



PROCEDURA WHISTLEBLOWING (ITALIA)

Sommario

| | |
|---|---|
| Scopo..... | 1 |
| Soggetti che possono effettuare la segnalazione (il “Segnalante”) – Ambito soggettivo | 2 |
| Contenuto delle segnalazioni – Ambito oggettivo | 2 |
| Segnalazioni escluse..... | 3 |
| Gestore della segnalazione | 3 |
| Il Canale Interno - Modalità di segnalazione | 3 |
| Istruzioni per la segnalazione sulla Piattaforma Whistleblowing e iter procedurale..... | 4 |
| Segnalazione inviata a soggetto non competente | 5 |
| Raccomandazioni per chi vuole effettuare una segnalazione | 5 |
| Caratteristiche della piattaforma..... | 5 |
| Tutele riconosciute ai Segnalanti..... | 5 |
| Estensione delle tutele | 6 |
| Sanzioni | 6 |
| Segnalazione esterna tramite canale ANAC..... | 6 |
| Divulgazione Pubblica | 6 |
| Responsabilità del Segnalante | 7 |
| Protezione del soggetto segnalato dalle segnalazioni in malafede | 7 |
| Tempi di conservazione della documentazione | 7 |
| Trattamento dei dati personali | 7 |
| Diffusione e comunicazione sul canale e sulla procedura di segnalazione | 7 |

Scopo

Al fine di adempiere a quanto previsto dal D.lgs. 24/2023 (di seguito “Decreto 24”) *“Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019”*, in materia di tutela delle persone che segnalano violazioni di disposizioni normative nazionali o dell’Unione Europea di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato e dalle Linee guida ANAC del 14 luglio 2023, Boston Scientific S.p.a. (la “Società”) ha adottato la presente procedura per disciplinare il processo di trasmissione, ricezione, analisi e gestione delle segnalazioni cd. “Whistleblowing”, ai sensi del comma 2 bis dell’art. 6 del D.lgs. 231/2001 in materia di responsabilità amministrativa degli enti, così come modificato dal Decreto 24.

La presente procedura persegue, altresì, lo scopo di comunicare a tutti i soggetti interessati di aver attivato una piattaforma che consente di inviare segnalazioni, anche in forma anonima, relative a violazioni di disposizioni normative nazionali e dell’Unione Europea che possono ledere l’interesse pubblico o l’integrità della Società, a condotte illecite rilevanti ai fini del D.lgs. 231/2001 o a violazioni del Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/2001, del Codice Etico e dei protocolli, policy e procedure adottate dalla Società.

Attraverso la Piattaforma Whistleblowing (di seguito "Piattaforma"), raggiungibile dal sito internet di Boston Scientific <http://advice.bostonscientific.com/>, o telefonicamente al numero 800.727.406, un soggetto interno o un soggetto terzo come di seguito identificati, vittima di una delle violazioni sopracitate che sia a conoscenza di condotte illecite già avvenute o potenzialmente configurabili in futuro può segnalare il comportamento, l'atto o l'omissione, anche in forma anonima, avendo garanzia del rispetto dell'obbligo di riservatezza previsto dall'art. 12 del Decreto 24, in modo da essere tutelato da qualsiasi conseguenza ritorsiva o discriminatoria legata alla segnalazione, secondo le previsione dell'art. 17 del Decreto 24. La Piattaforma, infatti, è gestita da un fornitore terzo indipendente ed è un canale informatico protetto che utilizza strumenti di crittografia per garantire la riservatezza dell'identità del segnalante, del contenuto della segnalazione e della relativa documentazione.

Soggetti che possono effettuare la segnalazione (il "Segnalante") – Ambito soggettivo

Il Segnalante è la persona fisica che effettua la segnalazione delle asserite violazioni di cui è venuta a conoscenza nell'ambito del proprio contesto lavorativo e/o delle attività lavorative o professionali svolte a favore della Società (*ex art. 2, co. 1, lett. g) e lett. i)* del Decreto 24).

I soggetti che possono effettuare una segnalazione sono:

- Soggetti Interni, quali ad esempio:
 - Dipendenti a tempo indeterminato e determinato
 - Dirigenti
 - Soggetti in periodo di prova o in fase di colloquio
 - Ex dipendenti (successivamente allo scioglimento del rapporto di lavoro)
 - Tirocinanti e Volontari retribuiti o non
 - Azionisti
 - Persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza (anche nell'ambito delle normali mansioni).
 - Coloro che, pur non rientrando nella categoria dei dipendenti, operano per la Società e sono sotto il controllo e la direzione della stessa (a titolo esemplificativo e non esaustivo: stagisti, lavoratori a contratto ed a progetto, lavoratori somministrati);
- Soggetti Esterni quali ad esempio:
 - Fornitori di beni o servizi
 - Collaboratori
 - Liberi professionisti, consulenti, collaboratori

Contenuto delle segnalazioni – Ambito oggettivo

Questa Piattaforma può essere utilizzata per segnalare:

- comportamenti attuati in violazione del Modello di Organizzazione, Gestione e Controllo, del codice etico o di altre disposizioni interne all'organizzazione;
- comportamenti illeciti rilevanti ai sensi del D.lgs. 231/2001;
- comportamenti illeciti derivanti da norme dell'Unione Europea o nazionali in materia di: appalti pubblici, servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento al terrorismo, tutela dell'ambiente, radioprotezione e sicurezza nucleare, salute pubblica, protezione dei consumatori, privacy e protezione dei dati e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione Europea;
- atti od omissioni riguardanti il mercato interno dell'Unione Europea.

