioni) e alla commissione nell'ambito di sistemi fraudolenti transfrontalieri.

8. IL CODICE ETICO

Come già accennato, MEMC si è dotata di un Codice Etico, i cui contenuti sono ampiamente conosciuti da tutti i dipendenti. Tale Codice, infatti, è accessibile tramite il sistema intranet di MEMC, per i dipendenti, e anche sul sito internet di GlobalWafer Co.

Al fine di facilitarne la diffusione e comprensione, il Codice Etico è stato altresì tradotto in inglese e viene inviato a Consulenti e Fornitori.

Tale Codice Etico definisce in maniera chiara ed analitica i comportamenti vietati e ribadisce il carattere di cogenza e vincolatività delle regole etiche interne e la possibilità di comminare sanzioni disciplinari da parte della Società, commisurate alla gravità delle infrazioni accertate.

Il Codice Etico ha posto particolare enfasi sulla prevenzione degli illeciti indicati dal Decreto ed ampio spazio hanno trovato nel manuale i temi della corruzione e, più in generale, della necessità di adottare comportamenti etici nella conduzione del *business*.

Gli argomenti trattati all'interno del Codice Etico sono i seguenti: 1) Sistema di gestione; 2) Etica; 3) Dove ottenere aiuto; 4) Whistleblowing – Gestione delle segnalazioni di violazioni della legge, del Codice Etico e delle politiche MEMC Electronic Materials S.p.A.

Per la trattazione di ogni singolo argomento si rimanda alla visione e consultazione del Codice stesso.

I contenuti del Codice Etico sono costantemente al centro di iniziative di formazione e sensibilizzazione; tutti i dipendenti si sono impegnati a conoscerne ed applicarne le norme con una specifica dichiarazione (in versione elettronica).

L'OdV ha la specifica responsabilità di curare l'aggiornamento del Codice Etico.

Il Codice Etico è in ogni caso indicato come primaria fonte regolamentare all'interno di tutte le nuove procedure operative emesse dall'azienda nell'ambito del sistema di qualità e, pertanto, i precetti in esso indicati devono essere intesi come parte integrante ed essenziale dell'insieme delle norme e delle procedure applicabili in ciascun settore operativo della Società. Il Codice Etico è pertanto da considerarsi quale parte integrante del presente Modello.

Il Codice Etico viene altresì illustrato e consegnato a tutte le persone neoassunte all'atto dell'ingresso in azienda. Di tale attività viene conservata apposita registrazione.

9. LE PROCEDURE

Le procedure aziendali, che si trovano nel Sistema DMS dell'Ente, sono identificate, descritte e richiamate nell'ambito della documentazione prodotta e conservata dall'azienda ai fini delle certificazioni da parte di enti di qualità, sicurezza e ambiente. Infatti, da diversi anni MEMC si sottopone volontariamente ai controlli ed ai più avanzati standard dettati dalle norme di qualità nazionali ed internazionali e, a tale scopo, emette ed aggiorna periodicamente una serie di procedure e norme operative, aventi ad oggetto la regolamentazione dei principali processi e flussi di lavoro.

Le procedure sono accessibili dal Sistema DMS soltanto previo utilizzo di *username* e *password*. Ad ogni modo possono accedere al Sistema DMS soltanto i dipendenti e il primo accesso deve essere previamente autorizzato dal Responsabile di Funzione.

Le procedure che più specificatamente attengono all'area finanza sono sottoposte anche a controllo da parte dei revisori contabili e anche dal reparto Internal Audit.

Le procedure riguardano tutti gli ambiti di operatività aziendale e, quindi, anche quei processi transazionali o amministrativi nel cui ambito, ove non correttamente regolamentati o disciplinati, possono favorire la commissione degli illeciti indicati dal Decreto.

Ogni procedura viene verificata dal punto di vista normativo, deve essere ufficialmente approvata dalla Direzione o dai suoi delegati ed indica chiaramente una funzione aziendale responsabile dell'applicazione. Per ogni procedura viene chiarito lo scopo e vengono indicati i riferimenti, di qualità, di tutela ambientale, di sicurezza sul posto di lavoro e normativi.

Il contenuto delle procedure è reso facilmente accessibile attraverso un portale dedicato immediatamente accessibile tramite la pagina intranet, da cui si accede al sistema DMS; tutti i dipendenti sono chiamati in ogni caso a conoscere ed applicare le procedure di interesse rispetto al loro specifico ambito operativo.

Le stesse procedure, analogamente a quanto avviene per le *policies* emesse dalla Capogruppo taiwanese, sono intese dalla generalità dei dipendenti come strumenti cogenti di regolamentazione dei flussi di lavoro e di identificazione dei ruoli e delle responsabilità a livello aziendale.

Pur essendo le attività aziendali a maggiore rischio già regolate da specifiche procedure, la Società

– con la supervisione dell'OdV, secondo quanto previsto dalla "Procedura flussi informativi" menzionata di seguito – ritiene di monitorare costantemente la situazione e, ove necessario, formalizzare nuove, più complete e più chiare procedure in alcune delle aree di attività considerate a potenziale rischio, come più specificamente indicato nella Parte Speciale.

Tutto ciò al fine di prevenire in maniera ancor più efficace la commissione di alcuni degli illeciti previsti dalla normativa e favorire una miglior conoscenza ed omogenea applicazione delle regole interne da parte di tutti i dipendenti.

10. LA FORMAZIONE

I Dipendenti di MEMC sono destinatari di un'intensa e periodica attività formativa avente molto spesso ad oggetto i temi dell'etica e del rispetto delle normative.

Le iniziative formative sono organizzate e gestite dalle funzioni specialistiche interne, anche su indicazione dell'OdV. Non di rado sono coinvolti consulenti esterni ed esperti dei vari settori. La Società in generale promuove la partecipazione dei Dipendenti ad iniziative formative, sia interne che esterne.

I *records* relativi alle partecipazioni sono tenuti ed aggiornati su files elettronici dalla Direzione Risorse Umane e tutto il processo delle attività di formazione è oggetto di specifica ed analitica procedura secondo gli standard di qualità.

All'esito delle iniziative i Dipendenti sono sottoposti a test finali, che vengono correttamente registrati e conservati.

La funzione Risorse Umane, in particolare, eroga corsi a tutti i livelli dell'organizzazione aziendale incentrati sui temi etici e della conoscenza e dell'applicazione delle normative; in tali corsi viene ribadita la necessità di tenere comportamenti coerenti con il rispetto delle norme e delle *policies* Global Wafers e MEMC adottate a livello internazionale nonché, per quanto concerne più in particolare il tema della responsabilità amministrativa delle imprese derivante da atto illecito, l'esigenza di conformarsi scrupolosamente alle regole ed alle procedure interne finalizzate a prevenire la commissione degli illeciti indicati dal Decreto n. 231/2001.

