



la lucente spa®

Politica di Whistleblowing

Approvata dal Consiglio di Amministrazione in data 29.06.2026

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE.....	3
2. EVOLUZIONE NORMATIVA.....	3
3. AMBITO DI APPLICAZIONE SOGGETTIVO.....	4
4. OGGETTO E CONTENUTO DELLA SEGNALAZIONE.....	4
5. CANALI DI SEGNALAZIONE INTERNA E GESTIONE DELLE SEGNALAZIONI.....	5
5.1 Segnalazioni tramite canale on-line.....	6
5.2 Segnalazioni orali.....	7
5.3 Canali di segnalazione esterna.....	7
5.3.1. Condizioni per poter effettuare la segnalazione esterna ad ANAC.....	7
5.4 Divulgazione pubblica.....	8
6. TUTELA DEL SEGNALANTE.....	8
6.1 Garanzia di riservatezza.....	10
7. ESAME, RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI.....	11
8. PUBBLICITA'.....	12

Edizione	Descrizione modifiche	Data
00	Prima emissione del documento in attuazione del D.Lgs. 24/2023	08/11/2023
01	Revisione alla luce delle Linee Guida ANAC 478/2025 e 479/2025 e della Guida operativa per gli enti privati di Confindustria del 14 maggio 2026	29/06/2026

1. SCOPO E CAMPO DI APPLICAZIONE

La Lucente S.p.A. (di seguito anche "**La Lucente**" o "**Società**") ha adottato un Modello di Organizzazione, Gestione e Controllo (di seguito anche "**Modello**") ai sensi del D.Lgs. 231/2001, nonché un Codice Etico aziendale.

Inoltre, La Lucente ha stabilito, documentato ed attuato il proprio sistema di gestione integrato in conformità agli standard applicabili: UNI EN ISO 9001, UNI EN ISO 14001, UNI EN ISO 45001, UNI EN ISO 37001, ISO/IEC 27001, SA 8000, UNI EN ISO 50001 e UNI PdR:125.

La presente procedura disciplina, come *infra* meglio dettagliato, il processo di ricezione, analisi e trattamento delle segnalazioni di violazioni di diritto nazionale e dell'Unione Europea, violazioni del Modello e delle procedure ad esso correlate, del Codice Etico, delle politiche o regolamenti aziendali, da chiunque inviate o trasmesse, anche in forma anonima.

2. EVOLUZIONE NORMATIVA

Il 30 novembre 2017 è entrata in vigore la legge n. 179 recante *«Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato»*.

In data 23 ottobre 2019 è intervenuta la direttiva europea 2019/1937 del Parlamento Europeo e del Consiglio, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione Europea e che è stata recepita in Italia con il D.Lgs. 10 marzo 2023 n. 24, in vigore dal 30 marzo 2023.

La Società, preso atto dell'art. 6, comma 2-bis, D.Lgs. 231/2001, per come modificato dalla legge 30 novembre 2017, n. 179 e successivamente dal D.Lgs. 10 marzo 2023, n. 24, ha inteso adeguarsi alla citata normativa, dotandosi di regole interne per il ricevimento e gestione delle segnalazioni e, altresì, di strumenti di tutela nei confronti di quanti, in buona fede, effettuano segnalazioni di tal specie all'Organismo di Vigilanza ex D.Lgs. 231/2001 della Società (di seguito anche "**OdV**"), individuato quale "Gestore" delle segnalazioni *whistleblowing*.

La Lucente ha, quindi, provveduto a dotarsi di un sistema di segnalazioni *whistleblowing*, in linea con la normativa citata e tenendo conto anche delle linee guida emanate dall'Autorità Nazionale Anticorruzione (di seguito "**ANAC**"), con delibere n. 311 del 12 luglio 2023, n. 478 e 479 del 26 novembre 2025, e della "Guida Operativa per gli Enti Privati", predisposta da Confindustria e pubblicata nella sua versione aggiornata in data 14 maggio 2026.

Con riferimento, poi, al sistema di gestione integrato adottato dalla Società, si rileva che:

- ✓ la norma ISO 37001 al punto 8.9 definisce che siano attuate procedure affinché le persone possano segnalare in buona fede ed in via confidenziale violazioni o carenze del sistema di gestione della corruzione;
- ✓ la norma SA 8000 al punto 9.6 chiede che siano attuate procedure affinché le

persone e le parti interessate possano segnalare in buona fede ed in via confidenziale violazioni o carenze rispetto allo standard;

- ✓ la Linea Guida Uni PdR 125 chiede che siano attuate procedure affinché le persone e le parti interessate possano segnalare in buona fede ed in via confidenziale violazioni o carenze rispetto allo standard.

3. AMBITO DI APPLICAZIONE SOGGETTIVO

Possono segnalare informazioni rilevanti ai sensi del successivo paragrafo (vd. *infra*) le persone appartenenti al contesto lavorativo de La Lucente e che rientrino nelle seguenti categorie:

- ✓ lavoratori subordinati;
- ✓ lavoratori autonomi;
- ✓ collaboratori a vario titolo;
- ✓ liberi professionisti e consulenti;
- ✓ volontari, stagisti e tirocinanti, anche se non retribuiti;
- ✓ persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- ✓ azionisti;
- ✓ soggetti che operano nel contesto lavorativo de La Lucente in virtù di rapporti con altri operatori economici.

La possibilità di segnalare e di beneficiare delle misure di protezione previste dal D.Lgs. 10 marzo 2023, n. 24, è prevista anche qualora la segnalazione avvenga nei seguenti casi:

- quando il rapporto giuridico con il segnalante non è ancora iniziato;
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico con il segnalante.