Il segnalante dovrà riferire solo gli elementi utili per consentire le necessarie valutazioni e verifiche. A tal fine, si suggerisce di inserire nella segnalazione:

- una descrizione chiara e completa di:
 - evento o fatto segnalato;
 - circostanze di tempo e luogo (se note), in cui si è verificato;
 - ogni altra informazione che possa fornire dettagli utili alla segnalazione;
 - qualsiasi documento a supporto dell'evento o fatto denunciato.

Si ricorda che non fornire informazioni sufficienti può comportare ritardi nel processo di valutazione e di indagine della segnalazione; in altre parole, se la segnalazione è generica e/o priva di dettagli specifici, potrebbe non essere possibile una revisione efficace.

Si suggerisce vivamente, in ottemperanza al principio di minimizzare la raccolta di dati non necessari, di evitare di fornire particolari sulla vita privata dei soggetti oggetto di segnalazione o comunque coinvolti, se non strettamente necessari e rilevanti ai fini di quanto segnalato.

Le misure di protezione previste dal Decreto 24 saranno concesse al Segnalante anonimo, se successivamente identificato.

Segnalazioni escluse

La presente procedura e le tutele previste dal Decreto 24 non si applicano a:

- contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate;
- segnalazioni di violazioni laddove già disciplinate in via obbligatoria nella parte II dell'allegato al Decreto 24 ovvero da normative nazionali che costituiscono attuazione degli atti dell'Unione Europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937;
- segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione Europea.

Gestore della segnalazione

Le segnalazioni verranno gestite tempestivamente (entro 7 giorni di calendario dall'avviso di ricevimento) da parte del Gestore della Segnalazione (di seguito il "Gestore") che è specificatamente formato per garantire la gestione dei casi conformemente a quanto prescritto dal Decreto 24.

Il Consiglio di Amministrazione della Società ha nominato come "Gestore", individualmente e per i rispettivi ruoli e competenze, i seguenti soggetti:

- Tim Trujillo, Chief Compliance Officer, Boston Scientific Corporation
- Paul Flynn, Senior Director, Global Compliance Investigations and Audit and Monitoring, Boston Scientific Corporation
- Erina Mohamad Ramly, Director, Global Compliance Investigations, Boston Scientific Corporation
- Michael DiFrancesco, Principal, Global Compliance Investigations, Boston Scientific Corporation
- Karen Oden, Analyst I, Compliance, Boston Scientific Corporation
- Stephanie Marchand, Fellow, Global Compliance Investigations, Boston Scientific Corporation
- Luigi dell'Aquila, Studio Professionale Associato a Baker McKenzie
- Federica Assumma, Presidente dell'Organismo di Vigilanza della Società
- Massimiliano Lei, membro dell'Organismo di Vigilanza della Società
- Mario Occhini, membro dell'Organismo di Vigilanza della Società

I soggetti nominati come "Gestore" sono stati preventivamente autorizzati ex art. 29 del GDPR per cui sono autorizzati a conoscere i dati identificativi del Segnalante, nel caso in cui questi abbia fornito il proprio nome.

Tutte le segnalazioni saranno inizialmente esaminate dal Gestore Baker McKenzie per assicurarsi che siano idonee a ricevere la protezione concessa dal Decreto 24 e per verificare eventuali conflitti di interesse relativi a uno dei Gestori delle segnalazioni.

I membri dell'Organismo di Vigilanza nominati come Gestori non riceveranno automaticamente tutte le segnalazioni, ma saranno coinvolti solo sugli argomenti di interesse dopo uno screening preliminare effettuato dagli altri Gestori.

Il Canale Interno - Modalità di segnalazione

I seguenti canali interni di segnalazione si impegnano a garantire la riservatezza dell'identità del Segnalante e la sicurezza delle informazioni, prevedendone l'accesso selettivo solo da parte del personale specificamente autorizzato. In particolare, il canale interno di segnalazione è una Piattaforma informatica che consente la

segnalazione in forma scritta, orale, oppure tramite incontro diretto con il Gestore della segnalazione fissato entro un termine ragionevole.

Istruzioni per la segnalazione sulla Piattaforma Whistleblowing e iter procedurale

Il Segnalante può accedere alla Piattaforma attraverso il link di seguito riportato [Boston Scientific-Compliance and Ethics](#)

All'accesso il sistema chiede al Segnalante di prendere visione delle informazioni sulla riservatezza e la tutela della sua identità. Le segnalazioni si possono effettuare in forma anonima o nominativa. Non appena il Segnalante invia la propria segnalazione, riceve un messaggio automatico che conferma la ricezione della segnalazione e gli viene fornito un "codice di accesso" di 7 caratteri per accedere alla segnalazione. La prima volta che accederà alla segnalazione, gli verrà inoltre richiesto di creare una password e delle domande di sicurezza. Il Segnalante può quindi esaminare lo stato della propria segnalazione e, se necessario, comunicare con il Gestore della segnalazione durante il processo di indagine e/o fornire ulteriori informazioni. La piattaforma descrive quali informazioni vengono raccolte in base all'opzione del Segnalante di effettuare la segnalazione in forma anonima o di fornire il proprio nome.