Durante i corsi, differenziati nei contenuti e nelle modalità di erogazione in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della Società, vengono spiegati ai Dipendenti i contenuti principali delle norme (con particolare riferimento alle tipologie di illeciti al momento previsti dal Decreto) e sono chiarite le potenziali conseguenze, sia individuali che societarie, derivanti da eventuali comportamenti aventi rilievo penale.

Particolare enfasi viene posta nei corsi alla necessità di evitare qualsiasi tipo di coinvolgimento in comportamenti o atti corruttivi come pure alla necessità di impostare in maniera assolutamente corretta (anche dal punto di vista formale) i rapporti ed i contatti con la Pubblica Amministrazione e più in generale con i funzionari pubblici.

Una specifica e mirata attività formativa è rivolta anche ai nuovi assunti, ai quali, all'atto dell'ingresso in azienda, vengono individualmente ribaditi i principi ed i valori adottati da MEMC in materia di etica negli affari e vengono illustrati i principali contenuti del Codice Etico: i neoassunti dichiarano formalmente il proprio impegno personale attraverso apposita dichiarazione conservata negli archivi della funzione Risorse Umane.

Sui temi dell'amministrazione e del bilancio sono state organizzate iniziative formative (anch'esse gestite dalle funzioni specialistiche interne) finalizzate ad aumentare la conoscenza dei requisiti normativi e delle procedure aziendali da parte di coloro che operano su questi temi, allo scopo di ulteriormente ridurre i rischi di poter ricadere nelle ipotesi configurate dalla normativa come illecito. Tali corsi vengono ripetuti con cadenza periodica, anche al fine di coinvolgere eventuali nuovi addetti e per necessità di aggiornamento continuo sulla disciplina normativa.

Per quanto riguarda la sicurezza sul lavoro, la formazione è disciplinata nel Manuale per la sicurezza, salute, tutela ambientale e gestione energetica, contenuto nel Sistema DMS, che specifica che la formazione deve essere commisurata a compiti, ruoli e responsabilità di tutto il personale aziendale.

I criteri formativi (contenuti, modalità di erogazione, periodicità) in ambito di sicurezza, salute, tutela ambientale e gestione energetica ("ESH") sono stabiliti dal Servizio ESH con riferimento alle mansioni svolte dagli interessati ed ai relativi impatti ESH associati. La formazione include l'addestramento (formalizzato secondo ben definite procedure MEMC SpA) sulla postazione lavorativa e il corretto apprendimento è puntualmente valutato con idonei strumenti di verifica. La Società dispone di opportuni sistemi di tracciabilità della formazione ottenuta dal singolo Dipendente.

Più in generale, in ogni campo, MEMC verifica l'effettivo espletamento delle attività formative, in particolare sul tema dell'etica, è oggetto di un periodico audit condotto dalla funzione di *internal auditing*, i cui esiti sono poi condivisi con il management aziendale.

11. L'ORGANIZZAZIONE AZIENDALE

Gli assetti organizzativi di MEMC possono variare nel tempo in funzione di diverse esigenze – anche locali – ma sostanzialmente tendono a rispecchiare, almeno nei caratteri principali, i criteri e le scelte, di natura organizzativa, adottate dalla Capogruppo.

Per ciò che concerne MEMC, è compito della Direzione Risorse Umane garantire – a livello generale – l'aggiornamento e la diffusione degli organigrammi aziendali, chiarendo il ruolo e le responsabilità delle diverse strutture organizzative operanti all'interno dell'azienda.

Ogni supervisore, come si evince dall'Organigramma aziendale, contenuto nel Sistema intranet dell'Ente, è in ogni caso tenuto a conoscere ed a spiegare ai propri collaboratori come la Società è organizzata, i compiti e le responsabilità della propria unità organizzativa, i contenuti delle diverse mansioni ed i doveri a queste associati. Da parte sua ogni Dipendente è tenuto a conoscere la propria mansione, i compiti, i poteri e le responsabilità inerenti al proprio ruolo.

La sottoposizione volontaria di MEMC ai processi di certificazione dei sistemi di qualità aziendale garantisce infine che sia data opportuna evidenza e certezza degli specifici assetti organizzativi adottati dalla Società, come pure – in termini generali – dell'individuazione dei principali processi decisionali e di controllo e delle responsabilità assegnate ad ogni unità organizzativa.

12. L'ATTRIBUZIONE DI POTERI

Il criterio generale adottato dalla Società prevede che ai dirigenti possano essere conferiti poteri di rappresentanza, attraverso il rilascio di procure speciali, che definiscono precise regole per il corretto esercizio di tali poteri e la valutazione inerente alla necessità dell'attribuzione dei poteri stessi. Ad ogni modo, il Presidente del CdA e il personale a cui è conferita procura speciale sono comunque soggetti a limiti previsti dalla regolamentazione della Capogruppo.

Le procure speciali e le relative sub-deleghe sono attribuite sulla base di delibere consiliari e l'attività ordinaria è gestita nel rispetto della DOA del Gruppo Global Wafer.

La Società gestisce altresì l'aggiornamento e la revoca dei poteri in azienda, garantendo l'applicazione uniforme delle regole interne.

La tipologia di poteri corrisponde alle esigenze operative aziendali. Il *management* dell'azienda è comunque sottoposto ad opportune attività di formazione e sensibilizzazione su questo tema, in particolare per ciò che concerne le problematiche associate ad eventuali abusi o comunque utilizzi non corretti dei poteri attribuiti ai procuratori della Società, soprattutto in ambito "pubblico".

13. LA REVISIONE ESTERNA – L'INTERNAL AUDIT

La Società affida l'incarico di revisione a primarie società che ne certificano i bilanci e le informazioni in esse riportate. Il conferimento dell'incarico viene approvato dall'Assemblea di MEMC.

Il personale coinvolto in tali verifiche è chiamato a cooperare apertamente e fattivamente al fine di consentire l'espletamento dell'incarico da parte della società di revisione.

Il processo di revisione esterna garantisce un ulteriore qualificato ed approfondito livello di controlli rispetto all'esigenza di accuratezza, veridicità e trasparenza dei dati e delle informazioni di natura finanziaria comunicati o pubblicati dalla Società.

A livello interno, gli audit sono condotti periodicamente durante l'anno fiscale dall'Internal Audit della Capogruppo, sia in remoto sia di persona, che presenta le risultanze della propria attività al CEO.

14. I RIFERIMENTI CONTRATTUALI

La prassi utilizzata da MEMC per formalizzare i propri rapporti con fornitori, clienti, consulenti, agenti od altri soggetti terzi, operanti sia in ambito privato che pubblico, è quella di stipulare appositi contratti che regolamentano tutti gli aspetti della relazione commerciale e che prevedono il richiamo espresso a precisi impegni in materia di etica e di rispetto delle normative.

All'interno dei testi contrattuali standard utilizzati dalla Società sono pertanto rinvenibili clausole, il cui contenuto può variare in funzione delle specifiche circostanze, che indicano impegni dettagliati e chiari, assunti da parte dei soggetti che interagiscono con la Società, per ciò che concerne i principi di etica e correttezza nonché l'esigenza di rispetto delle normative.

