INDICE

Ruolo	Nome e Cognome	Firma e Data
DPO / Responsabile Whistleblowing (redazione)	Avv. Michele Bolzonello	
Titolare del Trattamento (approvazione)	Grafiche Antiga S.p.A. — Silvio Antiga	
Organismo di Vigilanza 231	Steccanella Lionello	
Responsabile IT	Andrea Toneguzzi	

1. PREMESSA E SCOPO

La presente procedura integrata ha lo scopo di disciplinare un sistema di segnalazioni di irregolarità e problemi relativi alla sicurezza delle informazioni nell'ambito dell'attività svolta da Grafiche Antiga S.p.A.

In particolare, la procedura recepisce quanto previsto dal D.Lgs. 24/2023 (Decreto Whistleblowing) — di attuazione della Direttiva (UE) 2019/1937 — che disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'ente privato.

La policy integra altresì le disposizioni in materia di sicurezza delle informazioni (NIS2 — D.Lgs. 138/2024) e di protezione dei dati personali (GDPR 2016/679), garantendo un unico canale di segnalazione per tutte le categorie di eventi rilevanti.

La policy regola tutte le fasi del processo: dall'effettuazione della segnalazione alla ricezione, all'analisi, al trattamento e alla decisione, garantendo la riservatezza del segnalante e del segnalato, nonché la loro tutela da possibili azioni ritorsive.

RISERVATEZZA L'identità del segnalante è protetta in ogni fase del processo.	**PROTEZIONE DA RITORSIONI** Chi segnala in buona fede non subirà conseguenze negative.	**CANALE DEDICATO** Un canale riservato e indipendente, accessibile H24 tramite EthicPoint.

2. RIFERIMENTI NORMATIVI

Norma	Contenuto / Rilevanza
D.Lgs. 24/2023	Decreto Whistleblowing — recepisce la Direttiva UE 2019/1937. Obbliga aziende con 50+ dipendenti a canali di segnalazione interni e tutela del segnalante.
Direttiva (UE) 2019/1937	Direttiva del Parlamento Europeo e del Consiglio del 23 ottobre 2019 sulla protezione dei segnalanti.
NIS2 — D.Lgs. 138/2024 art.21	Impone misure di gestione dei rischi di sicurezza informatica, inclusa la segnalazione degli incidenti.
GDPR (UE) 2016/679 artt. 33-34	Obbligo di notifica delle violazioni dei dati personali. La procedura interna è il primo anello della catena di risposta.
D.Lgs. 231/2001	I Modelli Organizzativi devono prevedere canali informativi verso l'OdV; i segnalanti sono tutelati da ritorsioni.
Legge 179/2017	Prima estensione del whistleblowing al settore privato italiano.
Codice Privacy (D.Lgs. 196/2003)	Come modificato dal D.Lgs. 101/2018. Disciplina il trattamento dei dati personali.
Codice Civile art. 2087	Il datore di lavoro è tenuto a proteggere l'integrità fisica e morale del lavoratore.
Statuto dei Lavoratori (L. 300/1970) art.15	Vieta atti discriminatori per l'esercizio di diritti previsti dalla legge.
Linee guida ANAC	Delibera n. 311 del 12 luglio 2023 sulla protezione delle persone che segnalano violazioni.