4. OGGETTO E CONTENUTO DELLA SEGNALAZIONE

Attraverso i canali di segnalazione interna messi a disposizione dalla Società (vd. *infra*) è possibile comunicare, con garanzia di riservatezza, informazioni riguardanti:

- ✓ illeciti amministrativi, contabili, civili o penali;
- ✓ condotte illecite rilevanti ai sensi del D.Lgs. 231/2001, c.d. "reati presupposto" (artt. 24 e ss.);
- ✓ violazioni del Modello, che non rientrano nell'art. 2, comma 1, lettera a), numeri 3), 4), 5) e 6) del D.Lgs. n. 24/2023;
- ✓ violazioni del Codice Etico e delle procedure operative adottati da La Lucente, anche se non aventi immediata rilevanza penale;
- ✓ violazioni della sicurezza delle informazioni: trattamento illecito dei dati in violazione del Regolamento (UE) 2016/679 – GDPR, delle policy e dei regolamenti aziendali,

accesso abusivo ai sistemi informatici o telematici (art. 615-ter c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche e telematiche (art. 617-quater c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), etc.;

- ✓ violazioni del Sistema di Gestione Integrato, in conformità agli standard applicabili UNI EN ISO 9001, UNI EN ISO 14001, UNI EN ISO 45001, UNI EN ISO 37001, ISO/IEC 27001, SA 8000, UNI EN ISO 50001 e UNI PdR:125.

In linea generale, si precisa che la normativa prevede altresì la possibilità di segnalare:

- ✓ illeciti che rientrano nell'ambito del diritto dell'Unione Europea, relativamente a specifici settori (a titolo esemplificativo: servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; tutela dell'ambiente; tutela della vita privata e protezione dei dati personali; sicurezza delle reti e dei sistemi informativi);
- ✓ atti od omissioni che ledono gli interessi finanziari dell'Unione Europea;
- ✓ atti od omissioni riguardanti (art. 26, par 2, TFUE) la libera circolazione delle merci, delle persone, dei servizi e dei capitali nel mercato interno, comprese violazioni delle norme dell'Unione Europea in materia di concorrenza; aiuti di Stato; imposte sulle società;
- ✓ atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea.

In particolare, è possibile segnalare informazioni apprese durante lo svolgimento della propria attività lavorativa o professionale, ovvero durante il processo di selezione o in altre fasi pre o post contrattuali.

Restano escluse dalle segnalazioni ammissibili quelle aventi ad oggetto: contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate.

Il contenuto della segnalazione deve essere chiaro, preciso e circostanziato. In ogni caso, le misure di protezione previste per il segnalante si applicano anche in caso di infondatezza della segnalazione, se, al momento della segnalazione, la persona aveva fondato motivo di ritenere che le informazioni sulle violazioni fossero vere e rientrassero nell'ambito oggettivo di applicazione della procedura.

5. CANALI DI SEGNALAZIONE INTERNA E GESTIONE DELLE SEGNALAZIONI

Le segnalazioni possono essere presentate con diverse modalità:

- a. in forma scritta, tramite canale on-line sul sito internet de La Lucente S.p.A.;
- b. in forma orale, mediante un incontro diretto con l'OdV, da richiedere via e-mail all'indirizzo odv@lalucente.it.

La segnalazione deve contenere una circostanziata descrizione dei fatti e dei comportamenti considerati in contrasto con la normativa, indicando, ove possibile, anche i documenti, le regole che si considerano violate e gli altri riscontri utili a condurre

l'accertamento sui fatti contestati. Inoltre, il segnalante ha l'obbligo di dichiarare se ha un interesse personale collegato alla segnalazione.

L'OdV rilascia al segnalante avviso di ricevimento della segnalazione entro 7 (sette) giorni dalla ricezione della stessa da parte dell'OdV.

I tempi previsti per la conclusione del procedimento sono di 3 (tre) mesi dalla data dell'avviso di ricevimento della segnalazione o, in mancanza di tale avviso, di 3 (tre) mesi dalla scadenza del termine di 7 (sette) giorni dalla presentazione della segnalazione.

Nel caso in cui un componente dell'OdV si trovi in posizione di conflitto di interessi nella valutazione della segnalazione e/o nell'esecuzione dell'istruttoria, il componente ha obbligo di astenersi e la segnalazione sarà gestita dagli altri componenti dell'OdV. Ove la posizione in conflitto di interessi riguardi l'OdV nel suo complesso, è fatto divieto all'OdV di procedere con l'analisi e l'istruttoria della segnalazione. In tal caso, può essere attivato un processo alternativo di gestione che prevede che tale segnalazione sia visibile al Compliance Manager, che ne gestirà l'istruttoria, coinvolgendo, ove ritenuto opportuno, altre strutture interne o esterne alla Società.

Eventuali segnalazioni ricevute per errore da soggetti diversi dall'OdV, devono essere trasmesse da questi ultimi all'OdV entro 7 (sette) giorni dal loro ricevimento, nel rispetto della riservatezza del segnalante e del contenuto della segnalazione e dandone contestuale notizia alla persona segnalante.

Resta ferma la possibilità per il segnalante, laddove si verificano le particolari condizioni previste dal legislatore, di effettuare una segnalazione esterna ad ANAC (ai sensi degli artt. 65 e 7, D.Lgs. n. 24/2023), una divulgazione pubblica (ai sensi dell'art. 15, D.Lgs. n. 24/2023) o una denuncia all'autorità giudiziaria competente.

5.1. Segnalazioni tramite canale on-line

Nel caso di segnalazione tramite canale on-line, il segnalante ottiene un codice identificativo univoco, da utilizzare per essere informato sullo stato di lavorazione della segnalazione inviata e sull'esito dell'eventuale istruttoria, e tale da garantire la riservatezza della sua identità.