Alcuni dei testi contrattuali contengono altresì il richiamo al Codice Etico di MEMC ed al conseguente impegno delle controparti a conoscerne ed applicarne i contenuti nell'ambito della relazione contrattuale con la Società.

Particolare enfasi al tema dell'etica e delle normative è posta nell'ambito delle relazioni contrattuali che esplicano i loro effetti o comunque riguardano l'ambito della Pubblica Amministrazione, in cui viene senza ambiguità ribadito – anche attraverso il richiamo a testi, documenti o riferimenti separati – che la Società è contraria a qualsiasi pratica non conforme al dettato normativo.

Per quanto riguarda, in particolare, l'ambito dei consulenti, si richiede tra l'altro a questi ultimi di dichiarare e garantire:

- di non operare in situazione di conflitto di interesse o avvalendosi di relazioni interpersonali o contrattuali che possano porre il consulente od i terzi in situazioni di conflitto di interesse;
- di non avere assunto incarichi o di svolgere attività che risultino incompatibili, anche sul piano formale, contrattuale e legale, con la prestazione del rapporto di consulenza con la Società, anche in relazione ad attività ed incarichi attuali o pregressi nell'ambito della Pubblica Amministrazione, Enti Pubblici o privati od aziende concorrenti con la Società;
- di non aver subito condanne di qualsiasi tipo o non aver procedimenti giudiziali in corso per atti o comportamenti contrari all'etica ed alla moralità professionale;
- di non utilizzare, per lo svolgimento del rapporto di consulenza, informazioni confidenziali illegittimamente acquisite in relazione a precedenti attività o incarichi.

Tutti i soggetti con cui, a diverso titolo, la Società entra in relazione contrattuale sono in ogni caso sottoposti a preventiva verifica, da parte delle funzioni preposte, in merito alla loro serietà, correttezza, onorabilità ed affidabilità ed eventuali violazioni di norme o principi di etica professionale sono considerate alla stregua di gravi violazioni degli impegni contrattuali e possono quindi comportare la risoluzione degli accordi ed eventuali azioni di risarcimento da parte della Società.

Per i principi procedurali da adottare nelle relazioni contrattuali inerenti alle specifiche aree di rischio, si rinvia alla Parte Speciale del Modello.

15. FORMAZIONE DEI PROCESSI DECISIONALI

Tutti i processi decisionali che hanno luogo nell'ambito di MEMC avvengono attraverso precise modalità di condivisione e di valutazione che implicano, molto spesso, il coinvolgimento di più funzioni e comunque sempre della linea gerarchica. Ciò è particolarmente vero per quanto concerne tutti i processi decisionali relativi ad investimenti, esborsi, finanziamenti, spese, elargizione di contributi o donazioni, cessioni di beni o prestazioni di servizi (anche a titolo gratuito) destinati a terze parti, in quanto si ritiene che tali processi non possano essere gestiti in totale autonomia e discrezionalità da parte del singolo dipendente – per quanto lo stesso operi in posizioni di vertice in azienda – ma richiedano valutazioni condivise, chiari e ben definiti livelli di approvazione preventiva all'interno dell'organizzazione aziendale e, comunque, la possibilità di effettuare controlli o verifiche in qualsiasi momento da parte delle funzioni preposte.

Sotto questo profilo occorre fare riferimento all'articolata struttura di procedure, relativa ai processi di approvvigionamento, approvazione dello stesso, accettazione dell'addebito e liquidazione della spesa.

La logica di condivisione e di valutazione congiunta è applicata in MEMC anche alle attività ed alle verifiche che portano alla formazione del bilancio ed alla redazione dei singoli documenti che lo compongono.

A questo proposito occorre notare che mensilmente MEMC provvede alla redazione di un bilancio, che viene sempre sottoposto al controllo, vaglio ed esame della Capogruppo e, trimestralmente, a quello del revisore. A ciò si aggiungono le consuete attività annuali di revisione del bilancio stesso, a seguito delle quali viene emessa la relazione di certificazione.

I contenuti della comunicazione in materia societaria sono altresì verificati preventivamente dai responsabili di funzione e, in particolare dalla Direzione Finanziaria della Società, e dalla Capogruppo, oltre ad essere ovviamente sottoposti – come per legge – alle preventive valutazioni e verifiche da parte degli organi amministrativi e di controllo della Società. L'intero processo è anche supportato dai consulenti della Società.

Inoltre, sono parte integrante del flusso informativo dell'Ente le relazioni al bilancio da parte dei soggetti preposti, l'informativa semestrale *ex* art. 2381 c.c. e la relazione trimestrale dell'Ente al Collegio sindacale.

Per ciò che riguarda l'espletamento di pratiche aventi ad oggetto la richiesta di ammissione a fondi, finanziamenti e contributi, messi a disposizione dalle Autorità nazionali o da Organismi Comunitari, vengono svolti attenti controlli dalle funzioni preposte alla gestione di tali pratiche in relazione all'effettiva presenza dei requisiti e dei presupposti di legge come pure alla destinazione dei fondi stessi in accordo con le finalità perseguite dal Legislatore.

Ad ogni modo, i contratti di finanziamento e l'aperura di linee di credito devono essere preventivamente autorizzati dalla Capogruppo e deliberati dal CdA.

16. IL RUOLO SVOLTO DALL'ORGANISMO INDICATO DALL'ART. 6 DEL DECRETO

Il D. Lgs. 231/2001 precisa che l'organismo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere un organismo della società (art. 6. 1, lett. B) del D. Lgs. 231/2001, dotato di autonomi poteri di iniziativa e controllo.

Le Linee Guida di Confindustria suggeriscono che si tratti di un organismo dell'ente diverso dal Consiglio di Amministrazione, caratterizzato da autonomia, indipendenza, professionalità e continuità di azione, nonché da onorabilità e assenza di conflitti di interesse. L'organismo può anche sovrapporsi e coincidere con il Collegio Sindacale.

Un tale livello di autonomia presuppone che l'Organismo di Vigilanza risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (i.e. Consiglio di amministrazione). Qualora l'Organismo di Vigilanza coincida con il Collegio sindacale, esso risponderà al Consiglio di amministrazione unicamente nel proprio ruolo di OdV, nel rispetto del principio dell'indipendenza dei controlli del Collegio sindacale.

L'Organismo di Vigilanza, per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello, può ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario.

L'OdV è a tempo determinato e la sua durata coincide con quella del Collegio Sindacale.

Segnatamente, l'OdV è organismo collegiale permanente e con composizione multidisciplinare, che ha i compiti previsti dalla normativa, e, in particolare, quello di vigilare sul funzionamento e l'osservanza dei modelli di organizzazione e gestione e di curarne l'aggiornamento. È pertanto rimesso al suddetto organismo il compito di svolgere – in qualità di organismo di vigilanza – le funzioni di vigilanza e controllo previste dal Modello.