3. DEFINIZIONI

Violazioni	Comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente privato.
Segnalante (Whistleblower)	La persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.
Segnalazione interna	La comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interno (piattaforma EthicPoint).
Segnalazione esterna	La comunicazione presentata tramite il canale esterno messo a disposizione dall'ANAC.
Segnalazione anonima	Segnalazione non contenente dettagli che consentano l'identificazione del segnalante.
Facilitatore	Persona fisica che assiste il segnalante nel processo di segnalazione, operante nel medesimo contesto lavorativo.
Destinatario della segnalazione	Responsabile esterno (Avv. Michele Bolzonello / DPO) deputato a ricevere la segnalazione, con assoluto obbligo di riservatezza.
Persona coinvolta / Segnalato	La persona fisica o giuridica menzionata nella segnalazione come autore della violazione.
Ritorsione	Qualsiasi comportamento, atto od omissione posto in essere a causa della segnalazione e che causa un danno ingiusto al segnalante.
Contesto lavorativo	Attività lavorative o professionali, presenti o passate, attraverso le quali una persona acquisisce informazioni sulle violazioni.
Ricevente	Soggetto interno che riceve la segnalazione e la elabora nel rispetto delle cautele definite dalla presente procedura.
DPO	Data Protection Officer — responsabile della protezione dei dati personali e gestore del canale EthicPoint per la sicurezza delle informazioni.

4. DESTINATARI DELLA PROCEDURA

La presente procedura si applica a tutte le persone che segnalano, denunciano all'Autorità giudiziaria o contabile, o divulgano pubblicamente informazioni sulle violazioni di cui sono venute a conoscenza nell'ambito del proprio contesto lavorativo, e in particolare:

A CHI SI APPLICA QUESTA PROCEDURA

- Dipendenti a tempo indeterminato e determinato, apprendisti, lavoratori autonomi e titolari di rapporto di collaborazione con la Società
- Liberi professionisti e consulenti
- Volontari e tirocinanti, retribuiti e non retribuiti
- Eventuali azionisti (persone fisiche) e persone con funzione di amministrazione, direzione, controllo, vigilanza o rappresentanza
- Appaltatori e fornitori
- Clienti e visitatori che vengano a conoscenza di problemi relativi alla sicurezza delle informazioni

5. AMBITO DI APPLICAZIONE — COSA SI PUÒ SEGNALARE

Possono essere segnalate violazioni che ledono l'interesse pubblico o l'integrità dell'ente, nonché tutti i problemi, i rischi e le violazioni relativi alla sicurezza delle informazioni trattate da Grafiche Antiga S.p.A.

5.1 Violazioni whistleblowing

- Condotte illecite rilevanti per la disciplina legge 231/2001
- Violazioni del Modello 231 di organizzazione e gestione
- Reati presupposto per l'applicazione del D.lgs. 231/2001
- Corruzione e frode
- Appropriazione indebita e furto
- Riciclaggio di denaro
- Discriminazione, molestie, mobbing
- Violazioni fiscali e antitrust
- Rivelazione di segreti aziendali
- Condotte volte ad occultare violazioni già commesse o future (con elementi concreti)
- Qualsiasi violazione del codice etico, dei regolamenti aziendali e codice condotta fornitori

5.2 violazioni relative alla sicurezza delle informazioni

Sicurezza IT e dati	Informazioni commerciali e fisiche
• Accesso non autorizzato a sistemi o file • Violazione o sospetta violazione di dati personali (breach) • Attacco informatico in corso (phishing, ransomware, malware) • Credenziali condivise o password deboli	• Divulgazione non autorizzata di file clienti, offerte o contratti • Furto o smarrimento di documenti riservati cartacei • Accesso fisico non autorizzato a zone riservate

• Software non autorizzato su PC aziendali • Perdita o furto di dispositivo aziendale • Mancata applicazione di aggiornamenti critici	• Comportamento sospetto di colleghi, fornitori o visitatori • Scarti di stampa con dati personali non distrutti correttamente • Invio erroneo di file riservati a destinatari non autorizzati

5.3 Cosa NON si può segnalare

- Contestazioni o rivendicazioni legate esclusivamente a interessi personali del segnalante (vertenze di lavoro, conflitti interpersonali tra colleghi)
- Violazioni già disciplinate in via obbligatoria da atti dell'Unione europea con proprie procedure di segnalazione
- Violazioni in materia di sicurezza nazionale o appalti di difesa (salvo rientro nel diritto UE derivato)
- Segnalazioni di natura esclusivamente personale (es. richieste salariali) — per le quali si applicano le procedure HR ordinarie

NOTA: Non è necessario avere la certezza che si tratti di una violazione: è sufficiente un ragionevole sospetto fondato in buona fede. Una segnalazione in buona fede, anche se poi risultasse infondata, non comporta alcuna conseguenza per il segnalante.