Qualora il segnalante abbia indicato le proprie generalità e il proprio indirizzo e-mail all'atto della trasmissione della segnalazione, il segnalante riceverà il codice identificativo univoco della segnalazione sull'indirizzo e-mail indicato, entro 7 (sette) giorni dalla ricezione della stessa da parte dell'Organismo di Vigilanza.

Nel caso di segnalazione anonima, in cui le generalità del segnalante e l'indirizzo e-mail non sono note, sarà in ogni caso possibile per il segnalante accedere al sistema con il codice identificativo univoco assegnato e monitorare lo stato della propria segnalazione.

È onere del segnalante conservare con cura il codice identificativo della segnalazione, in quanto, in caso di smarrimento, lo stesso non potrà essere recuperato o duplicato in alcun modo.

Tutte le segnalazioni che pervengono all'OdV al di fuori del canale on-line, verranno censite su tale canale a cura dell'OdV medesimo, entro 7 (sette) giorni dalla ricezione, così da consentire, ove possibile, il rilascio al segnalante di un codice identificativo univoco per accedere al sistema e monitorare lo stato della propria segnalazione.

5.2. Segnalazioni orali

Il segnalante può effettuare una segnalazione anche in forma orale, domandando la fissazione di un incontro diretto con l'Organismo di Vigilanza.

L'OdV offrirà la sua disponibilità a svolgere l'incontro entro un termine ragionevole di tempo dalla richiesta, sia in luogo interno che esterno alla sede della Società. Le modalità e i tempi dell'incontro saranno definiti in coerenza con l'obiettivo di tutelare la riservatezza circa l'identità del segnalante e del contenuto della segnalazione. La segnalazione effettuata oralmente sarà documentata mediante verbale a cura dell'OdV. Tale verbale potrà essere verificato, rettificato e confermato da parte della persona segnalante, mediante la propria sottoscrizione.

Per ragioni di sicurezza e tutela della riservatezza sarà vietato, in questi casi, ricorrere a sistemi di video e/o fono registrazione, salvo che gli strumenti impiegati non garantiscano i più elevati standard di sicurezza informatica e conformità al GDPR.

5.3 Canali di segnalazione esterna

Presso l'ANAC è attivo un canale di segnalazione esterna che garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La segnalazione esterna può essere presentata nei confronti di ANAC:

a) in forma scritta, utilizzando l'apposita piattaforma informatica reperibile sul sito internet istituzionale dell'Autorità (<https://www.anticorruzione.it/-/whistleblowing>);

b) in forma orale:

- avvalendosi delle linee telefoniche dedicate;
- utilizzando i sistemi di messaggistica vocale appositamente predisposti;
- chiedendo la fissazione di un incontro diretto con i funzionari di ANAC.

5.3.1 Condizioni per poter effettuare la segnalazione esterna ad ANAC

La segnalazione esterna può essere presentata esclusivamente se al momento della presentazione:

- il canale di segnalazione interna non è attivo oppure, anche se attivo, non è conforme a quanto previsto dall'art. 4, D.Lgs. 24/2023;
- la persona segnalante ha già effettuato una segnalazione interna ai sensi della presente

procedura e la stessa non ha avuto seguito;

- la persona segnalante ha fondati motivi di ritenere che, laddove decidesse di effettuare una segnalazione interna, alla stessa non sarebbe dato efficace seguito;
- la persona segnalante ha fondati motivi di ritenere che, laddove decidesse di effettuare una segnalazione interna, da ciò conseguirebbe per lei un rischio di ritorsioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le Linee Guida ANAC, emanate con delibera n. 311 del 12 luglio 2023 e modificate con delibera n. 479 del 26 novembre 2025, introducono, inoltre, la possibilità di effettuare segnalazioni ad ANAC per i soggetti che avendo un legame qualificato con il segnalante, denunciante o divulgatore pubblico, subiscono ritorsioni in ragione di detta connessione. Si tratta di: facilitatori, persone del medesimo contesto lavorativo, colleghi di lavoro che hanno un rapporto abituale e corrente con il segnalante, e anche soggetti giuridici nei casi in cui siano enti di proprietà del segnalante, denunciante, divulgatore pubblico o enti in cui lavora o enti che operano nel medesimo contesto lavorativo.

5.4 Divulgazione pubblica

La persona segnalante può effettuare una divulgazione pubblica e beneficiare delle misure di protezione previste dal D.Lgs. n. 24/2023 a condizione che, al momento della divulgazione pubblica¹:

- la persona segnalante abbia previamente effettuato una segnalazione interna ed esterna ovvero abbia effettuato direttamente una segnalazione esterna, e non abbia ottenuto riscontro nei termini previsti dalla normativa;
- la persona segnalante abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante abbia 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.

6 TUTELA DEL SEGNALENTE

Il D.Lgs. 10 marzo 2023, n. 24, prevede specifiche misure di protezione a favore delle persone segnalanti, nonché a tutela dei seguenti ulteriori soggetti:

- i c.d. "facilitatori", ossia le persone fisiche che abbiano assistito una persona segnalante nel processo di segnalazione, operando all'interno del medesimo contesto lavorativo;
- le persone del medesimo contesto lavorativo della persona segnalante e che sono

¹ Ai fini del D.Lgs. n. 24/2023, per "divulgazione pubblica" si intende il comportamento di chi rende di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

legate da uno stabile legame affettivo o di parentela entro il quarto grado;

- i colleghi di lavoro della persona segnalante e che hanno con detta persona un rapporto abituale e corrente;
- gli enti di proprietà della persona segnalante o per i quali la stessa persona lavori, nonché agli enti che operano nel medesimo contesto lavorativo del segnalante.