Entro il temine di 7 giorni dalla data di ricezione il Gestore comunicherà con il Segnalante tramite la Piattaforma per confermare che la segnalazione è stata ricevuta e/o per richiedere ulteriori informazioni.

Il Segnalante dovrà descrivere con parole proprie il fatto che intende segnalare, dopo aver selezionato alcune risposte a specifiche domande fornite dalla Piattaforma. A supporto della descrizione dell'oggetto della segnalazione si possono allegare file o altri documenti.

Il Gestore effettua una valutazione preventiva della segnalazione al fine di verificare se sono presenti tutti i requisiti per poter accordare al Segnalante le tutele previste dal Decreto 24 e se è possibile avviare l'istruttoria. In particolare, il Gestore prenderà in considerazione quanto segue:

- se il segnalante è uno dei soggetti richiamati dall'art. 3 del Decreto 24;
- se l'oggetto della segnalazione rientra nelle violazioni richiamate dall'art. 2 ed è, quindi, di competenza del Gestore e non è tra le esclusioni espressamente disciplinate dall'art.1 comma 2 del Decreto 24;
- se è manifestatamente assente la lesione dell'interesse pubblico o dell'integrità dell'ente;
- se è manifestatamente infondata la segnalazione per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- se la segnalazione dell'illecito ha un contenuto generico tale da non consentire la comprensione dei fatti, ovvero è corredata da documentazione non appropriata o non pertinente o vi è una carenza di dati che costituiscono elementi essenziali per la segnalazione di illeciti;
- se vi è mancanza dei dati che costituiscono elementi essenziali della segnalazione di illeciti indicati dal regolamento per la gestione delle segnalazioni.

Nel corso dell'istruttoria, il Gestore manterrà un'interlocuzione con il Segnalante per richiedere ulteriori approfondimenti e/o informazioni aggiuntive, tracciare le attività svolte e fornire informazioni, anche d'ufficio, sullo stato di avanzamento dell'istruttoria, almeno con riferimento alle principali tappe decisionali. Nel caso in cui sia necessario comunicare i dati personali del Segnalante o qualsiasi dettaglio relativo alla segnalazione o al Segnalante a soggetti terzi (consulenti appositamente incaricati per la gestione dell'indagine o parte di essa, responsabili di funzione aziendali quali Responsabile HR, Direttore amministrativo, Ufficio Legale, ecc.), il Gestore chiederà, tramite la Piattaforma, esplicito consenso alla comunicazione a terzi, motivando la richiesta ed esplicitando i soggetti a cui i dati del Segnalante ed il contenuto della segnalazione verranno comunicati. Il consenso o il rifiuto del Segnalante rimarranno tracciati nella piattaforma.

Per garantire un processo di indagine efficace, è responsabilità del Segnalante accedere periodicamente alla Piattaforma per verificare se sono necessarie ulteriori informazioni o azioni, compresa la concessione del consenso alla condivisione dei dati personali del Segnalante o di qualsiasi dettaglio relativo alla segnalazione o al Segnalante a terzi.

Alla chiusura dell'indagine, o comunque entro tre (3) mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di 7 giorni dalla presentazione della segnalazione, il Gestore fornirà un riscontro sullo stato dell'indagine al Segnalante come definito all'art. 2 del Decreto 24.

Segnalazione inviata a soggetto non competente

Qualora la segnalazione interna sia presentata ad un soggetto diverso da quelli individuati e autorizzati dall'ente (il Gestore) la segnalazione deve essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione al Segnalante.

Raccomandazioni per chi vuole effettuare una segnalazione

Coloro che vogliono presentare una segnalazione devono indicare chiaramente nell'oggetto della segnalazione che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni subite in ragione della segnalazione.

Tale specificazione permette, nel caso in cui la segnalazione pervenga erroneamente ad un soggetto non competente oppure attraverso un canale diverso da quelli specificamente previsti dal Decreto 24, la trasmissione tempestiva da parte di quest'ultimo al soggetto autorizzato a ricevere e gestire le segnalazioni di whistleblowing.

Si precisa, inoltre, che la segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e seguenti della legge 241/1990, all'accesso civico generalizzato di cui all'art. 5 co. 2 del D.lgs. 33/2013, nonché all'accesso di cui all'art. 2-undecies co. 1 lett. f) del codice in materia di protezione dei dati personali.

Caratteristiche della piattaforma

La Piattaforma, fornita dalla società Convercent by One Trust, adotta misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR, inclusa la crittografia. Il documento che dettaglia le misure tecniche ed organizzative è disponibile a questo [link](#).