Si è scelto di prevedere un organismo collegiale composto da soggetti in possesso di specifiche competenze, in linea con le disposizioni del D. Lgs. 24/2023, con le Linee Guida di Confindustria e con la giurisprudenza:

- autonomia e indipendenza. I requisiti di autonomia e indipendenza sono fondamentali e presuppongono che l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo;
- onorabilità. In particolare, i membri dell'OdV non hanno riportato sentenze penali, anche non definitive, di condanna o di patteggiamento per reati che comportino l'interdizione dai pubblici uffici o che siano tra quelli richiamati dal Decreto;
- comprovata professionalità. L'OdV possiede, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio;
- continuità d'azione. L'OdV svolge in modo continuativo le attività necessarie per la vigilanza del Modello con adeguato impegno e con i necessari poteri di indagine; è una struttura riferibile alla Società, in modo da garantire la dovuta continuità nell'attività di vigilanza; cura

l’attuazione del Modello, assicurandone costante aggiornamento; non svolge mansioni operative che possano condizionare e contaminare quella visione d’insieme sull’attività aziendale che ad esso si richiede;

- capacità specifiche in tema di attività ispettiva e consulenziale;
- disponibilità dei mezzi organizzativi e finanziari necessari per lo svolgimento delle proprie funzioni.

L'OdV è dotato di autonomi poteri di iniziativa e controllo e di spesa.

All'OdV è stato espressamente attribuito il compito di aggiornare il Codice Etico adottato in azienda, di assicurarne la compiuta conoscenza e rispetto da parte di tutti i dipendenti, anche attraverso la promozione di adeguate attività formative e/o favorendo l’assunzione delle necessarie misure correttive, anche di natura disciplinare. L’OdV può implementare dette attività attraverso le più idonee funzioni aziendali.

L'OdV opera secondo un regolamento. L’OdV si riunisce periodicamente e gli argomenti trattati, nonché le decisioni assunte, vengono verbalizzati in apposito libro, tenuto nelle forme previste per i libri sociali.

L’OdV può essere convocato in qualsiasi momento da ciascuno degli Amministratori e può a sua volta presentare richiesta scritta per la convocazione del Consiglio di Amministrazione, per riferire sul funzionamento del Modello, sull’individuazione delle aree a rischio reato e su situazioni particolari riguardanti i soggetti destinatari del Decreto.

Inoltre, tramite apposita relazione da redigersi semestralmente, l'OdV riferisce al Consiglio di Amministrazione in merito alle attività svolte e all’attuazione del Modello.

In generale l'OdV di MEMC ha il compito di:

- vigilare sull’osservanza delle prescrizioni del Modello da parte di tutti i destinatari;
- proporre integrazioni e/o modifiche e/o aggiornamenti al Modello, qualora esso lo ritenga opportuno in relazione a mutate condizioni aziendali ovvero sulla base di nuove indicazioni del legislatore. A tal fine l’OdV collabora continuativamente con le altre unità organizzative interessate, proponendo agli organi competenti (Consiglio di Amministrazione) eventuali correzioni e adeguamenti.

Su un piano strettamente operativo, l'OdV ha il compito di:

- individuare ed attivare le opportune procedure di controllo, ferma restando la responsabilità primaria dei soggetti che all’interno di MEMC si trovino in una posizione apicale (i.e. top management, dirigenti, amministratori);
- individuare le attività a rischio reato;
- promuovere iniziative di diffusione del Modello, nonché iniziative di sensibilizzazione nei confronti di tutti i soggetti coinvolti nelle aree a rischio reato;

- raccogliere e documentare tutte le informazioni riguardanti il rispetto del presente Modello;
- coordinarsi con i responsabili delle funzioni aziendali, anche attraverso riunioni, al fine di meglio individuare le aree di rischio e prevenire la commissione di reati;
- ricevere notizia delle attività di controllo svolte in MEMC da parte di soggetti terzi (i.e. Autorità Indipendenti, Ispettorato del lavoro) e da parte di funzioni aziendali opportunamente preposte allo svolgimento del controllo (i.e. internal audit);
- ricevere le segnalazioni effettuate da chiunque (es. Dipendenti, consulenti, etc.), nello svolgimento della propria attività, venga a conoscenza di violazioni, o presunte violazioni, o fatti, ordinari o straordinari, rilevanti ai fini della attuazione e dell'efficacia del Modello;
- nel ricevere le segnalazioni di cui al punto precedente, agire in modo da proteggere i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, diretta o indiretta, assicurando altresì la riservatezza dell'identità del segnalante;
- attivare indagini interne al fine di accertare presunte violazioni delle prescrizioni del Modello;
- portare, ove lo ritenga opportuno, a conoscenza di soggetti esterni (es. rappresentanti, agenti, consulenti, partners, ecc.) apposite informative sulle politiche e le procedure adottate da MEMC sulla base del presente Modello.

Il ruolo di prevenzione, vigilanza e controllo svolto dall'OdV, nonché i poteri ed i compiti a questo affidati, sono resi noti a tutti i dipendenti.

L'OdV svolge il ruolo di presidio permanente sui temi dell’etica e del rispetto della normativa, con finalità di prevenzione e controllo, dando conto del proprio operato agli organi amministrativi della Società.

Risultano comunque cause di ineleggibilità e incompatibilità con l’incarico di membro dell’Organismo di Vigilanza, anche a garanzia del requisito di onorabilità:

- essere membro munito di deleghe operative del CdA di MEMC o di Società da questa controllate e/o partecipate, o di Società controllanti e/o partecipanti;
- essere revisore contabile di MEMC o di Società da questa controllate e/o partecipate, o di Società controllanti e/o partecipanti;
- avere relazioni di coniugio, parentela o affinità fino al quarto grado con i soggetti di cui ai punti precedenti;
- aver svolto, negli ultimi tre anni, funzioni di amministrazione, direzione o controllo in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
- aver intrattenuto rapporti di lavoro dipendente o autonomo, negli ultimi tre anni, con entità con le quali o nei confronti delle quali possono essere potenzialmente compiuti i reati considerati dal D. Lgs. 231/2001;
- essere stato condannato con sentenza anche non irrevocabile a:

- pena detentiva che comporta l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle ordinarie persone giuridiche;
- pena detentiva per aver commesso uno dei reati previsti dal D. Lgs. 231/2001;

- essere stato destinatario di una sentenza di patteggiamento per aver commesso uno dei reati previsti dal D. Lgs. 231/2001.

L'indipendenza dell'OdV, inoltre, è assicurata dalla disponibilità di una dotazione di risorse finanziarie, della quale l'OdV potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, ecc.).

Infine, per lo svolgimento dei propri compiti, l'OdV deve coordinarsi, con le funzioni competenti presenti in azienda, per i diversi profili specifici e in particolare, ma non esclusivamente:

- con i Responsabili della Direzione Finanziaria, per gli adempimenti societari che possono avere rilevanza rispetto alla commissione dei reati societari;
- con il Responsabile funzione Risorse Umane sia in ordine alla diffusione delle informazioni che riguardo alla formazione del personale e ai procedimenti disciplinari;
- con il Responsabile della sicurezza (RSPP) per l'osservanza di tutte le norme poste dalla legge e dalle procedure aziendali interne in materia di salute, sicurezza ed igiene sul lavoro;
- con il Responsabile Ambientale per l'osservanza di tutte le norme poste dalla legge e dalle procedure aziendali interne in materia di ambiente;
- con ogni altra funzione ritenuta di volta in volta rilevante ai fini delle proprie attività.