I motivi che hanno indotto la persona a segnalare o denunciare o divulgare pubblicamente sono irrilevanti ai fini della sua protezione.

La Lucente S.p.A. riconosce e fa proprie le misure di protezione previste dal D.Lgs. 24/2023, comminando sanzioni nei confronti di chiunque le violi, ponendo in essere atti discriminatori o ritorsivi nei confronti dei segnalanti. In particolare, si ricorda che il D.Lgs. cit. prevede il divieto assoluto di ritorsioni, quali a titolo esemplificativo:

- a) il licenziamento, la sospensione o misure equivalenti;
- b) la retrocessione di grado o la mancata promozione;
- c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- e) le note di merito negative o le referenze negative;
- f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- g) la coercizione, l'intimidazione, le molestie o l'ostracismo;
- h) la discriminazione o comunque il trattamento sfavorevole;
- i) 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;
- j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- k) 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;
- l) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- m) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- n) l'annullamento di una licenza o di un permesso;
- o) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Gli atti assunti in violazione del divieto di ritorsioni sono nulli.

6.1. Garanzia di riservatezza

È sempre garantita la riservatezza sull'identità del segnalante. In nessun caso, pertanto, l'identità del segnalante sarà divulgata o rivelata a terzi senza il suo preventivo, espresso e formale consenso².

Sono ammesse le seguenti deroghe, previste dalla legge:

- procedimento penale (art. 12, comma 3): l'identità è coperta dal segreto ai sensi dell'art. 329 c.p.p., senza necessità di consenso;
- procedimento dinanzi alla Corte dei conti (art. 12, comma 4): l'identità non può essere rivelata fino alla chiusura della fase istruttoria;
- procedimento disciplinare (art. 12, comma 5): qualora la contestazione sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa, l'identità non può essere rivelata in nessun caso. Qualora invece la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità sia indispensabile per la difesa dell'incolpato, la segnalazione è utilizzabile a fini disciplinari solo previo consenso espresso del segnalante. In assenza di consenso, la segnalazione non può essere utilizzata a fini disciplinari.

In tutte le ipotesi in cui la rivelazione dell'identità sia dovuta, al segnalante è dato avviso mediante comunicazione scritta delle ragioni della stessa.

Durante le attività di indagine sulla segnalazione è, inoltre, garantita la riservatezza sull'identità della persona coinvolta e della persona menzionata nella segnalazione, sul contenuto della stessa e sulla relativa documentazione a supporto, nonché sul fatto stesso della segnalazione.

La riservatezza sull'identità della persona coinvolta e della persona menzionata, sul contenuto e sul fatto della segnalazione, nonché sulla documentazione inerente, può essere derogata – in tutto o in parte – in caso di accertata fondatezza della segnalazione (in termini di ragionevolezza), anche al fine di consentire l'attivazione degli opportuni e ulteriori accertamenti nell'ambito degli eventuali procedimenti disciplinari, giuslavoristici, civili, penali o amministrativi.

I dati personali trattati ai fini della gestione delle segnalazioni devono essere:

- i. limitati a quelli strettamente e obiettivamente necessari per verificare la fondatezza della segnalazione e per la relativa gestione;
- ii. trattati lecitamente e secondo correttezza.

² Nei casi in cui l'eventuale procedimento disciplinare a carico della persona coinvolta dalla segnalazione sia fondato interamente o in maniera prevalente sulla segnalazione, il mancato consenso del segnalante a rivelare la propria identità determinerà l'impossibilità a procedere nella contestazione.

Si precisa che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione, non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

All'interno del canale on-line di riferimento e nell'apposita sezione del sito internet, viene resa disponibile al segnalante e al segnalato una specifica informativa in materia di protezione dei dati personali trattati in applicazione della presente procedura.

Il trattamento dei dati personali di tutti soggetti interessati coinvolti nel processo di segnalazione è effettuato da parte di La Lucente S.p.A. nella sua qualità di Titolare del trattamento ai sensi dell'art. 4, n. 7. del GDPR, nel pieno rispetto della normativa sulla tutela dei dati personali vigente e delle procedure adottate dalla Società in materia.

La Società ha definito il proprio processo di gestione delle segnalazioni, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati e disciplinando il rapporto con eventuali soggetti esterni che trattano dati personali per suo conto ai sensi dell'articolo 28 del GDPR. Il trattamento dei dati personali effettuati ai fini della presente procedura è svolto esclusivamente da personale espressamente autorizzato a la propria identità determinerà l'impossibilità a procedere nella contestazione. 9 trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del GDPR e dell'articolo 2 quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

La Società, nell'ambito del processo di whistleblowing, rende in favore degli interessati un'apposita informativa ai sensi degli art. 13 e 14 del GDPR, disponibile sul canale di segnalazione. Le tutele di cui alla presente procedura non sono garantite e al segnalante è irrogata una sanzione disciplinare qualora – anche con sentenza di primo grado – sia stata accertata la sua responsabilità penale per i reati di diffamazione o di calunnia ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

7 ESAME RACCOLTA CONSERVAZIONE ED ARCHIVIAZIONE DELLE INFORMAZIONI

Le attività di verifica circa la fondatezza delle circostanze rappresentate nella segnalazione sono di competenza dell'Organismo di Vigilanza, il quale vi provvede nel rispetto dei principi di equità, imparzialità e riservatezza ed effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante – se conosciuto – e di eventuali altri soggetti che possono riferire sui fatti segnalati.

L'OdV esamina le segnalazioni ricevute, effettuando un'istruttoria preliminare al fine di verificare l'esistenza di dati ed informazioni utili a circostanziarne l'accaduto.