Tutele riconosciute ai Segnalanti

Boston Scientific tutela i Segnalanti contro qualsiasi forma di ritorsione o discriminazione collegata, direttamente o indirettamente, alla segnalazione, secondo quanto previsto dal Decreto 24, e adotta misure idonee a garantire la riservatezza dell'identità del Segnalante e delle altre Persone coinvolte, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle Persone coinvolte.

La Società ha previsto specifiche misure a tutela del Segnalante e degli altri soggetti individuati dall'art. 3 del Decreto 24, affinché non siano oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni connesse alla segnalazione.

Il Capo III (artt. 16 -22) del Decreto 24 prevede le misure di protezione avverso i comportamenti discriminatori e ritorsivi attuati nei confronti della persona che effettua la segnalazione.

Per misure discriminatorie si intendono, ad esempio, le azioni disciplinari ingiustificate ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili.

In particolare, si indicano alcuni provvedimenti che potranno essere dichiarati nulli, se assunti in violazione dell'art. 17 del Decreto 24:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi.

Estensione delle tutele

Le misure di protezione di cui al Capo III si applicano anche a:

- ai facilitatori (persone fisiche che assistono il Segnalante nel processo di segnalazione, operano all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata);
- alle persone del medesimo contesto lavorativo del Segnalante, che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del Segnalante che lavorano nel medesimo contesto lavorativo dello stesso e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà del Segnalante per i quali le stesse persone lavorano, nonché' agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Qualora si verificasse l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni, l'art. 19 del Decreto 24 prevede che tale circostanza possa essere comunicata, oltreché alla Società, anche all'ANAC che informa l'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, laddove la misura discriminatoria non fosse rimossa dalla Società stessa.

Sanzioni

Il Sistema disciplinare di Boston Scientific S.p.a. prevede sanzioni nel caso in cui vengano commesse ritorsioni o quando venga accertato che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'art. 12 del Decreto 24.

Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni ritorsivi nei confronti delle persone segnalanti, si presume che gli stessi siano stati posti in essere a causa della segnalazione. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione, è a carico di colui che li ha posti in essere (Datore di lavoro o soggetto da lui delegato).

Segnalazione esterna tramite canale ANAC

L'ANAC ha attivato canali di segnalazione che devono garantire, anche tramite il ricorso a strumenti di crittografia, la riservatezza:

- dell'identità della persona segnalante
- della persona coinvolta e di qualsiasi persona comunque menzionata nella segnalazione
- del contenuto della segnalazione e della relativa documentazione

Il ricorso alla segnalazione esterna tramite canale ANAC è consentita solo a condizione che:

- non sia stata prevista l'istituzione obbligatoria di un canale di segnalazione interno al contesto lavorativo, anche se obbligatorio, ovvero il canale di segnalazione interno non sia attivo o, pur essendo stato istituito, non sia conforme all'art. 4 del Decreto 24;
- la persona segnalante abbia già effettuato una segnalazione interna ai sensi dell'articolo 4 e la stessa non abbia avuto seguito;
- la persona segnalante abbia fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- la persona segnalante abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Divulgazione Pubblica

Il Segnalante, ai sensi dell'art. 15 del Decreto 24, è tutelato anche quando effettua una c.d. "divulgazione pubblica" delle informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone (ex art. 2, comma 1, lett. f), Decreto 24).

La tutela del Segnalante in questo caso è garantita solo se, al momento della divulgazione, ricorre una delle seguenti condizioni:

- ✓ il Segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna, alle condizioni e con le modalità previste dalla normativa, ma non è stato dato riscontro nei termini previsti;

- ✓ il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- ✓ il Segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

Responsabilità del Segnalante

Il Segnalante è ritenuto responsabile, anche disciplinamente, nell'ipotesi di segnalazioni caluniose o diffamatorie, ovvero di segnalazioni effettuate con dolo o colpa grave, di fatti non rispondenti al vero.

L'Art. 21, co. 1 lett. c) del Decreto 24, prevede che l'ANAC possa irrogare una sanzione pecuniaria da 500 a 2.500 euro nei confronti del Segnalante, ove sia accertata la sua responsabilità civile, a titolo di dolo o colpa grave, per gli illeciti di calunnia e diffamazione.

Il Segnalante è responsabile, anche in sede disciplinare, per le Segnalazioni effettuate al solo scopo di danneggiare il soggetto segnalato e/o altri soggetti, nonché per ogni altra ipotesi di utilizzo improprio od opportunistico del Canale di Whistleblowing.

Protezione del soggetto segnalato dalle segnalazioni in malafede

Tutti i soggetti sono tenuti al rispetto della dignità, dell'onore e della reputazione di ciascuno. A tale fine, è fatto obbligo ai Segnalanti di dichiarare se hanno un interesse privato collegato alla segnalazione. Più in generale, la società garantisce adeguata protezione dalle segnalazioni in malafede, censurando simili condotte ed informando che le segnalazioni inviate allo scopo di danneggiare o altrimenti recare pregiudizio nonché ogni altra forma di abuso del presente documento sono fonte di responsabilità, sia in sede disciplinare che nelle altre sedi competenti.

Tempi di conservazione della documentazione

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario all'elaborazione della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del Decreto 24 e nel rispetto di quanto previsto dal Regolamento (UE) 2016/679 in materia di protezione dei dati.