17. VERIFICHE PERIODICHE DEL MODELLO

L'attività di vigilanza svolta continuativamente dall'Organismo per: 1) verificare l'effettività del Modello (vale a dire, la coerenza tra i comportamenti concreti dei destinatari ed il Modello medesimo), 2) effettuare la valutazione periodica dell'adeguatezza, rispetto alle esigenze di prevenzione dei reati di cui al D. Lgs. 231/2001, delle procedure codificate che disciplinano le attività a rischio e 3) procedere agli opportuni aggiornamenti del Modello, si concretizza, *in primis*, nel "Piano di Lavoro dell'Attività di controllo" dell'OdV.

Il sistema di controllo è atto a:

- assicurare che le modalità operative soddisfino le prescrizioni di legge vigenti;
- individuare le aree che necessitano di azioni correttive e/o miglioramenti e verificare l'efficacia delle azioni correttive;
- sviluppare la cultura del controllo, anche al fine di supportare al meglio eventuali visite ispettive da parte di altri soggetti deputati, a diverso titolo, ad attività di verifica.

Le verifiche interne sono gestite dall'Organismo di Vigilanza. Per lo svolgimento delle attività di verifica pianificate l'Organismo di Vigilanza può avvalersi della collaborazione di personale di altre funzioni, che non risultino coinvolte nelle attività verificate e che possiedano specifiche competenze in materia di controllo interno e un adeguato livello di autonomia, o di consulenti esterni.

Al fine di agevolare l'attività di vigilanza sull'efficacia e funzionamento del Modello, l'OdV è destinatario di:

- informazioni, utili e necessarie allo svolgimento dei compiti di vigilanza affidati all'OdV stesso;
- segnalazioni, relative a violazioni, presunte o effettive, del Modello e/o condotte illecite rilevanti ai sensi del D. Lgs. 231/2001, avvenute o in corso di esecuzione.

Informazioni

In ambito aziendale, devono essere comunicati all'Organismo di Vigilanza, sulla base della "procedura flussi informativi", contenuta nel DMS:

- su base periodica, le informazioni/dati/notizie identificate dall'Organismo di Vigilanza e/o da questi richieste alle singole funzioni; tali informazioni devono essere trasmesse nei tempi e nei modi che saranno definiti dall'Organismo medesimo;
- su base occasionale, ogni altra informazione, di qualsivoglia genere, proveniente anche da terzi ed attinente al rispetto e all'attuazione del Modello nelle aree di attività "critiche" ed il rispetto delle previsioni del Decreto, che possano essere ritenute utili ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza. In particolare, a titolo non esaustivo, devono essere obbligatoriamente e tempestivamente trasmesse all'Organismo le informazioni concernenti:
    - provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, tributaria o da

qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti;

- richieste di assistenza legale inoltrate dai dirigenti e/o dai Dipendenti in caso di avvio di procedimento giudiziario a loro carico per i reati previsti dal Decreto;
- rapporti predisposti dai responsabili delle funzioni aziendali nell'ambito delle attività di controllo svolte, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto;
- notizie relative a cambiamenti organizzativi, da cui possa derivare un mutamento delle aree "critiche";

– notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari, rientranti nel campo di applicazione del D. Lgs. 231/2001.

18. SEGNALAZIONI IN MATERIA DI WHISTLEBLOWING

Informativa

La legge 179/2017, il D. Lgs. 231/2001 e il D. Lgs. 24/2023 prevedono l'adozione, anche ai fini dell'applicazione della normativa 231/2001 di appositi strumenti supportati da piattaforma informatica all'interno delle Organizzazioni Pubbliche e Private, attraverso i quali i dipendenti, i collaboratori e tutti i soggetti identificati dalla normativa come possibili segnalatori (Whistleblower), segnalano, a specifici individui od organismi (compresi organi di polizia e autorità pubbliche), una possibile frode, un reato, un illecito o qualunque condotta irregolare commessa da altri soggetti appartenenti all'organizzazione.

A monte si colloca la direttiva europea 2019/1937, che mira a stabilire norme minime comuni per garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri sia all'interno di un'organizzazione, sia all'esterno. In casi specifici, è prevista la possibilità di effettuare la segnalazione mediante la divulgazione pubblica attraverso i media.

La nuova disciplina si applica alle violazioni delle disposizioni normative nazionali e dell'Unione europea che ledono l'interesse o l'integrità dell'ente, di cui i soggetti segnalanti siano venuti a conoscenza in un contesto lavorativo.

La presente sezione si propone inoltre di disciplinare il processo di ricezione, analisi e trattamento delle segnalazioni, da chiunque inviate o trasmesse, anche in forma anonima, e descrive i canali di comunicazione istituiti, attraverso i quali è possibile effettuare segnalazioni.

Il Whistleblowing è da considerarsi come strumento fondamentale per contrastare possibili illeciti, per diffondere nei dipendenti la cultura dell'etica e della legalità all'interno delle

organizzazioni, nonché per creare un clima di trasparenza ed un senso di partecipazione e appartenenza.

Segnalazioni

L'obbligo di informazione grava su:

- i vertici aziendali ed i componenti degli organi sociali;
- gli azionisti;
- i dipendenti e i collaboratori aziendali (a titolo di solo esempio: stagisti, tirocinanti, lavoratori somministrati etc.), anche in periodo di prova o cessati;
- i partner commerciali, i clienti, i fornitori, i consulenti, i soci e, più in generale, chiunque sia in relazione d'interessi con la Società;

(d'ora in avanti collettivamente "Destinatari"), che vengono in possesso di notizie relative alla commissione dei reati o a comportamenti non in linea alle regole di condotta.

Le segnalazioni devono essere circostanziate e fondate su elementi di fatto, precisi e concordanti.

I canali dedicati alla trasmissione delle segnalazioni garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione, in ottemperanza a quanto stabilito dall'art. 6 del D. Lgs. 231/2001.

Inoltre:

- nelle ipotesi di segnalazione o denuncia, effettuate nelle forme e nei limiti di cui all'art. 6 del D. Lgs. 231/2001, il perseguimento dell'interesse all'integrità dell'ente, nonché alla prevenzione e alla repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326 (Rivelazione ed utilizzazione di segreti di ufficio), 622 (rivelazione del segreto professionale) e 623 (rivelazione di segreti scientifici o industriali) del codice penale e all'articolo 2105 (obbligo di fedeltà) del codice civile;
- la disposizione precedente non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata;
- quando notizie e documenti che sono comunicati all'organo deputato a riceverli siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

Procedura

Tutti i Destinatari della presente Procedura sono tenuti a segnalare potenziali attività illecite che possano violare la legge, il Codice Etico o le politiche di MEMC.