Qualora dall'analisi preliminare non emergano elementi sufficientemente circostanziati o risulti infondato il richiamo dei fatti, la segnalazione viene archiviata.

Laddove emergano elementi utili e sufficienti perché la segnalazione venga ritenuta fondata, verrà avviata l'effettiva fase di approfondimento istruttorio, coinvolgendo, ove ritenuto opportuno, altre strutture interne o esterne alla Società.

Al termine degli approfondimenti, l'OdV definisce l'istruttoria e ne formalizza per iscritto gli esiti, provvedendo, in relazione alle risultanze, alla trasmissione agli organi o funzioni competenti per le eventuali iniziative di competenza.

L'OdV conserva i dati e i documenti relativi ad ogni segnalazione per 36 mesi dalla chiusura della segnalazione, nel rispetto della normativa vigente e della presente procedura, fatte salve, in ogni caso, esigenze di carattere giudiziario e/o specifici obblighi di legge che giustifichino un tempo di conservazione superiore.

I dati personali contenuti nella segnalazione verranno trattati nel rispetto della normativa e delle procedure e/o informative adottate e/o che saranno adottate dalla Società in materia di protezione dei dati personali.

8 PUBBLICITÀ

La presente procedura, nel rispetto di quanto disposto dall'art. 5, lett. e), D.Lgs. 24/2023, è resa disponibile secondo le modalità di seguito indicate:

- a) pubblicazione in una sezione dedicata del sito internet aziendale, la stessa dalla quale è possibile accedere al canale informatico (piattaforma) di segnalazione (<https://digitalroom.bdo.it/lalucente/home.aspx>);
- b) affissione in formato cartaceo presso i locali aziendali frequentati dai lavoratori, nonché dai rappresentanti di fornitori e clienti, dai consulenti, ecc.
- c) organizzazione di periodiche sessioni formative, volte a illustrarne il funzionamento (eventualmente con l'ausilio di esemplificazioni e dello studio di casi pratici).



la lucente spa®

Whistleblowing Policy

Approved by the Board of Directors on 29 June 2026

CONTENTS

1. PURPOSE AND SCOPE OF APPLICATION.....	3
2. REGULATORY DEVELOPMENTS.....	3
3. SCOPE OF APPLICATION.....	4
4. SUBJECT MATTER AND CONTENT OF REPORTS.....	4
5. INTERNAL REPORTING CHANNELS AND MANAGEMENT OF REPORTS.....	5
5.1 Reports via the online channel.....	6
5.2 Verbal reports.....	7
5.3 External reporting channels.....	7
5.3.1. Conditions for making an external report to ANAC.....	7
5.4 Public disclosure.....	8
6. PROTECTION OF WHISTLEBLOWERS.....	8
6.1 Guarantee of confidentiality.....	10
7. REVIEW, COLLECTION AND STORAGE OF INFORMATION.....	11
8. PUBLICITY.....	12

Edition	Description of changes	Date
00	First issue of the document implementing Legislative Decree 24/2023	8 November 2023
01	Revision in light of ANAC Guidelines 478/2025 and 479/2025 and the Confindustria Operational Guide for private bodies dated 14 May 2026	29 June 2026

1. PURPOSE AND SCOPE OF APPLICATION

La Lucente S.p.A. (hereinafter also referred to as “**La Lucente**” or “**the Company**”) has adopted an Organisation, Management and Control Model (hereinafter also referred to as the “**Model**”) pursuant to Legislative Decree 231/2001, as well as a Corporate Code of Ethics.

Furthermore, La Lucente has established, documented and implemented its integrated management system in accordance with the applicable standards: UNI EN ISO 9001, UNI EN ISO 14001, UNI EN ISO 45001, UNI EN ISO 37001, ISO/IEC 27001, SA 8000, UNI EN ISO 50001 and UNI PdR:125.

This procedure governs, as detailed below, the process for receiving, analysing and handling reports of breaches of national and European Union law, breaches of the Compliance Model and related procedures, the Code of Ethics, and company policies or regulations, submitted or transmitted by any person, including anonymously.

2. REGULATORY DEVELOPMENTS

On 30 November 2017, Law No. 179 came into force, setting out “*Provisions for the protection of persons who report offences or irregularities of which they have become aware in the course of their employment in the public or private sector*”.

On 23 October 2019, European Directive 2019/1937 of the European Parliament and of the Council came into force, concerning the protection of persons who report breaches of European Union law; this was transposed into Italian law by Legislative Decree No. 24 of 10 March 2023, which came into force on 30 March 2023.

The Company, having taken note of Article 6, paragraph 2-bis, of Legislative Decree 231/2001, as amended by Law No. 179 of 30 November 2017 and subsequently by Legislative Decree No. 24 of 10 March 2023, No. 24, has sought to comply with the aforementioned legislation by adopting internal rules for the receipt and handling of reports and, furthermore, by establishing safeguards for those who, in good faith, submit such reports to the Company's Supervisory Body pursuant to Legislative Decree 231/2001 (hereinafter also referred to as the “SB”), designated as the the “Manager” of *whistleblowing* reports.

Lucente has therefore established a *whistleblowing* reporting system, in line with the aforementioned legislation and taking into account the guidelines issued by the National Anti-Corruption Authority (hereinafter “ANAC”), through Resolutions Nos. 311 of 12 July 2023, Nos. 478 and 479 of 26 November 2025, and the “Operational Guide for Private Entities”, drawn up by Confindustria and published in its updated version on 14 May 2026.