Trattamento dei dati personali

La Società e Boston Scientific Corporation sono co-titolari del trattamento ai sensi del Regolamento (UE) 2016/679, c.d. GDPR e forniscono ai destinatari una specifica informativa privacy. I dati personali dei Segnalanti, delle persone segnalate e di tutti i soggetti coinvolti nella segnalazione sono trattati coerentemente con quanto previsto dal Decreto 24, tenuto conto dell'equo bilanciamento tra i diritti della Persone Coinvolta ed il diritto alla riservatezza dell'identità del Segnalante, mettendo in atto misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali in conformità alla normativa e nel pieno rispetto del Regolamento (UE 2016/679).

L'esercizio dei diritti da parte del Segnalante o della Persona coinvolta, in relazione ai propri dati personali trattati nell'ambito del processo di gestione delle Segnalazioni, può essere limitato per garantire la tutela dei diritti e delle libertà altrui. Non è permesso alla Persona coinvolta di avvalersi dei propri diritti per ottenere informazioni sull'identità del Segnalante.

Diffusione e comunicazione sul canale e sulla procedura di segnalazione

La società ha messo a disposizioni informazioni chiare sul canale e sulla procedura per effettuare la segnalazione pubblicando la procedura sul sito internet della società [Boston Scientific -Compliance and Ethics](#), accessibile a chiunque, e sulla intranet aziendale accessibile solo ai dipendenti nell'area denominata "Whistleblowing" ed affiggendo la stessa nelle bacheche aziendali situate in ogni ufficio della Società.



WHISTLEBLOWING PROCEDURE (ITALY)

Contents

| | |
|---|---|
| Purpose..... | 1 |
| Parties Who Can Report (the Reporter) - Subjective Scope | 2 |
| Content of Report - Objective Scope..... | 2 |
| Reports Excluded | 3 |
| Report Manager | 3 |
| The Internal Channel - Reporting Procedure..... | 4 |
| Whistleblowing Platform Reporting Instructions and Procedural Process..... | 4 |
| Report Sent to Unauthorized Parties..... | 5 |
| Recommendations for Parties Intending to Make a Report..... | 5 |
| Platform Features..... | 5 |
| Protection Given to Reporters..... | 5 |
| Extension of Protection | 6 |
| Sanctions | 6 |
| External Reporting via the National Anti-Corruption Authority (“ANAC”) Channel | 6 |
| Public Disclosure..... | 6 |
| Reporter's Responsibilities | 7 |
| Protection of Parties Subject to Reports Made in Bad Faith | 7 |
| Document Retention Times..... | 7 |
| Processing Personal Data | 7 |
| Dissemination and Communication Regarding the Channel and the Reporting Procedure | 7 |

Purpose

In order to comply with the terms of Legislative Decree 24/2023 (hereinafter “Decree 24”) “*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019*”, regarding the protection of persons who report breaches of national or European Union regulations that have come to their attention in a public or private work environment and by the ANAC [National Anti-Corruption Authority] Guidelines of July 14, 2023, Boston Scientific S.p.a. (the “Company”), has adopted this procedure to regulate the process of transmitting, receiving, analyzing and managing so-called “Whistleblowing” Reports, in accordance with paragraph 2 bis of Article 6, Legislative Decree No. 231/2001 on the administrative responsibility of entities, as amended by Decree 24.

The purpose of this procedure is also to inform all interested parties that a platform has been set up that allows

reporting, even anonymously, of breaches of national and European Union regulations that may damage the public interest or the integrity of the Company, illegal conduct relevant for the purposes of Legislative Decree 231/2001 or breaches of the Organization, Management and Control Model ex Legislative Decree 231/2001, of the Code of Ethics and protocols, policies and procedures adopted by the Company.

Through the Whistleblowing Platform (hereinafter the "Platform"), which is accessible at the Boston Scientific website <http://advice.line.bostonscientific.com>, or via telephone at 800.727.406 an internal or external party as identified below, victim of any of the above violations who is aware of illegal conduct that has already occurred or that may be envisaged in the future, may report the behavior, act or omission, anonymously, ensuring compliance with the obligation of confidentiality provided by Art. 12 of Decree 24, so as to be protected from any retaliatory or discriminatory consequences related to reporting, according to the provisions of Art. 17 of Decree 24. The Platform, in fact, is operated by an independent third party vendor, and is a protected information channel that uses encryption tools to ensure the confidentiality of the reporting party's identity, the content of the report and the related documentation.

Parties Who Can Report (the Reporter) - Subjective Scope

The **Reporter** is the natural person making the report disclosing the alleged breaches brought to their attention within the context of their work and/or work activities or professional activities carried out for the Company (ex Art. 2, par. 1, point g) and point i) of Decree 24).