La segnalazione di possibili violazioni è incoraggiata, per consentire alla Società di indagare nel merito e adottare le necessarie misure correttive. Dette misure consentono a MEMC di ridurre eventuali rischi o danni per il singolo dipendente, i colleghi e la Società stessa.

A tal fine, chiunque voglia effettuare una segnalazione può, a sua scelta e discrezione, utilizzare il canale di comunicazione raggiungibile mediante collegamento al portale GRC CORA WHISTLEBLOWING, che consente di effettuare segnalazioni in forma anonima o nominativa.

Il segnalante può ovviamente utilizzare anche altri canali di segnalazione esterni, purché ciò avvenga in conformità alla legge.

Forme di tutela

MEMC ha previsto l'incarico della gestione delle segnalazioni ai membri dell'OdV, in qualità di istruttori, i quali sono stati autorizzati al trattamento dei dati personali e formati in tal senso.

Nel corso delle verifiche potranno essere coinvolti altri soggetti interni alla Società (figure responsabili di struttura) per richiesta di informazioni o pareri, ma rimarranno estranei al dettaglio della segnalazione e a qualsiasi elemento che possa portare all'identificazione del soggetto segnalante.

Il portale permette di:

- separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima, e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti;
- gestire le segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- mantenere, per quanto possibile, riservato il contenuto delle segnalazioni durante l'intera fase di gestione della segnalazione;
- adottare protocolli sicuri per il trasporto dei dati in rete, nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;
- adottare adeguate modalità di conservazione dei dati e della documentazione (fisico, logico, ibrido);
- adottare politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);

- adottare politiche di accesso ai dati (funzionari abilitati all'accesso, amministratori del sistema informatico);
- al segnalante, attraverso appositi strumenti informatici, di verificare lo stato di avanzamento dell'istruttoria;
- garantire l'anonimato non permettendo di risalire all'identità del segnalante se non nell'eventuale procedimento disciplinare a carico del segnalato: ciò a causa del fatto che l'identità del segnalante non può essere rivelata senza il suo consenso, a meno che la sua conoscenza non sia assolutamente indispensabile per la difesa dell'incolpato come previsto dall'art. 54-bis, co. 2, del D. Lgs. 165/2001;
- attuare modalità di audit degli accessi al sistema, la cui consultazione deve essere riservata esclusivamente ai soggetti che ne hanno diritto;
- avere funzionalità conformi al modello software ANAC;
- inserire i dati anagrafici anche successivamente all'invio della segnalazione;
- avere HTTP Link Referrer Privacy: al fine di garantire la privacy utente, sono state prese adeguate contromisure per l'accesso a risorse esterne dall'interno della piattaforma, integrando comportamenti di oscuramento del Referrer applicativo;
- avere Header avanzati per la sicurezza: tutte le richieste vengono trattate con l'ausilio di Header avanzati per la sicurezza applicativa, come Strict-Transport-Security e X-Content-Security-Policy.

La piattaforma GRC CORA Whistleblowing è un'applicazione Web-Based accessibile da qualsiasi PC e dispositivo Mobile (*tablet*, *smartphone*). La piattaforma consente la compilazione, l'invio e la ricezione delle segnalazioni, oltre alla possibilità di dialogare con l'istruttore in forma anonima.

Attraverso adeguate procedure, MEMC assicura la riservatezza dell'identità del segnalante, vieta ogni forma di ritorsione o discriminazione nei confronti di chiunque abbia effettuato una segnalazione e di terzi connessi al segnalante e adotta le misure volte a tutelare i diritti dei soggetti segnalati.

I soggetti a qualsiasi titolo coinvolti nella gestione delle segnalazioni sono tenuti, nei limiti previsti dalla legge, alla riservatezza in merito all'esistenza e al contenuto della segnalazione e all'attività compiuta al riguardo e garantiscono la riservatezza sull'identità del segnalante, del segnalato e degli altri soggetti coinvolti, secondo quanto previsto dalla normativa vigente.

Sicurezza della piattaforma

Relativamente agli aspetti legati alla Cyber Security GRC CORA Whistleblowing è periodicamente oggetto di Application Security Assessment (ISO 27001, OWASP) dei Sistemi negli ambienti di pre-esercizio ed esercizio.

Sono riportate di seguito le principali caratteristiche di sicurezza della piattaforma:

- Data Retention Policy: Ogni segnalazione memorizzata nel Database incrementa l'attrattiva per potenziali Hacker. Le segnalazioni hanno una data di validità che può essere estesa dal Receiver, una segnalazione scaduta viene rimossa insieme a tutti i suoi dati.
- Server Resiliency: Il Server è configurato in modo da rendere inoffensivi attacchi di tipo D/DOS. Richieste massive provenienti da uno stesso indirizzo IP che possano configurarsi come attacco, sono automaticamente inibite.
- Web content security: La comunicazione tra *front end* e *back* end utilizza le *best practice*, condivise a livello internazionale, tra cui *header* di sicurezza e cifratura della comunicazione con TLS 1.3.
- File Encryption: Un *receiver* può utilizzare la propria chiave PGP, se posseduta. Ciascun file è salvato su *dicker* utilizzando una chiave simmetrica casuale AES, la chiave è salvata su *ramdisk*.
- GDPR: La Piattaforma di Whistleblowing è a norma con il regolamento generale sulla protezione dei dati (GDPR – General Data Protection Regulation, regolamento UE 2016/679)

Oggetto della segnalazione

Le segnalazioni hanno ad oggetto fatti (di qualsivoglia natura, anche meramente omissivi), già accaduti o che molto verosimilmente potrebbero accadere, riferibili a persone della società MEMC o a Terzi che possano integrare illeciti, irregolarità o comunque condotte poste in essere in violazione:

- illeciti amministrativi, contabili, civili o penali;
- violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti; salute pubblica; salute e sicurezza dei lavoratori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.
- violazioni delle Politiche e del Codice Etico societario.

Le segnalazioni devono riguardare fatti di cui il segnalante abbia conoscenza diretta, avendo lo stesso fondati motivi di ritenere che le informazioni segnalate siano vere al momento della comunicazione.

Le segnalazioni devono essere effettuate tempestivamente rispetto alla conoscenza dei fatti in modo da renderne concretamente possibile la verifica.

Sono escluse le comunicazioni, doglianze, rivendicazioni, istanze aventi ad oggetto tematiche differenti da quelle delle segnalazioni. Le segnalazioni non devono riguardare rimostranze di carattere personale.

Qualora sia necessario inviare una comunicazione non attinente ai profili *whistleblowing*, tale comunicazione può essere inviata al reparto HR dell'Ente.

Qualora l'OdV riceva una segnalazione non attinente alle tematiche *whistleblowing*, la trasmetterà senza indugio o comunque entro 7 (sette) giorni al reparto HR. Il reparto HR provvederà entro i medesimi termini, qualora si verifichi il caso contrario.