6. CANALE DI SEGNALAZIONE DEDICATO (EthicPoint)

Grafiche Antiga S.p.A. ha istituito un unico canale di segnalazione dedicato, separato dai normali flussi aziendali e gestito in modo indipendente, accessibile 24 ore su 24, 7 giorni su 7.

CANALE UFFICIALE DI SEGNALAZIONE
www.graficheantiga.it › Sezione: Segnalazioni — EthicPoint
Link diretto: https://ethicpoint.eu/grafiche-antiga/
Accessibile H24 · Anonimato tecnico garantito · Gestito da soggetto terzo indipendente · Crittografia end-to-end

GARANZIA TECNICA: Il portale EthicPoint è gestito da un soggetto terzo indipendente, certificato ai sensi del D.Lgs. 24/2023. Nessun dipendente, manager o membro della Direzione di Grafiche Antiga S.p.A. ha accesso alle segnalazioni prima che il Responsabile esterno le abbia valutate. Le comunicazioni sono cifrate end-to-end e consentono la messaggistica anonima bidirezionale.

6.1 Modalità di segnalazione

Modalità	Come accedere	Note
Portale EthicPoint (canale principale)	www.graficheantiga.it → Segnalazioni — EthicPoint. Disponibile H24, 7 giorni su 7.	Canale primario. Anonimato tecnico completo. Messaggistica cifrata bidirezionale.
Segnalazione orale	Tramite la stessa piattaforma EthicPoint (funzione audio) oppure richiesta di incontro con il Responsabile esterno.	Il responsabile provvede alla trascrizione garantendo la riservatezza.

7. COME EFFETTUARE UNA SEGNALAZIONE — ELEMENTI NECESSARI

È necessario che la segnalazione sia il più possibile circostanziata per consentire la valutazione dei fatti da parte dei soggetti competenti. La segnalazione può essere effettuata in modo nominale o in forma anonima: in entrambi i casi vengono garantite le stesse tutele.

7.1 Processo di segnalazione (5 fasi)

1 — RILEVA	2 — RACCOGLI	3 — SEGNALA	4 — CONFERMA	5 — ESITO
Noti o sospetti un problema	Annota data, ora, luogo. Conserva eventuali prove	Accedi a www.graficheantiga.it → EthicPoint	Entro 7 giorni lavorativi ricevi conferma e codice univoco	Entro 3 mesi ricevi informazioni sull'esito

7.2 Informazioni da includere nella segnalazione

Informazione	Dettaglio / Esempio
Circostanze di tempo e luogo	Es. «Ho notato l'anomalia martedì 15 aprile 2025 verso le 10:30»
Descrizione del fatto	Cosa è successo, cosa è stato visto o sentito, perché desta preoccupazione; modalità con cui se ne è venuti a conoscenza
Sistemi, documenti o aree coinvolte	Es. «File in cartella 'Commesse 2025' sul server», «PC postazione pre-stampa 3»
Identità del soggetto cui attribuire i fatti (se nota)	Generalità o elementi che consentano l'identificazione; ruolo ricoperto
Eventuali testimoni	Generalità, ruolo o altri elementi di altri soggetti che possano riferire sui fatti
Prove disponibili	Screenshot, email, documento fisico, log — allegare se possibile
Se i fatti sono stati riferiti da terzi	Indicare se appresi in prima persona o riferiti al segnalante da altri

Se già segnalati altrove	Indicare se i fatti sono stati trasmessi anche ad altre funzioni aziendali o autorità pubbliche
Dati del segnalante (opzionale)	Nome, cognome, ruolo, recapito. Non obbligatorio in caso di segnalazione anonima

Il codice identificativo univoco ricevuto al termine della registrazione consente di: verificare lo stato di avanzamento della segnalazione, dialogare con il soggetto ricevente, e integrare la segnalazione con ulteriori elementi. È importante conservarlo: in caso di smarrimento non può essere recuperato o duplicato.

8. GESTIONE DELLA SEGNALAZIONE INTERNA

Il soggetto incaricato delle procedure competenti a ricevere e a dare seguito alla segnalazione è l'Avv. Michele Bolzonello in qualità di Responsabile esterno per il whistleblowing / DPO.

Chi gestisce le segnalazioni è tenuto al rispetto delle seguenti indicazioni del legislatore:

- Rilascia alla persona segnalante un avviso di ricevimento entro 7 giorni dalla data di ricezione
- Mantiene le interlocuzioni con la persona segnalante
- Dà corretto seguito alle segnalazioni ricevute
- Fornisce un riscontro alla persona segnalante entro 3 mesi

8.1 Fasi del processo di gestione

Fase	Entro	Azioni
1 — Ricezione	Immediato	La segnalazione viene registrata nel Registro con numero di protocollo progressivo, data e ora di ricezione.
2 — Conferma	7 gg lavorativi	Avviso di ricevimento al segnalante (se identificabile) con il numero di protocollo assegnato.
3 — Valutazione ammissibilità	90 giorni	Valutazione della sussistenza dei requisiti essenziali: qualifica del segnalante, interesse all'integrità della Società, illiceità della condotta segnalata.
4 — Indagine / Verifica fondatezza	90 giorni	Il destinatario, con eventuale supporto dell'OdV e del Responsabile IT, conduce attività di verifica nel rispetto dei principi di imparzialità e riservatezza.
5 — Esito	3 mesi	Il destinatario comunica l'esito al segnalante nei limiti consentiti dalla riservatezza. In caso di violazione confermata, attiva le procedure disciplinari.
6 — Archiviazione	5 anni	Il fascicolo viene archiviato nel Registro separato per 5 anni dalla chiusura, poi distrutto/anonimizzato con procedura certificata.

URGENZA: In caso di situazione urgente (es. attacco informatico in corso, violazione attiva di dati personali), il DPO attiva la risposta immediata entro 2 ore dalla ricezione della segnalazione, indipendentemente dal completamento delle formalità.

9. GARANZIE DI RISERVATEZZA E TRATTAMENTO DEI DATI

Ogni trattamento dei dati personali è effettuato nel rispetto degli obblighi di riservatezza di cui all'art. 12 del D.Lgs. 24/2023 e in conformità al GDPR (UE) 2016/679. La tutela è assicurata al Segnalante, al Facilitatore e alla Persona coinvolta.

#	Garanzia	Descrizione
1	**Accesso riservato**	Le segnalazioni sono accessibili esclusivamente al DPO esterno e, se necessario, all'OdV. Nessun responsabile di reparto o manager HR ha accesso diretto prima della valutazione preliminare.
2	**Anonimato garantito**	Il segnalante può scegliere di non indicare le proprie generalità. Il DPO non compie alcun tentativo di risalire all'identità del segnalante anonimo.
3	**Divieto di divulgazione**	L'identità del segnalante non può essere rivelata a terzi senza esplicito consenso scritto, salvo obbligo di legge. Anche in tal caso il segnalante viene informato, ove possibile.
4	**Conservazione dei dati**	La documentazione è conservata per non più di 5 anni dalla data di comunicazione dell'esito finale. I dati non utili sono cancellati tempestivamente.
5	**Separazione degli archivi**	Le segnalazioni sono archiviate in un registro separato da qualsiasi altro archivio aziendale. L'accesso è protetto da credenziali dedicate note solo al DPO.
6	**Diritti dell'interessato (segnalato)**	La persona segnalata non può esercitare i diritti GDPR (accesso, rettifica, cancellazione) in quanto ciò potrebbe pregiudicare la tutela della riservatezza del segnalante.

10. MISURE DI PROTEZIONE E TUTELA DEL SEGNALANTE

Il Decreto Whistleblowing prevede le seguenti misure di protezione nei confronti del Segnalante e dei Soggetti Collegati:

- Divieto di ritorsione in ragione di una segnalazione
- Misure di sostegno: informazioni, assistenza e consulenza gratuita da parte di enti del terzo settore (elenco disponibile sul sito ANAC)
- Protezione dalle ritorsioni: possibilità di comunicare all'ANAC le ritorsioni subite; nullità degli atti assunti in violazione del divieto di ritorsione
- Limitazioni di responsabilità in caso di rivelazione di violazioni coperte da obbligo di segreto, se vi erano fondati motivi che la rivelazione fosse necessaria
- Limitazioni di responsabilità per l'acquisizione o l'accesso alle informazioni sulle violazioni (salvo reato)
- Sanzioni a carico di chi attua ritorsioni

Le tutele si applicano a:

- La persona Segnalante
- Il Facilitatore
- Persone del medesimo contesto lavorativo legate al segnalante da stabile legame affettivo o di parentela entro il quarto grado

- Colleghi di lavoro con rapporto abituale e corrente con il segnalante
- Enti di proprietà del segnalante o per i quali le stesse persone lavorano

11. PROTEZIONE DA RITORSIONI

DIVIETO ASSOLUTO DI RITORSIONI — ART. 17 D.LGS. 24/2023: Grafiche Antiga S.p.A. vieta categoricamente qualsiasi forma di ritorsione nei confronti di chi effettua una segnalazione in buona fede. La violazione di questo divieto costituisce illecito disciplinare e può determinare responsabilità civile e penale.

11.1 Comportamenti vietati (ritorsioni)

Ritorsioni dirette	Ritorsioni indirette
• Licenziamento, anche mascherato da riorganizzazione • Sospensione, messa in disponibilità o riduzione dell'orario • Retrocessione o mancata promozione ingiustificata • Sanzione disciplinare ingiustificata o eccessiva • Trasferimento forzato o cambiamento di sede non concordato • Mancato rinnovo del contratto a termine	• Esclusione da riunioni, gruppi di lavoro o comunicazioni • Assegnazione di mansioni dequalificanti o umilianti • Isolamento sociale o professionale • Commenti denigratori sul luogo di lavoro o sui social • Segnalazione falsa o strumentale a carico del segnalante • Pressioni psicologiche per far ritirare la segnalazione

11.2 Tutele del segnalante in caso di ritorsione

	Tutela	Descrizione
A	**Segnalazione al DPO**	Il segnalante può riferire la ritorsione direttamente al DPO tramite il canale EthicPoint.
B	**Segnalazione all'ANAC**	Tramite whistleblowing.anticorruzione.it. L'ANAC può irrogare sanzioni fino a 50.000 €.
C	**Tutela giurisdizionale**	Il segnalante può ricorrere al Giudice del Lavoro. L'onere della prova che l'atto non è ritorsivo grava sull'azienda (art.17 co.8 D.Lgs. 24/2023).
D	**Sospensione del provvedimento ritorsivo**	Il giudice può sospendere il provvedimento in via cautelare con ripristino immediato del segnalante.
E	**Risarcimento del danno**	Il segnalante ha diritto al risarcimento integrale dei danni patrimoniali e non patrimoniali subiti.

12. POSSIBILITÀ DI ANONIMATO

Le segnalazioni anonime, effettuate senza identificazione del whistleblower, vengono prese in considerazione purché adeguatamente circostanziate e corredate da elementi sufficienti a permettere un'adeguata attività di indagine. Il segnalante anonimo successivamente identificato che abbia comunicato di aver subito ritorsioni può beneficiare delle tutele previste dal decreto.

Il portale EthicPoint garantisce l'anonimato tecnico completo. L'inserimento dei dati personali non è obbligatorio e può avvenire anche in fase successiva, riprendendo la segnalazione tramite il codice identificativo univoco assegnato.

13. RESPONSABILITÀ DEL WHISTLEBLOWER

La presente policy lascia impregiudicata la responsabilità penale e disciplinare del whistleblower nell'ipotesi di segnalazione calunniosa o diffamatoria. Le tutele NON sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale per i reati di diffamazione o calunnia o la responsabilità civile per dolo o colpa grave.

Sono altresì fonte di responsabilità disciplinare le segnalazioni manifestamente opportunistiche o effettuate al solo scopo di danneggiare terzi, nonché ogni utilizzo improprio o intenzionale strumentalizzazione dell'istituto.

14. TUTELA DEL SEGNALATO

Al fine di evitare conseguenze pregiudizievoli anche solo di carattere reputazionale, la tutela riservata al Segnalante va accordata anche al Segnalato, con particolare riguardo nella fase di inoltro della segnalazione a terzi. Ogni relazione istruttoria assicura che la documentazione non contenga riferimenti all'identità del Segnalato in modo da proteggerlo da conseguenze premature.

15. CANALI DI SEGNALAZIONE ESTERNI

Indipendentemente dalla presente procedura interna, qualsiasi soggetto ha sempre il diritto di rivolgersi direttamente agli organi di controllo e alle autorità competenti.

Autorità / Organo	Competenza	Contatto / Portale
Garante per la Protezione dei Dati Personali (GPDP)	Violazioni GDPR, trattamento illecito di dati personali	www.garanteprivacy.it — servizi.gpdp.it
Autorità Nazionale Anticorruzione (ANAC)	Segnalazioni whistleblowing e ritorsioni subite	whistleblowing.anticorruzione.it
Agenzia per la Cybersicurezza Nazionale (ACN)	Incidenti di sicurezza informatica NIS2	www.acn.gov.it — csirt.gov.it
Polizia Postale e delle Comunicazioni	Reati informatici, accessi abusivi, frodi informatiche	www.commissariatodips.it

Ispettorato Nazionale del Lavoro (INL)	Ritorsioni lavorative, discriminazioni, violazioni D.Lgs. 24/2023	www.ispettorato.gov.it

16. SANZIONI PER ABUSO E PER RITORSIONI

Segnalazioni in malafede o false	Ritorsioni verso il segnalante
• Procedimento disciplinare fino al licenziamento • Responsabilità civile per i danni causati alle persone falsamente accusate • Eventuale responsabilità penale (calunnia, diffamazione — artt. 368, 595 c.p.) *Nota: la segnalazione in buona fede risultata infondata non costituisce malafede.*	• Procedimento disciplinare fino al licenziamento per giusta causa • Sanzione amministrativa ANAC da 10.000 a 50.000 € (art.21 D.Lgs. 24/2023) • Risarcimento integrale dei danni al segnalante • Eventuale responsabilità penale (mobbing, abuso d'ufficio)

17. COMUNICAZIONE E FORMAZIONE

Grafiche Antiga S.p.A. si impegna a garantire che la presente procedura sia effettivamente conosciuta e accessibile a tutte le parti interessate:

- La procedura è pubblicata sul portale intranet aziendale in sezione accessibile a tutti i dipendenti
- Una sintesi (Informativa Breve — Allegato A) è affissa nelle bacheche di reparto (pre-stampa, stampa, finishing, uffici amministrativi)
- In sede di assunzione, ogni nuovo dipendente riceve copia della procedura e firma per presa visione
- Formazione specifica inclusa nel piano di formazione annuale sulla sicurezza
- I fornitori e collaboratori esterni ricevono la procedura al momento della firma del contratto / NDA
- Il DPO è disponibile a sessioni informative su richiesta di qualsiasi reparto o gruppo di dipendenti

17.1 Revisione e aggiornamento

Evento	Azione
Ogni 12 mesi	Revisione ordinaria della procedura da parte del DPO con approvazione della Direzione
Dopo ogni segnalazione gestita	Verifica dell'efficacia del processo; eventuale aggiornamento dei tempi o delle modalità operative
Variazioni normative	Aggiornamento entro 30 giorni dall'entrata in vigore di nuove norme rilevanti (GDPR, NIS2, D.Lgs. 24/2023)
Cambiamenti organizzativi rilevanti	Cambio DPO, cambio OdV, fusioni, acquisizioni, apertura nuove sedi

18. ALLEGATO 1 — MODALITÀ OPERATIVE

Fase 1: Invio di una Segnalazione e relativa registrazione

La segnalazione deve essere effettuata attraverso il canale di segnalazione indicato. All'atto della ricezione, il Destinatario provvede ad attribuire un numero identificativo progressivo e ad alimentare il Registro delle Segnalazioni contenente almeno i seguenti campi:

- Protocollo identificativo
- Data di ricezione
- Canale di ricezione della segnalazione
- Esito della fase di valutazione sull'ammissibilità
- Esito della fase di valutazione della fondatezza
- Condivisione delle risultanze
- Conclusione

Fase 2: Valutazione dell'ammissibilità della Segnalazione

Una volta ricevuta la segnalazione, il destinatario ha a disposizione 90 giorni per valutarne l'ammissibilità verificando la sussistenza dei seguenti requisiti:

- Il segnalante è tra i destinatari del whistleblowing così come identificati dalla norma
- Vi è l'interesse all'integrità della Società
- La condotta segnalata rappresenta un illecito così come specificato nella procedura

Qualora uno dei requisiti non sussista il Destinatario procede in base alle previsioni normative: cancellazione della segnalazione dal sistema o comunicazione all'Autorità Giudiziaria ove applicabile.

Fase 3: Valutazione della fondatezza della Segnalazione

Dichiarata l'ammissibilità, il destinatario avvia un'attività di verifica e analisi per valutarne la fondatezza nel rispetto dei principi di imparzialità e riservatezza, inclusa l'audizione del segnalante e di eventuali altri soggetti, con termine di 90 giorni dall'avvio dell'istruttoria.

Se la segnalazione non risulta fondata, il destinatario procede con l'archiviazione motivata. Se risulta fondata, trasmette la relazione di risultanze istruttorie all'OdV e/o agli organi preposti, assicurandosi che la documentazione non contenga riferimenti identificativi del segnalante o del segnalato.

Fase 4: Condivisione delle risultanze

Il destinatario è costantemente informato di tutte le attività svolte dagli organi preposti. Sarà redatta una relazione finale sulle risultanze, sulle carenze riscontrate e sulle azioni di miglioramento, trasmessa alla Società per l'attivazione di eventuali provvedimenti disciplinari.

Fase 5: Tenuta dei dati contenuti nella Segnalazione

La segnalazione e la relativa documentazione è archiviata per 12 mesi dalla ricezione, salvo l'instaurazione di un'azione giudiziaria o disciplinare nei confronti del denunciato o del denunciante. In tal caso la documentazione è conservata fino alla conclusione del procedimento. Trascorsi i termini, la segnalazione

sarà cancellata o anonimizzata. (La conservazione complessiva massima è di 5 anni dall'esito finale della segnalazione ai sensi del D.Lgs. 24/2023.)

19. ALLEGATO 2 — INFORMATIVA BREVE (da affiggere in bacheca)

Il testo seguente è destinato alla pubblicazione nelle bacheche di reparto in formato A4 o A3.

GRAFICHE ANTIGA S.P.A.

HAI NOTATO UN PROBLEMA DI SICUREZZA?

Accesso non autorizzato · Email errata · File riservato esposto · Dispositivo smarrito · Comportamento sospetto · Qualsiasi rischio per le informazioni aziendali

SEGNALALO IN MODO SICURO E RISERVATO

www.graficheantiga.it

Sezione: Segnalazioni — EthicPoint

Riservatezza garantita · Nessuna ritorsione · Anonimato possibile

Procedura SEG-SI-001 / PGQ 83-2 — D.Lgs. 24/2023 · NIS2 · GDPR