Parties who can make a report are:

- Internal Parties, such as:
 - Permanent and fixed-term employees
 - Managers
 - Parties on trial periods or in the interview phase
 - Former employees (after termination of employment)
 - Paid or non-paid trainees and volunteers
 - Shareholders
 - Persons with administrative, management, control, supervisory or representative roles (including within their normal duties).
 - Those who, while not in the employee category, work for the Company and are under the control and management of the Company (including but not limited to: interns, contract workers and those hired to work on specific projects, temporary workers);
- External Parties such as:
 - Suppliers of Goods or Services
 - Collaborators
 - Freelancers, consultants, collaborators

Content of Report - Objective Scope

This Platform can be used to report:

- behaviors that are in breach of the Organization, Management and Control Model, code of ethics, or other provisions within the organization;
- unlawful conduct relevant to Legislative Decree 231/2001;
- unlawful conduct arising from EU or national rules on: public procurement, financial product services and markets and prevention of money laundering and financing of terrorism, environmental protection, radiation protection and nuclear safety, public health, consumer protection, privacy and data protection and security of networks and information systems;
- acts or omissions which affect the financial interests of the EU;
- acts or omissions relating to the EU's internal market.

The Reporter should report only the information that is required for evaluation and verification. For this reason, it is suggested that the report should include:

- a clear and complete description of:
 - event or fact reported;
 - circumstances of time and place (if known), in which it occurred;
 - any other information that may provide useful details for the report;
 - any documents in support of the event or fact reported.

Please note that reporting insufficient information may lead to delays in the evaluation and investigations process, i.e. if the report is generic and/or lacks specific details, it may not be possible to be effectively reviewed.

It is strongly suggested, in line with the principle of minimizing unnecessary data collection, that details of the private lives of the parties being reported or otherwise involved, not be provided, if not strictly necessary and relevant for reporting purposes.

The protection measures provided by Decree 24 will be granted to the Anonymous Reporter, if subsequently identified.

Reports Excluded

This procedure and the safeguards provided for by Decree 24 do not apply to:

- complaints, claims or requests related to a personal interest of the person making the report that refer exclusively to their individual employment or public sector employment relationships, or pertaining to their employment or public sector employment relationships with higher-ranking figures;
- reports of breaches already regulated on a mandatory basis in part II of the Annex to Decree 24 or by national regulations that constitute the implementation of the European Union acts indicated in Part II of the Annex to the Directive (EU) 2019/1937;
- reports of breaches of national security, as well as contracts related to defense or national security, unless such matters fall within secondary legislation relevant to the European Union.

Report Manager

Reports will be managed promptly (within 7 calendar days of acknowledgment of receipt) by the Report Manager (hereafter the “Report Manager”) who is specifically trained to ensure that cases are handled in accordance with the requirements of Decree 24.

The Board of Directors on February 28, 2025 appointed the following parties, individually and for the respective roles and competences, as “Report Manager”:

- Tim Trujillo, Chief Compliance Officer
- Paul Flynn, Senior Director, Global Compliance Investigations and Audit and Monitoring
- Erina Mohamad Ramly, Director, Global Compliance Investigations
- Michael DiFrancesco, Administrator
- Karen Oden, Administrator
- Stephanie Marchand, Fellow, Global Compliance Investigations
- External Counsel, Baker McKenzie
- Federica Assumma, President of the Supervisory Board
- Massimiliano Lei, Supervisory Board
- Mario Occhini, Supervisory Board

Parties appointed as “Report Manager” have been previously authorized pursuant to Article 29 of the GDPR and so are authorized to know the reporter’s identifying data, in the event the Reporter provided their name.

All the reports will be initially reviewed by Baker McKenzie to ensure they are eligible for the protection granted by the Decree 24 and to check any possible conflict of interest related to any of the Report Managers.

The members of the Supervisory Board appointed as Report Manager will not automatically receive all the reports but will be involved only on topics of interest after a preliminary screening performed by other Report Managers.

The Internal Channel - Reporting Procedure

The following Internal Reporting channels pledge to protect the confidentiality of the Reporter's identity and the security of the information by providing selective access to said information only by specifically authorized personnel. In particular, the Internal Reporting channel is an **IT Platform** that allows the report to be made in **written format or verbally**, or by means of a direct meeting with the **Report Manager** within a reasonable

timeframe only upon a request from the Reporter.

Whistleblowing Platform Reporting Instructions and Procedural Process

The Reporter can access the platform via the link listed below and available on the Company website and on the corporate intranet site: [Boston Scientific-Compliance and Ethics](#)

Upon access, the system asks the Reporter to review the information on confidentiality and identity protection. Reports can be made anonymously or using the Reporter's name. As soon as the Reporter submits their report, they will receive an automated message which acknowledges receipt of the report and provides the Reporter a 7-character "Access Number" to access their report. They will also be prompted to create a password and security information the first time they access the report. The Reporter can then review status of their report, and if needed, communicate with the Report Manager throughout the investigation process and/or provide additional information. The Platform describes what information is collected based on the Reporter's option to report anonymously or to provide their name.

Within 7 days of the date of receipt of the report, the Report Manager will communicate with the Reporter via the Platform to acknowledge that the report has been received and/or request additional information.

The Reporter should use their own words to describe the facts that they intend to report, after selecting some answers to specific questions on the Platform. Files or other documents can be attached to support the description of the subject of the report.