Ragioni della segnalazione

Le segnalazioni fatte in buona fede e nell'interesse del bene comune possono permettere di individuare per tempo e porre rimedio a comportamenti irregolari o illeciti che possono danneggiare la Società e/o le persone.

Contenuto della segnalazione

Il segnalante deve fornire tutti gli elementi utili a consentire di procedere alle dovute ed appropriate verifiche ed accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione. A tal fine, la segnalazione deve preferibilmente contenere i seguenti elementi:

a) qualifica del soggetto che effettua la segnalazione (salvo il caso di segnalazione anonima);

b) descrizione dei fatti oggetto di segnalazione, con indicazione, se conosciute, delle circostanze di tempo e di luogo in cui sono stati commessi;

c) generalità o altri elementi che consentano di identificare il soggetto/i che ha/hanno posto/i in essere i fatti segnalati;

d) indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;

e) eventuali persone a conoscenza dei fatti;

f) produzione di eventuali documenti o file multimediali utili ai fatti;

g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

Trasmissione della segnalazione

Al fine di consentire al segnalante di procedere con la segnalazione in modo tempestivo, come già specificato, MEMC ha messo a disposizione sul proprio sito web un apposito portale GRC CORA Whistleblowing raggiungibile al seguente indirizzo web: https://memc.openblow.it.

Dopo l'accesso al portale il segnalante sarà guidato nella compilazione di un questionario formato da domande aperte e/o chiuse che gli permetteranno di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, dimensioni economiche, etc.).

Il segnalante potrà o meno fornire la propria identità. In ogni caso il segnalante potrà fornire le proprie generalità in un secondo momento sempre attraverso il portale.

Al fine di impedire l'identificazione del segnalante, l'accesso al portale è soggetto alla politica "no-log": ciò significa che i sistemi informatici aziendali non sono in grado di identificare il punto di accesso al Portale (indirizzo IP) anche nel caso in cui l'accesso venisse effettuato da un computer connesso alla rete aziendale.

Nel momento dell'invio della segnalazione il portale rilascerà al segnalante un codice identificativo univoco di 16 cifre (KEY CODE). Questo codice, conosciuto solamente dal segnalante, non potrà essere recuperato in alcun modo in caso di smarrimento. Il KEY CODE servirà al segnalante per accedere, sempre tramite il portale, alla propria segnalazione al fine di:

- monitorarne lo stato di avanzamento;
- richiedere ulteriori informazioni attraverso la chat;
- fornire le proprie generalità;
- rispondere ad eventuali domande di approfondimento.

Tale KEY CODE non va assolutamente perso.

Inoltre, si possono effettuare le segnalazioni attraverso i seguenti canali, anche se non preferenziali:

- chiamando il numero 800237555, in questo caso la segnalazione viene verbalizzata per iscritto a cura dell'istruttore;
- incontro diretto con un istruttore, l'incontro verrà verbalizzato e sottoscritto.

Gestione della segnalazione

Le segnalazioni trasmesse mediante il portale sono ricevute dall'OdV, che gestisce le segnalazioni e provvede a dare seguito alle verifiche nel rispetto dei principi di imparzialità e riservatezza, effettuando ogni attività ritenuta opportuna. In particolare, le segnalazioni sono soggette al seguente iter istruttorio:

- dare avviso alla persona segnalante del ricevimento della segnalazione entro 7 (sette) giorni dalla data del suo ricevimento;
- mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni;
- dare diligente seguito alle segnalazioni ricevute;
- svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;
- dare riscontro alla persona segnalante entro 3 (tre) mesi o, se ricorrono giustificate e motivate ragioni, 6 (sei) mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei 7 (sette) giorni dal ricevimento;
- comunicare alla persona segnalante l'esito finale della segnalazione.

Qualora la segnalazione riguardi uno o più membri dell'OdV, essa dovrà essere destinata agli HR Managers/Directors.

Conservazione della segnalazione e privacy

Le segnalazioni interne ed esterne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre 5 (cinque) anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personali.

19. SISTEMA DISCIPLINARE

Funzione del sistema disciplinare

La funzione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabili in caso di violazione delle regole di cui al presente Modello, rende effettiva l'azione di vigilanza dell'OdV ed ha lo scopo di garantire l'efficace attuazione del Modello stesso.

La definizione di tale sistema disciplinare costituisce, infatti, ai sensi dell'articolo 6, comma 2, lettera e) del Decreto, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità di MEMC.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale che l'autorità giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D. Lgs. n. 231/2001.

Nel prosieguo si descrivono anche le misure sanzionatorie che MEMC intende adottare in caso di violazione del Modello da parte di amministratori, nonché di esponenti di altri organi societari e dei Dipendenti, in coordinamento con il sistema disciplinare di cui al Contratto Collettivo nazionale di lavoro applicato da MEMC e nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970 n. 300 (Statuto dei Lavoratori).

Sanzioni nei confronti dei Dipendenti soggetti al CCNL

La violazione delle regole comportamentali di cui al presente Modello da parte dei Dipendenti soggetti al CCNL costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori – nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970 n. 300 e delle eventuali normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio del CCNL di riferimento e precisamente:

- richiamo verbale;
- multa fino all'importo di 3 ore di paga ed indennità di contingenza;
- ammonizione scritta;
- sospensione dal lavoro fino a 3 giorni;
- licenziamento con preavviso;
- licenziamento senza preavviso.

Restano ferme e si intendono qui richiamate tutte le previsioni del citato CCNL, relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.

Fermi restando gli obblighi per MEMC nascenti dallo Statuto dei Lavoratori, i comportamenti

sanzionabili sono i seguenti:

1) violazione, da parte del dipendente, delle procedure interne, anche previste o espressamente richiamate dal presente Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello;

2) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano MEMC ad una situazione oggettiva di rischio per effetto della commissione di uno dei Reati;

3) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello e diretti dolosamente e in modo univoco al compimento di uno o più Reati anche se poi non effettivamente commessi;

4) adozione, nell'espletamento di attività connesse ai Processi Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tali da poter determinare l'applicazione a carico di MEMC delle sanzioni previste dal D. Lgs. 231/2001;

5) effettuazione – con dolo o colpa grave – di segnalazioni ai sensi della disciplina *whistleblowing* che si rivelino infondate, all'esito di accertamento, anche con sentenza di primo grado, della responsabilità civile del segnalante, o con sentenza di condanna, anche in primo grado, per i reati di diffamazione e calunnia;

6) commissione di qualsiasi ritorsione, che provoca o può provocare, in via diretta o indiretta, un danno ingiusto al segnalante e/o agli altri soggetti previsti dalla norma;

7) violazione dell'obbligo di riservatezza.

In caso di lavoratore Dipendente, le sanzioni sono da commisurare al livello di responsabilità ed autonomia dello stesso, all'eventuale esistenza di precedenti disciplinari a suo carico, all'intenzionalità del suo comportamento, nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio cui MEMC può ragionevolmente ritenersi esposto, ai sensi e per gli effetti del Decreto, a seguito della condotta censurata.