With regard to the integrated management system adopted by the Company, it should be noted that:

- ✓ clause 8.9 of ISO 37001 stipulates that procedures must be put in place to enable individuals to report, in good faith and confidentially, breaches or shortcomings in the anti-bribery management system;

- ✓ SA 8000, in clause 9.6, requires that procedures be put in place to enable individuals and interested parties to report, in good faith and confidentially, any breaches or shortcomings in relation to the standard;
- ✓ Uni PdR 125 Guidance requires that procedures be put in place to enable individuals and interested parties to report, in good faith and confidentially, breaches or shortcomings in relation to the standard.

3. SCOPE OF APPLICATION

Persons belonging to La Lucente's workplace who fall into the following categories may report relevant information in accordance with the following paragraph (see *below*):

- ✓ employees;
- ✓ self-employed workers;
- ✓ contributors in various capacities;
- ✓ freelancers and consultants;
- ✓ volunteers, interns and trainees, even if unpaid;
- ✓ persons holding administrative, managerial, supervisory, monitoring or representative roles;
- ✓ shareholders;
- ✓ persons operating within La Lucente's working environment by virtue of relationships with other economic operators.

The right to make a report and to benefit from the protective measures provided for by Legislative Decree No. 24 of 10 March 2023 also applies where the report is made in the following circumstances:

- when the legal relationship with the whistleblower has not yet commenced;
- during the probationary period;
- following the termination of the legal relationship with the whistleblower.

4. SUBJECT AND CONTENT OF THE REPORT

Through the internal reporting channels made available by the Company (see *below*), it is possible to report, with a guarantee of confidentiality, information concerning:

- ✓ administrative, accounting, civil or criminal offences;
- ✓ unlawful conduct relevant under Legislative Decree 231/2001, known as 'predicate offences' (Articles 24 et seq.);
- ✓ breaches of the Model that do not fall within the scope of Article 2(1)(a)(3), (4), (5) and (6) of Legislative Decree No 24/2023;
- ✓ breaches of the Code of Ethics and the operating procedures adopted by La Lucente, even if they do not have immediate criminal relevance;
- ✓ breaches of information security: unlawful processing of data in breach of Regulation

(EU) 2016/679 – GDPR, company policies and regulations, unauthorised access to IT or telecommunications systems (Article 615-ter of the Italian Criminal Code), unlawful interception, obstruction or interruption of IT and telecommunications communications (Article 617-quater of the Italian Criminal Code), damage to information, data and computer programmes (Article 635-bis of the Italian Criminal Code), etc.;

- ✓ breaches of the Integrated Management System, in accordance with the applicable standards UNI EN ISO 9001, UNI EN ISO 14001, UNI EN ISO 45001, UNI EN ISO 37001, ISO/IEC 27001, SA 8000, UNI EN ISO 50001 and UNI PdR:125.

In general, it should be noted that the legislation also provides for the possibility of reporting:

- ✓ offences falling within the scope of European Union law, relating to specific sectors (for example: services, financial products and markets, and the prevention of money laundering and terrorist financing; environmental protection; privacy and the protection of personal data; and the security of networks and information systems);
- ✓ acts or omissions that harm the financial interests of the European Union;
- ✓ acts or omissions relating (Article 26(2) TFEU) to the free movement of goods, persons, services and capital within the internal market, including infringements of European Union competition rules; State aid; corporation tax;
- ✓ acts or conduct that undermine the object or purpose of European Union provisions.

In particular, it is possible to report information obtained in the course of one's work or professional activities, or during the recruitment process or at other pre- or post-contractual stages.

Reports are not admissible if they concern: disputes, claims or requests relating to a personal interest of the reporting person or of the person who has lodged a complaint with the judicial or accounting authorities, which relate exclusively to their own individual employment relationships, or which concern their employment relationships with their superiors.

The content of the report must be clear, precise and detailed. In any event, the protective measures provided for the whistleblower also apply even if the report proves to be unfounded, provided that, at the time of making the report, the person had reasonable grounds to believe that the information regarding the breaches was true and fell within the objective scope of application of the procedure.

5. CHANNELS, INTERNAL REPORTING AND MANAGEMENT OF REPORTS

Reports may be submitted in various ways:

- a. in writing, via the online channel on the La Lucente S.p.A. website;
- b. orally, through a face-to-face meeting with the Supervisory Body, to be requested by email at odv@lalucente.it.

The report must contain a detailed description of the facts and conduct considered to be in breach of the regulations, indicating, where possible, the documents, the rules deemed to have been breached and any other information useful to La Lucente S.p.A. in

conducting an investigation into the alleged facts. Furthermore, the whistleblower is obliged to declare whether they have a personal interest related to the report.

The Supervisory Body shall issue the whistleblower with an acknowledgement of receipt of the report within 7 (seven) days of the Supervisory Body receiving it.

The expected timeframe for concluding the proceedings is 3 (three) months from the date of the acknowledgement of receipt of the report or, in the absence of such an acknowledgement, 3 (three) months from the expiry of the 7 (seven)-day period following the submission of the report.

Should a member of the Supervisory Board find themselves in a position of conflict of interest when assessing the report and/or conducting the preliminary investigation, that member is obliged to recuse themselves and the report will be handled by the other members of the Supervisory Board. Where the conflict of interest concerns the SB as a whole, the SB is prohibited from proceeding with the analysis and investigation of the report. In such cases, an alternative handling procedure may be activated, whereby the report is made available to the Compliance Manager, who will manage the investigation, involving, where deemed appropriate, other departments within or outside the Company.

Any reports received in error by parties other than the Supervisory Board must be forwarded by those parties to the Supervisory Board within 7 (seven) days of receipt, whilst respecting the confidentiality of the reporting person and the content of the report, and notifying the reporting person at the same time.

This is without prejudice to the whistleblower's right, where the specific conditions laid down by law are met, to make an external report to ANAC (pursuant to Articles 6, 5 and 7, Legislative Decree No. 24/2023), to make a public disclosure (pursuant to Article 15 of Legislative Decree No. 24/2023) or to lodge a complaint with the competent judicial authority.

5.1. Reports via the online channel

In the case of a report submitted via the online channel, the whistleblower is assigned a unique identification code, to be used to check the processing status of the report submitted and the outcome of any investigation, and which ensures the confidentiality of their identity.

If the whistleblower has provided their personal details and email address when submitting the report, they will receive the report's unique identification code at the email address provided within 7 (seven) days of the Supervisory Body receiving the report.

In the case of an anonymous report, where the whistleblower's personal details and email address are not known, the whistleblower will still be able to access the system using the unique identification code assigned and monitor the status of their report.

It is the reporter's responsibility to keep the report identification code safe, as, if lost, it cannot be recovered or duplicated in any way.

All reports received by the Supervisory Body outside the online channel will be recorded on that channel by the Supervisory Body itself within 7 (seven) days of receipt, so as to enable, where possible, the issue of a unique identification code to the reporter to access the system and monitor the status of their report.

5.2. Verbal reports

The whistleblower may also make a report verbally by requesting a face-to-face meeting with the Supervisory Body.

The Supervisory Body will make itself available to hold the meeting within a reasonable timeframe of the request, either on or off the Company's premises. The arrangements and timing of the meeting will be determined in line with the objective of safeguarding the confidentiality of the whistleblower's identity and the content of the report. Any report made verbally shall be documented in minutes drawn up by the Supervisory Body. These minutes may be verified, corrected and confirmed by the reporting person by means of their signature.

For reasons of security and confidentiality, the use of video and/or audio recording systems shall be prohibited in such cases, unless the equipment used guarantees the highest standards of IT security and compliance with the GDPR.

5.3 External reporting channels

ANAC operates an external reporting channel which ensures – including through the use of encryption – the confidentiality of the identity of the whistleblower, the person involved and the person mentioned in the report, as well as the content of the report and the related documentation.

External reports may be submitted to ANAC:

a) in writing, using the dedicated online platform available on the Authority's official website (<https://www.anticorruzione.it/-/whistleblowing>);

b) orally:

- via the dedicated telephone lines;
- using the specially set up voice messaging systems;
- by requesting a face-to-face meeting with ANAC officials.

5.3.1 Conditions for making an external report to ANAC

An external report may only be submitted if, at the time of submission:

- the internal reporting channel is not active or, even if active, does not comply with the provisions of Article 4 of Legislative Decree 24/2023;
- the whistleblower has already made an internal report in accordance with this procedure and no action has been taken on it;

- the whistleblower has reasonable grounds to believe that, were they to decide to make an internal report, it would not be effectively followed up;
- the whistleblower has reasonable grounds to believe that, were they to decide to make an internal report, this would expose them to a risk of retaliation;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or clear danger to the public interest.

The ANAC Guidelines, issued by Resolution No. 311 of 12 July 2023 and amended by Resolution No. 479 of 26 November 2025, also introduce the possibility for individuals who have a qualified connection with the whistleblower, complainant or public discloser to make reports to ANAC if they suffer retaliation by reason of that connection. These include: facilitators, persons in the same working environment, work colleagues who have a regular and ongoing relationship with the whistleblower, and also legal entities where these are organisations owned by the whistleblower, complainant or public discloser, or organisations where they work, or organisations operating in the same working environment.

5.4 Public disclosure

The whistleblower may make a public disclosure and benefit from the protective measures provided for by Legislative Decree No. 24/2023, provided that, at the time of the public disclosure¹ :

- the whistleblower has previously made an internal and external report, or has made an external report directly, and has not received a response within the time limits laid down by the legislation;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;
- the whistleblower has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the particular case.

6 PROTECTION OF WHISTLEBLOWERS

Legislative Decree No. 24 of 10 March 2023 provides for specific protective measures for whistleblowers, as well as for the protection of the following additional persons:

- so-called 'facilitators', i.e. individuals who have assisted a whistleblower in the reporting process whilst working within the same workplace;
- people in the same workplace as the whistleblower who are linked to them by a stable emotional bond or kinship up to the fourth degree;
- the whistleblower's work colleagues with whom they have a regular and ongoing

¹ For the purposes of Legislative Decree No. 24/2023, 'public disclosure' means the act of making information about breaches public through the press or electronic media, or in any other way via channels capable of reaching a large number of people.

relationship;

- organisations owned by the whistleblower or for which they work, as well as organisations operating within the same workplace as the whistleblower.

The reasons that led the person to report, make a complaint or disclose information publicly are irrelevant for the purposes of their protection.

La Lucente S.p.A. recognises and endorses the protective measures provided for by Legislative Decree 24/2023, imposing sanctions on anyone who breaches them by engaging in discriminatory or retaliatory acts against whistleblowers. In particular, it should be noted that the aforementioned Legislative Decree provides for an absolute prohibition on retaliation, including, by way of example:

- a) dismissal, suspension or equivalent measures;
- b) demotion or failure to promote;
- c) a change of duties, a change of workplace, a reduction in salary, or a change to working hours;
- d) suspension from training or any restriction on access to it;
- e) negative performance appraisals or negative references;
- f) the imposition of disciplinary measures or other sanctions, including financial penalties;
- g) coercion, intimidation, harassment or ostracism;
- h) discrimination or otherwise unfavourable treatment;
- i) failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion;
- j) the non-renewal or early termination of a fixed-term employment contract;
- k) damage, including to a person's reputation, particularly on social media, or economic or financial harm, including the loss of economic opportunities and loss of income;
- l) inclusion on inappropriate lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in that sector or industry in the future;
- m) the early termination or cancellation of a contract for the supply of goods or services;
- n) the revocation of a licence or permit;
- o) a requirement to undergo psychiatric or medical examinations.

Any actions taken in breach of the prohibition on retaliation are null and void.

6.1. Guarantee of confidentiality

The confidentiality of the whistleblower's identity is always guaranteed. Under no circumstances, therefore, will the whistleblower's identity be disclosed or revealed to third parties without their prior, express and formal consent².

The following exceptions, provided for by law, are permitted:

- criminal proceedings (Article 12, paragraph 3): the identity is protected by professional secrecy pursuant to Article 329 of the Code of Criminal Procedure, without the need for consent;
- proceedings before the Court of Auditors (Article 12, paragraph 4): the identity may not be disclosed until the conclusion of the preliminary investigation;
- disciplinary proceedings (Article 12(5)): where the allegation is based on separate and additional findings to those in the report, even if arising from it, the identity may not be disclosed under any circumstances. If, on the other hand, the charge is based, in whole or in part, on the report and knowledge of the identity is essential for the defence of the accused, the report may be used for disciplinary purposes only with the express consent of the whistleblower. In the absence of consent, the report may not be used for disciplinary purposes.

In all cases where disclosure of identity is required, the whistleblower shall be notified in writing of the reasons for such disclosure.

Furthermore, during the investigation into the report, confidentiality is guaranteed regarding the identity of the person involved and the person mentioned in the report, the content of the report and the relevant supporting documentation, as well as the fact of the report itself.

Confidentiality regarding the identity of the person involved and the person mentioned, the content and the fact of the report, as well as the relevant documentation, may be waived – in whole or in part – if the report is found to be well-founded (in terms of reasonableness), including to enable the initiation of appropriate and further investigations within the context of any disciplinary, labour, civil, criminal or administrative proceedings.

Personal data processed for the purposes of managing reports must be:

- i. limited to that which is strictly and objectively necessary to verify the validity of the report and for its management;

² In cases where any disciplinary proceedings against the person implicated in the report are based entirely or predominantly on the report, the whistleblower's refusal to consent to the disclosure of their identity will render it impossible to proceed with the disciplinary proceedings.

- ii. processed lawfully and fairly.

It should be noted that personal data which is clearly not relevant to the processing of a specific report is not collected or, if collected accidentally, is deleted immediately.

Within the relevant online channel and in the dedicated section of the website, a specific privacy notice regarding the protection of personal data processed in accordance with this procedure is made available to both the whistleblower and the person subject to the report.

The processing of personal data of all data subjects involved in the reporting process is carried out by La Lucente S.p.A. in its capacity as Data Controller pursuant to Article 4(7) of the GDPR, in full compliance with current data protection legislation and the procedures adopted by the Company in this regard.

The Company has established its own procedure for managing reports, identifying appropriate technical and organisational measures to ensure a level of security commensurate with the specific risks arising from the processing carried out, based on a data protection impact assessment, and regulating its relationship with any external parties who process personal data on its behalf in accordance with Article 28 of the GDPR. The processing of personal data carried out for the purposes of this procedure is performed exclusively by staff expressly authorised to do so; failure to provide proof of identity will make it impossible to proceed with the complaint. 9 process such data in accordance with Articles 29 and 32(4) of the GDPR and Article 2-quaterdecies of the Personal Data Protection Code referred to in Legislative Decree No. 196 of 30 June 2003.

As part of the whistleblowing process, the Company provides data subjects with a specific privacy notice in accordance with Articles 13 and 14 of the GDPR, which is available on the reporting channel. The safeguards set out in this procedure are not guaranteed, and the whistleblower shall be subject to disciplinary action if – even following a first-instance judgement – they are found to be criminally liable for the offences of defamation or slander, or civilly liable on the same grounds, in cases of wilful misconduct or gross negligence.

7 EXAMINATION, COLLECTION, RETENTION AND ARCHIVING OF INFORMATION

The Supervisory Body is responsible for verifying the validity of the circumstances set out in the report; it shall carry out this task in accordance with the principles of fairness, impartiality and confidentiality, undertaking any action deemed appropriate, including the personal hearing of the whistleblower – if known – and of any other individuals who may be able to provide information on the reported facts.

The Supervisory Body examines the reports received, carrying out a preliminary investigation to verify the existence of data and information useful for establishing the details of the incident.

If the preliminary analysis does not reveal sufficiently detailed evidence or if the allegations prove to be unfounded, the report is closed.

Where sufficient and relevant evidence emerges to consider the report well-founded, the substantive investigation phase will be initiated, involving, where deemed appropriate, other departments within or outside the Company.

Upon completion of the investigation, the Supervisory Board concludes the inquiry and formalises the findings in writing, ensuring that, depending on the results, the matter is forwarded to the relevant bodies or functions for any necessary action within their remit.

The Supervisory Board retains the data and documents relating to each report for 36 months from the closure of the report, in accordance with current legislation and this procedure, subject, in any case, to judicial requirements and/or specific legal obligations that justify a longer retention period.

Personal data contained in the report will be processed in accordance with the legislation and procedures and/or privacy notices adopted and/or to be adopted by the Company regarding the protection of personal data.

8 PUBLICATION

This procedure, in accordance with the provisions of Article 5(e) of Legislative Decree 24/2023, is made available as follows:

- a) publication in a dedicated section of the company's website, from which the online reporting channel (platform) can be accessed (<https://digitalroom.bdo.it/lalucente/home.aspx>);
- b) display in paper format at company premises frequented by employees, as well as by representatives of suppliers and customers, consultants, etc.;
- c) organisation of regular training sessions aimed at explaining how the procedure works (where appropriate, with the aid of examples and practical case studies).