The Report Manager makes an **initial assessment** of the report to check if all the requirements have been met in order to be able to give the Reporter the protection provided by Decree 24, and if it is possible to start the investigation. In particular, the report manager will consider the following:

- if Reporter is one of the parties cited by Art. 3 of Decree 24;
- if subject matter of the report falls within the breaches referred to by Art. 2 and, therefore, falls within the scope of the Report Manager and is not one of the exclusions expressly governed by Art. 1 paragraph 2 of Decree 24;
- if damage to the public interest or the integrity of the institution is manifestly absent;
- if there is no basis for the report because there are no facts to justify an investigation;
- if the report of the offense contains generic information that does not allow for an understanding of the facts, or is accompanied by inappropriate or non-relevant documentation, or there is a lack of data that is essential when reporting unlawful behavior;
- if there is a lack of data that is essential when reporting offenses listed by Report Management regulations;

During the investigation, the Report Manager will maintain a dialog with the Reporter to request additional insights and/or additional information, track activities carried out and provide information, even *ex officio*, on the progress of the investigation, at least with reference to the main decision-making milestones. In the event that it is necessary to communicate the Reporter's personal data or any detail related to the report or the Reporter to third parties (consultants specifically appointed to manage the investigation or part thereof, company managers e.g. HR Manager, Administrative Director, Legal Counsel, etc.), the Report Manager will ask, via the Platform, for explicit consent to communicate said data to third parties, provide reasons for the request and explain to whom the Reporter's data and the contents of the report will be communicated. The Reporter's consent or refusal will be tracked on the Platform.

To ensure an effective investigation process, it is Reporter's responsibility to periodically access the Platform to check if further information or action is needed, including granting consent to share Reporter's personal data or any detail related to the report or the Reporter to third parties.

When the investigation is closed, or in any case within **three (3) months** of the date of acknowledgment of receipt or, in the absence of such acknowledgment, within three months of the expiration of the 7-day deadline following the submission of the report, the Report Manager will provide feedback on the status of the investigation to the Reporter as defined in Art. 2 of the Decree 24.

Report Sent to Unauthorized Parties

If the internal report is submitted to a party other than the parties identified and authorized by the organization (the Report Manager), the report must be forwarded, within seven days of its proper receipt, to the authorized party, and the Reporter notified at the same time of the submission.

Recommendations for Parties Intending to Make a Report

Parties who intend to submit a report must clearly indicate in the subject of the report that this is a report in which they desire to keep their identity confidential and benefit from the safeguards provided in the event of any retaliation suffered as a result of the report.

This specification makes it possible, should the report erroneously be sent to an unauthorized party or be reported via a channel other than those specifically provided for by Decree 24, for the prompt transmission by said unauthorized party to the party authorized to receive and manage whistleblowing reports.

It should also be noted that the report and accompanying documents are not subject to the right of access to administrative acts provided for in Articles 22 et seq. of Law 241/1990, to the generalized civic access referred to in Art. 5 par. 2 of Legislative Decree 33/2013, as well as to the access referred to in Art. 2 undecies par. 1 point f) of the data protection code.

Platform Features

The Platform, supplied by Convergent by One Trust, adopts technical and organizational measures to ensure appropriate levels of security pursuant to Articles 25 and 32 of the GDPR, including encryption. An overview of those measures can be found [here](#).

Protection Given to Reporters

Boston Scientific protects Reporters against any form of retaliation or discrimination directly or indirectly related to the report, as required by Decree 24, and takes appropriate measures to ensure the confidentiality of the identity of the Reporter and other Persons involved, without prejudice to the legal obligations and protection of the rights of the Company or the Persons involved.

The Company has set out specific measures to protect the Reporter and others identified by Art. 3 of Decree 24, so that they are not subject to retaliation, discrimination or, under any circumstances, reporting-related penalties.

Section III (Art. 16 -22) of Decree 24 provides for measures to protect against discriminatory and retaliatory behavior against the person making the report.

Discriminatory measures means, for example, unjustified disciplinary action and any other form of retaliation leading to intolerable working conditions.

In particular, it is stated that certain measures may be declared null and void if taken in breach of Art. 17 of Decree 24:

- dismissal, suspension or equivalent measures;
- demotion of rank or failure to promote;
- change in duties, change in workplace, reduction in salary, change in working hours;
- suspension of training or any restriction of access to training;
- negative merit points or negative references;
- the adoption of disciplinary measures or other penalties, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavorable treatment;

- failure to convert a temporary employment contract into a permanent employment contract where the worker had a legitimate expectation of such conversion;
- and any other form of adverse treatment that could be detrimental to the individual concerned.
- on-renewal or early termination of a temporary employment contract;
- damage, including to personal reputation, particularly on social media, or financial or economic losses, including loss of economic opportunity and loss of income.

Extension of Protection

The protective measures referred to in Section III also apply to:

- facilitators (natural persons who assist a reporting party in the reporting process, operate within the same work environment and whose assistance must be kept confidential);
- persons in the same working environment as the reporting party, who are linked to said party by a stable emotional or family bond up to the fourth degree;
- the Reporter's work colleagues who work in the same work environment and who have a habitual and current relationship with that person;
- entities owned by the Reporter for which said persons work, as well as entities operating in the same working environment as the aforementioned persons.

In the event of discriminatory measures being taken against the reporting parties, Article 19 of Decree 24 provides that this situation can be communicated, not only to the Company, but also to ANAC which informs the National Labor Inspectorate, for measures within its remit, if the discriminatory measure is not lifted by said Company.

Sanctions

The Boston Scientific S.p.a. Disciplinary System provides for penalties in the event of retaliation or when it is determined that reporting has been obstructed or that an attempt has been made to obstruct it or that the confidentiality obligation set out in Art. 12 of Decree 24 has been breached.

Within the context of judicial or administrative proceedings, or in any case of out-of-court disputes relating to the detection of retaliatory conduct, acts or omissions against reporting parties, it is assumed that the latter were implemented as a result of the reporting. The burden of proving that said conduct or acts are motivated by reasons other than the reporting shall be borne by the person carrying out said conduct or acts (employer or person authorized by it).

External Reporting via the National Anti-Corruption Authority (“ANAC”) Channel

ANAC has set up reporting channels that must guarantee, including through the use of encryption tools, the confidentiality:

- of the identity of the reporting party
- of the person involved and of any person who may be mentioned in the report
- of the contents of the report and its documentation

The use of external reporting via the ANAC channel is only allowed provided that:

- no provision has been made for the mandatory set up of an internal reporting channel within the context of the working environment, even if this is mandatory. The internal reporting channel is not active or, although it has been set up, does not comply with Art. 4 of Decree 24;
- the reporting party has already made an internal report pursuant to Article 4 and the report was not followed up on;
- the reporting party has reasonable grounds to believe that, if an internal report were filed, the report would not be effectively followed up or that said report could bring about the risk of retaliation;
- the reporting party has reasonable grounds to believe that the breach could constitute an imminent or manifest danger to the public interest.

Public Disclosure

The Reporter, pursuant to Art. 15 of Decree 24, is also protected when making a so-called “**public disclosure**” of information on the breaches via the press or electronic media or, in any event, by a means of dissemination capable of reaching a large number of people (ex Art. 2, par. 1, point f), Decree 24).

The protection of the Reporter in this case is guaranteed only if, at the time of disclosure, one of the following

conditions applies:

- the Reporter has already made an internal and external report or has made a direct external report, under the conditions, and using the procedures, set out by the regulations, but acknowledgment was not received within the deadlines set;
- the Reporter has good reason to believe that the breach could constitute an imminent or clear danger to the public interest;
- the Reporter has reason to believe that the external report may result in a risk of retaliation or may not be effectively pursued because of the specific circumstances of the actual case, such as cases where evidence may be concealed or destroyed, or where there is a reasonable fear that the person receiving the report may have colluded with the perpetrator of the breach or be involved in the breach.

Reporter's Responsibilities

The Reporter is held liable, including being subject to disciplinary action, in the event of slanderous or libelous reports, or reports made intentionally, or due to gross misconduct, of facts that are not true.

Art. 21, par. 1 point c) of Decree 24, provides that ANAC may impose a fine of EUR 500 to 2.500 on the Reporter, where public liability is ascertained, as a result of willful or gross misconduct, for slander and defamation.

The Reporter shall be held liable, including during disciplinary action, for Reports made solely for the purpose of damaging the person who is the subject of the report and/or other parties, and any other hypotheses of improper or opportunistic use of the Whistleblowing Channel.

Protection of Parties Subject to Reports Made in Bad Faith

All parties are expected to respect each other's dignity, honor and reputation. For this purpose, Reporters parties are required to declare whether they have a private interest related to the report. More generally, the company guarantees adequate protection against bad faith reports, censoring such conduct and informing parties that reports filed in order to damage or otherwise cause harm, and any other form of abuse of this document, are a source of liability, either in a disciplinary setting and in other appropriate settings.

Document Retention Times

Reports and related documentation shall be kept for the time necessary to process the report and, in any event, no longer than five years from the date of notification of the final outcome of the reporting procedure, in accordance with the confidentiality obligations referred to in Article 12 of Decree 24 and in accordance with Regulation (EU) 2016/679 on data protection.

Processing Personal Data

The Company is the Data Controller of the processing pursuant to Regulation (EU) 2016/679, the so-called GDPR and provides the recipients with a specific privacy policy. The personal data of Reporters, Persons being Reported and all parties involved in the Report are processed in accordance with the provisions of Decree 24, taking into account the fair balance between the rights of the Person Involved and the right to confidentiality of the Reporter's Identity, taking appropriate technical and organizational measures to ensure the security of personal data in accordance with legislation and in full compliance with the Regulation (EU 2016/679).

Rights exercised by the Reporter or the Person involved, in relation to their personal data processed as part of the Report management process, may be limited to ensure the protection of the rights and freedoms of others. The Person involved is not allowed to use their rights to obtain information on the identity of the Reporter.

Dissemination and Communication Regarding the Channel and the Reporting Procedure

The company has provided clear information regarding the channel and the procedure for filing a report by publishing the procedure on the company's website [Boston Scientific -Compliance and Ethics](#), which can be accessed by anyone and on the company intranet which is accessible only to employees in the "Whistleblowing" area and by posting it on company notice boards located in each of the Company's offices.