Sono di competenza delle Risorse Umane:

- i procedimenti disciplinari; e
- l'irrogazione delle sanzioni.

Ai Dipendenti verrà data un'immediata e diffusa informazione circa l'introduzione di ogni eventuale nuova disposizione, tramite circolare interna diretta a chiarire le ragioni che le hanno giustificate e a riassumerne il contenuto.

Misure nei confronti dei Dirigenti

In caso di violazione, da parte di Dipendenti che ricoprano la qualifica di Dirigente, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con i Processi Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, MEMC si riserva di applicare nei confronti dei diretti responsabili le misure più idonee in conformità a quanto previsto dal CCNL applicato dalla Società per i Dirigenti.

Al Dirigente potranno anche essere revocate le procure eventualmente conferitegli. È fatto salvo, in ogni caso, l'obbligo del Dirigente di risarcire i danni provocati a MEMC da ogni comportamento contrario alle prescrizioni del Modello.

L'irrogazione delle sanzioni ai Dirigenti compete al Consiglio di Amministrazione

Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di uno o più componenti del Consiglio di Amministrazione, l'OdV informa il Collegio Sindacale e l'intero Consiglio di Amministrazione. Detti organi, in relazione alla gravità della violazione, sono tenuti a prendere gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'Assemblea al fine di adottare le misure più idonee previste dalla legge (nei casi più gravi, anche la revoca per giusta causa).

Misure nei confronti dei Sindaci

In caso di violazione del presente Modello da parte di uno o più Sindaci, l'OdV informa il Collegio Sindacale e il Consiglio di Amministrazione, i quali prendono gli opportuni provvedimenti.

Qualora il Collegio Sindacale svolga anche le funzioni di OdV, la segnalazione riguardante uno o più membri del Collegio Sindacale sarà effettuata agli HR Managers/Directors, i quali informeranno prontamente il Consiglio di Amministrazione, che adotta gli opportuni provvedimenti.

Misure nei confronti dell'Organismo di Vigilanza

In caso di violazione del Modello da parte di uno o più componenti dell'OdV, il Consiglio di Amministrazione provvede ad assumere le opportune iniziative in base alla gravità dell'accaduto.

In caso di gravi violazioni, fatta salva l'applicazione delle misure previste dai contratti in essere, si potrà procedere alla revoca dell'incarico. Rientra in tale ipotesi la violazione delle misure di tutela del segnalante ai sensi della Legge Whistleblowing.

Misure nei confronti dei Consulenti e dei Partner

Ogni violazione da parte dei Consulenti o dei Partner delle regole del Modello agli stessi applicabili è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni a MEMC, come ad esempio nel caso di applicazione allo stesso da parte dell'autorità giudiziaria delle misure previste dal Decreto.

Sanzioni in tema di whistleblowing

MEMC è tenuto a sanzionare le seguenti condotte:

1) effettuazione – con dolo o colpa grave – di segnalazioni ai sensi della disciplina *whistleblowing* che si rivelino infondate, all'esito di accertamento, anche con sentenza di primo grado, della responsabilità civile del segnalante, o con sentenza di condanna, anche in primo grado, per i reati di diffamazione e calunnia;

2) commissione di qualsiasi ritorsione, che provoca o può provocare, in via diretta o indiretta, un danno ingiusto al segnalante e/o agli altri soggetti previsti dalla norma;

3) non istituzione dei canali di segnalazione, mancata adozione di procedure di *whistleblowing* conformi alla normativa, non effettuazione di attività di verifica e di analisi delle segnalazioni;

4) messa in atto di comportamenti con i quali la segnalazione è ostacolata o potrebbe essere ostacolata;

5) violazione dell'obbligo di riservatezza.

Sanzioni nei confronti del soggetto segnalante

Qualora, a seguito di verifiche interne, la segnalazione concernente la commissione di un illecito o la violazione del Modello risulti priva di fondamento, saranno effettuati accertamenti sulla sussistenza di grave colpevolezza o dolo circa l'indebita segnalazione e, in caso di esito positivo, il Consiglio di Amministrazione e/o la funzione aziendale a ciò incaricata darà corso alle azioni disciplinari previste dal CCNL applicabile, ovvero dai contratti vigenti e dalla legge applicabile nonché, ricorrendone i presupposti o le ragioni, alle denunce penali nei confronti del segnalante, salvo che quest'ultimo non produca ulteriori elementi a supporto della propria segnalazione.

Resta ferma ogni eventuale responsabilità del segnalante per calunnia, diffamazione, falso ideologico, danno morale o altro danno civilmente o penalmente rilevante.

Segnalante lavoratore dipendente

In conformità al principio di proporzionalità delle sanzioni disciplinari, potranno essere adottati, nei confronti dei Dipendenti, i seguenti provvedimenti sanzionatori:

- ammonizione verbale o scritta, qualora il segnalante violi con dolo o colpa grave le procedure previste in tema di *whistleblowing*, inviando segnalazioni false;
- multa non superiore a tre ore di retribuzione oraria, qualora il segnalante violi con dolo o colpa grave più volte, a distanza di meno di un anno dalla precedente violazione, le procedure previste in tema di *whistleblowing*, inviando segnalazioni false;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni di effettivo lavoro, qualora il segnalante violi con dolo o colpa grave le procedure previste in tema di *whistleblowing*, inviando segnalazioni false ed arrecando altresì un danno all'ente;
- licenziamento senza preavviso, qualora il segnalante violi con dolo o colpa grave più volte, a distanza di meno di un anno dalla precedente violazione, le procedure previste in tema di *whistleblowing*, inviando segnalazioni false ed arrecando altresì un danno all'ente.

Segnalante dirigente

Qualora i dirigenti si rendano responsabili con dolo o colpa grave di violazioni delle procedure previste in tema di *whistleblowing*, saranno applicabili nei confronti dei medesimi le misure ritenute più idonee dal Consiglio di Amministrazione, in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro applicabile.

Segnalante amministratore

Qualora singoli amministratori di MEMC si rendano responsabili di violazioni delle procedure previste in tema di *whistleblowing*, l'Organismo di Vigilanza informerà senza indugio il Consiglio di Amministrazione ed il Collegio Sindacale affinché sia adottato ogni provvedimento ritenuto opportuno e compatibile con la vigente normativa.

Segnalante terzo contraente

I soggetti terzi – quali membri dell'organo di controllo e collaboratori esterni – in caso di eventuale violazione delle procedure in tema di *whistleblowing*, potranno subire le conseguenze previste dalle clausole contrattuali, ivi compresi, a titolo esemplificativo, la risoluzione, il recesso ed il risarcimento dei danni.

Sanzioni nei confronti di chi viola le tutele del segnalante

La violazione dell'obbligo di riservatezza del segnalante ovvero il compimento di atti ritorsivi o discriminatori nei confronti del segnalante è fonte di responsabilità disciplinare ai sensi del CCNL applicabile ovvero dei contratti vigenti e della legge applicabile, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge.