AGGIORNAMENTO MODELLO EX D.LGS. 231/2001
IN SEGUITO ALL'ENTRATA IN VIGORE DEL C.D. "AI ACT"
GM-AUDIOLOGICA
(AGOSTO 2026)

1. PREMESSE E AMBITO DI APPLICAZIONE

La Società, consapevole delle profonde implicazioni organizzative e di responsabilità derivanti dall'impiego di sistemi di intelligenza artificiale (di seguito "IA"), ha deliberato di integrare il proprio Modello di organizzazione, gestione e controllo ex d.lgs. 231/2001 (di seguito "Modello 231") con il presente **Addendum IA**.

Il presente Addendum:

- recepisce i principi e gli obblighi derivanti dal Regolamento (UE) 2024/1689 ("**AI Act**");
- tiene conto della legge 23 settembre 2025 n. 132 e della normativa nazionale di accompagnamento in materia di IA;
- si coordina con la disciplina sulla sicurezza dei prodotti digitali e delle infrastrutture (tra cui Direttiva NIS2, Cyber Resilience Act, Regolamento DORA, nonché il GDPR e normativa privacy);
- è volto a prevenire, in particolare, i reati commessi mediante o con l'ausilio di sistemi di IA, inclusi quelli riconducibili al nuovo **art. 25-vicies d.lgs. 231/2001** e alle fattispecie penali inerenti alla sicurezza dei sistemi ad alto rischio (es. art. 437-bis c.p.) e ai contenuti deepfake (art. 612-quater c.p.).

L'Addendum si applica a tutti i sistemi di IA utilizzati dalla Società, sia sviluppati internamente sia acquisiti da fornitori esterni, in qualunque ambito organizzativo.

2. DEFINIZIONI

Ai fini del presente Addendum, per:

1. **Sistema di intelligenza artificiale** si intende qualsiasi sistema compatibile con la definizione di cui all'AI Act, progettato per generare output (contenuti, previsioni, raccomandazioni, decisioni) tramite tecniche statistiche, di machine learning o logiche simili, che influenzano processi decisionali umani o automatizzati.
2. **Provider** si intende il soggetto che sviluppa o immette sul mercato un sistema di IA, secondo la definizione dell'AI Act.
3. **Deployer** si intende il soggetto che utilizza un sistema di IA nel proprio contesto organizzativo (la Società assume, per i sistemi di IA impiegati nei propri processi, la qualifica di deployer).

4. **Sistema di IA ad alto rischio** si intende qualsiasi sistema di IA rientrante nelle categorie di alto rischio ai sensi dell'AI Act (ad es. sistemi impiegati per selezione del personale, credit scoring, accesso a servizi essenziali, sicurezza di prodotti e infrastrutture).
5. **Deepfake** si intende qualsiasi contenuto (audio, video, immagine, testo) creato o significativamente alterato tramite IA, idoneo a presentare come reali dati, fatti o informazioni che non lo sono, con capacità di incidere sulla reputazione, la dignità o i diritti delle persone.

3. PRINCIPI GENERALI SULL'USO DELL'IA

3.1. L'uso di sistemi di IA da parte della Società deve avvenire nel rispetto dei diritti fondamentali, della dignità della persona, della non discriminazione e dei principi di correttezza, trasparenza e proporzionalità.

3.2. L'IA deve essere considerata strumento di supporto alla decisione e non sostituto integrale del giudizio umano; la decisione finale su profili rilevanti per diritti, sicurezza, rapporti di lavoro, relazioni commerciali e compliance resta in capo a soggetti umani responsabili.

3.3. L'impiego di IA in ambiti suscettibili di generare rischi penali o para-penali (es. discriminazioni, violazioni privacy, lesioni alla sicurezza, frodi, reati informatici) è subordinato a preventiva valutazione di impatto e alla verifica della conformità ai presidi del Modello 231.

3.4. È vietato l'utilizzo di sistemi di IA vietati o non conformi ai requisiti dell'AI Act (in particolare quelli classificati a rischio inaccettabile), anche qualora forniti o gestiti da terzi.

4. GOVERNANCE E RESPONSABILITÀ

4.1. L'Amministratore definisce la strategia aziendale sull'IA, individuando:

- le aree in cui l'IA può essere impiegata;
- i criteri di valutazione dei rischi;
- le linee guida per la scelta dei sistemi e dei fornitori;
- il perimetro dei controlli da integrare nel Modello 231.

4.2. La Società, nel corso dei prossimi due mesi, si impegna ad istituire una funzione o comitato interno di AI Governance/Compliance, che:

- coopera con le funzioni Compliance 231, IT/Sicurezza informatica, Privacy/DPO, Risk Management;
- si coordina con l'ODV per curare l'aggiornamento della mappatura dei sistemi di IA, in particolare di quelli ad alto rischio;
- monitora le evoluzioni normative europee e nazionali sull'IA e sulla sicurezza digitale.

4.3. L'utilizzo di IA non attenua ma, al contrario, accentua la responsabilità organizzativa della Società; la mancata gestione dei bias, dei malfunzionamenti, delle vulnerabilità di sicurezza o degli utilizzi impropri dei sistemi di IA è considerata, ai fini 231, indice di "colpa d'organizzazione" (cd. colpa artificiale).

5. PROTOCOLLI PER L'ACQUISIZIONE, SVILUPPO E MESSA IN SERVIZIO DEI SISTEMI DI IA

5.1. Due diligence sui fornitori (provider)

Prima dell'acquisto o della messa in uso di sistemi di IA forniti da terzi, la Società:

- verifica, per quanto ragionevolmente esigibile, la conformità del sistema all'AI Act (documentazione tecnica, valutazione di conformità, marcatura CE per sistemi ad alto rischio, registrazione nei database rilevanti);
- accerta l'esistenza di presidi di cybersecurity e di aggiornamento in linea con la normativa europea di settore (NIS2, CRA, DORA);
- richiede clausole contrattuali su responsabilità, manutenzione, aggiornamenti normativi, supporto in caso di incidenti e data breach.

5.2. Sviluppo interno e addestramento dei modelli

Qualora la Società sviluppasse internamente sistemi di IA o modelli di machine learning, la stessa dovrà:

- predisporre regole sulla qualità, adeguatezza, non discriminazione e aggiornamento dei dati utilizzati per l'addestramento;
- effettuare test di validazione prima di ogni messa in produzione;
- mantenere documentazione tecnica sufficiente a consentire il controllo degli algoritmi e degli output.

5.3. Autorizzazione alla messa in servizio

Ogni introduzione o modifica significativa di un sistema di IA ad alto impatto è subordinata a:

- predisposizione di una valutazione di impatto sui diritti, sulla sicurezza e sui rischi penali;
- parere delle funzioni competenti (quali AI Governance/Compliance, IT, Privacy/DPO, Compliance 231);
- deliberazione formalizzata dell'Amministratore.

6. PROTOCOLLI DI UTILIZZO, SUPERVISIONE E TRACCIABILITÀ

6.1. Supervisione umana

L'utilizzo di sistemi di IA, segnatamente quelli ad alto rischio, deve essere sempre soggetto a supervisione umana effettiva; il personale incaricato è tenuto a:

- controllare la coerenza degli output rispetto ai dati e ai criteri di riferimento;
- segnalare tempestivamente anomalie, errori evidenti, bias e discrepanze;
- non limitarsi alla mera "ratifica" delle proposte algoritmiche, soprattutto in ambiti sensibili.

6.2. Tracciabilità e trasparenza

La Società assicura:

- la tracciabilità dei sistemi di IA utilizzati (registro interno dei sistemi, delle versioni e dei principali parametri di configurazione);
- la tracciabilità delle decisioni rilevanti assunte con il supporto di IA, mediante idonea documentazione (log, report, note istruttorie);
- l'informativa interna ed esterna sull'uso di IA, nel rispetto degli obblighi di trasparenza verso dipendenti, clienti, utenti e altri stakeholder.

6.3. Divieti di utilizzo improprio

È vietato:

- utilizzare applicazioni di IA non approvate dalla Società su dati aziendali o personali;
- caricare documenti riservati, dati sensibili o informazioni strategiche su strumenti di IA pubblici non controllati;
- utilizzare sistemi di IA per generare o diffondere contenuti deepfake in contesti aziendali o comunque collegati alla Società.

7. SICUREZZA DIGITALE E PROTEZIONE DEI DATI

7.1. La Società adotta misure tecniche e organizzative di sicurezza informatica allineate al quadro normativo europeo e nazionale, con particolare riferimento a:

- protezione dei sistemi di IA da accessi non autorizzati, manipolazioni dei dati, avvelenamento dei modelli, furti di informazioni;
- gestione degli aggiornamenti, delle patch e delle vulnerabilità;
- procedure di risposta agli incidenti (incident response) e piani di continuità operativa.

7.2. La gestione dei dati utilizzati dai sistemi di IA, inclusi i dataset di addestramento, deve essere conforme al GDPR e alla normativa nazionale sulla protezione dei dati personali, con particolare attenzione a:

- liceità del trattamento, correttezza e trasparenza;
- limitazione delle finalità e minimizzazione dei dati;
- pseudonimizzazione/anonimizzazione ove possibile;
- sicurezza e resilienza dei sistemi.

8. INCIDENTI, MALFUNZIONAMENTI E SEGNALAZIONI

8.1. In caso di malfunzionamento, errore significativo, bias o incidente connesso all'uso di un sistema di IA (anche solo sospetto), il personale è tenuto a:

- sospendere, ove necessario, l'utilizzo del sistema;
- segnalare immediatamente l'evento alle funzioni AI Governance/Compliance, IT, Privacy/DPO e Compliance 231;
- collaborare alla raccolta delle informazioni rilevanti per l'analisi delle cause.

8.2. Le funzioni competenti:

- analizzano l'evento e individuano le cause (tecniche, organizzative, umane);
- adottano misure correttive e di mitigazione;
- verificano se l'evento possa integrare violazioni rilevanti ai fini leggibili 231 (lett. informatici, privacy, nuovi reati da IA ex art. 25-vicies) e, se del caso, informano l'Organismo di Vigilanza e gli organi sociali.

9. FORMAZIONE E CULTURA AZIENDALE SULL'IA

9.1. La Società promuove specifici programmi di formazione e alfabetizzazione sull'IA, rivolti:

- agli organi apicali e ai responsabili di funzione, per illustrare i rischi giuridici e penali connessi all'IA e l'impatto sui Modelli 231;
- al personale che utilizza, direttamente o indirettamente, sistemi di IA, per evidenziare i limiti degli algoritmi, il rischio di errori, l'importanza della verifica critica degli output e il divieto di delega cognitiva totale al sistema.

9.2. La partecipazione ai programmi formativi è obbligatoria per le figure individuate, e costituisce parametro di valutazione della conformità ai presidi del Modello 231.

10. SISTEMA DISCIPLINARE E CONTROLLI DELL'ODV

10.1. Il sistema disciplinare aziendale è integrato in modo da prevedere, tra le condotte sanzionabili:

- l'uso non autorizzato o improprio di sistemi di IA;
- la violazione dei protocolli e delle misure di sicurezza previsti dal presente Addendum;
- la mancata segnalazione di incidenti o malfunzionamenti;
- la creazione, alterazione o diffusione di contenuti deepfake in ambito aziendale o connesso alla Società.

10.2. L'Organismo di Vigilanza (OdV):

- vigila sull'attuazione del presente Addendum;
- verifica periodicamente l'efficacia dei protocolli relativi all'IA;
- analizza, nell'ambito della propria attività di controllo, gli incidenti digitali, i contenziosi o le indagini connesse all'uso di IA;
- propone aggiornamenti e miglioramenti alla governance dell'IA ai fini 231.

11. AGGIORNAMENTO E COORDINAMENTO CON IL MODELLO 231

11.1. Il presente Addendum è parte integrante del Modello 231 e deve essere periodicamente rivisto e aggiornato in considerazione:

- delle evoluzioni normative europee e nazionali in materia di IA e sicurezza digitale;
- dell'evoluzione tecnologica dei sistemi di IA impiegati dalla Società;
- dell'esperienza applicativa, degli incidenti e delle risultanze dei controlli dell'OdV.

11.2. Ogni aggiornamento significativo dell'Addendum è deliberato dall'organo amministrativo competente, previo parere dell'OdV e delle funzioni interessate.

L'ODV

Palermo, 26/08/2026