

CODICE ETICO E DI CONDOTTA

Policy Aziendale – Consulenza finanziaria per agevolazioni

Documento	Codice Etico e di Condotta – Policy Aziendale
Società	Creditalia Progetti per l'Impresa Srl
Ambito	Consulenza finanziaria per agevolazioni (incentivi finanziari e fiscali) e relazioni con Clienti, Partner, PA, Ministeri, Regioni, Soggetti gestori
Versione	1.0
Data	03/01/2025

Registro revisioni

Versione	Data	Descrizione modifiche	Approvazione
1.0	25/02/2026	Prima emissione (policy estesa).	Direzione

Sommario

Registro revisioni	1
1. Premessa e finalità	3
2. Ambito di applicazione e destinatari	3
3. Definizioni (Glossario)	3
4. Principi generali	4
5. Rapporti con i Clienti (dalla fattibilità alla rendicontazione)	4
6. Rapporti con Pubblica Amministrazione, Ministeri, Regioni e Soggetti gestori	5
7. Conflitti di interesse	5
8. Integrità documentale, dichiarazioni e autocertificazioni	5
9. Gestione delle anomalie (Stop & Escalation)	6
10. Anticorruzione, omaggi, ospitalità e spese	6
11. Riservatezza, privacy e sicurezza delle informazioni	7
12. Segnalazioni (whistleblowing) e protezione del segnalante	7
13. Attuazione, formazione, controlli e aggiornamento	7
Allegato A – Checklist minima di conformità (per pratica agevolata)	8
Allegato B – Schema “Stop & Escalation” (testo operativo)	8
Allegato C – Regole su omaggi, ospitalità e spese (sintesi)	8
Allegato D – “Do & Don’t” (una pagina)	8

1. Premessa e finalità

Creditalia Progetti per l'Impresa Srl (di seguito Creditalia) opera nella consulenza e assistenza finanziaria per l'accesso ad agevolazioni finanziarie e fiscali, supportando imprese e altri soggetti nella predisposizione, presentazione, gestione e rendicontazione di domande e progetti, e nel dialogo con Enti pubblici, Soggetti gestori, Ministeri e Regioni.

Questa Policy (Codice Etico e di Condotta) definisce i principi e i comportamenti attesi, nonché le condotte vietate o sconsigliate, con l'obiettivo di:

- (i) garantire legalità e integrità;
- (ii) assicurare qualità e tracciabilità documentale;
- (iii) tutelare clienti e stakeholder;
- (iv) preservare la reputazione di Creditalia e la correttezza dei procedimenti amministrativi.

2. Ambito di applicazione e destinatari

La presente Policy si applica a: Amministratori, Dipendenti, Consulenti, Collaboratori, Tecnici convenzionati, Partner e chiunque operi per conto di Creditalia o nell'ambito di iniziative in co-branding/white-label. È parte integrante delle regole di condotta verso Clienti, Pubblica Amministrazione e Soggetti Terzi.

3. Definizioni (Glossario)

Termine	Definizione
Cliente/Mandante	Impresa o Soggetto che conferisce mandato a Creditalia per servizi di consulenza/assistenza.
Ente concedente / Soggetto gestore	Amministrazione o Società incaricata della gestione della misura/bando e delle erogazioni.
PA	Pubblica Amministrazione (Ministeri, Regioni, Enti strumentali, ecc.).
Agevolazione	Contributo, Finanziamento agevolato, Credito d'imposta o altra misura di sostegno pubblico.
SAL	Stato di Avanzamento Lavori/Spesa (richiesta di erogazione intermedia) e Saldo finale.
Delega	Atto che autorizza Creditalia a richiedere e ricevere informazioni/documenti presso enti terzi per conto del cliente.
Anomalia interna	Evento/omissione/informazione non coerente, potenzialmente impattante su ammissibilità, tempi, erogazione, responsabilità o reputazione.

4. Principi generali

Legalità: Rispetto di leggi, regolamenti e regole di bando; divieto di scorciatoie o rappresentazioni non veritiere.

Integrità e correttezza: Onestà e lealtà nei rapporti con Clienti, Partner e PA; tolleranza zero verso condotte improprie.

Trasparenza: Informazioni chiare su condizioni, vincoli, rischi, tempi e probabilità; distinzione tra fatti e interpretazioni.

Competenza e diligenza: Aggiornamento continuo; cura della qualità tecnica e documentale; controlli incrociati sulle attività critiche.

Responsabilità e tracciabilità: Decisioni e comunicazioni tracciate; gestione documentale ordinata; conservazione secondo requisiti applicabili.

Riservatezza e protezione dati: Trattamento dei dati nel rispetto del GDPR; minimizzazione e sicurezza dei flussi informativi.

5. Rapporti con i Clienti (dalla fattibilità alla rendicontazione)

Comportamenti da tenere

- Formalizzare incarico, perimetro e responsabilità del Cliente (veridicità dati, tempi, pagamenti).
- Informare su obblighi tipici: tracciabilità pagamenti, documenti quietanzati, conservazione e controlli.
- Gestire in modo proattivo scadenze e richieste integrazioni; segnalare tempestivamente inerzie o mancanze.
- Evitare promesse: presentare scenari, vincoli e rischi in modo realistico e documentato.

Vietato o sconsigliato

- Garantire l'esito della domanda o promettere "corsie preferenziali".
- Presentare documenti o dichiarazioni senza verifiche minime di coerenza, completezza e tracciabilità.
- Suggestire alterazioni, omissioni o rappresentazioni non veritiere di spese, tempi o requisiti.

6. Rapporti con Pubblica Amministrazione, Ministeri, Regioni e Soggetti gestori

Comportamenti da tenere

- Utilizzare canali formali e tracciabili (PEC, protocolli, piattaforme) e conservare evidenze di invii e riscontri.
- Rispondere in modo completo e puntuale alle richieste di integrazione documentale entro i termini previsti.
- Mantenere comunicazioni rispettose, collaborative e basate su dati verificabili; prevenire conflitti e contenziosi.
- Gestire SAL (stato avanzamento lavori) con disciplina documentale (quietanze, estratti conto, report tecnici, allegati richiesti).

Vietato o sconsigliato

- Esercitare pressioni indebite o aggirare i canali ufficiali.
- Trasmettere informazioni non verificate o presentate in modo fuorviante.
- Offrire o promettere utilità, favori, regali o ospitalità salvo quelli “d’uso” di modico valore e occasionali ai sensi del DPR 62/2013, art. 4

7. Conflitti di interesse

Comportamenti da tenere

- Dichiarare tempestivamente conflitti reali o potenziali (rapporti economici, parentela, partecipazioni, incarichi).
- Astenersi da decisioni operative quando il conflitto non è gestibile; richiedere riassegnazione/secondo controllo.

Vietato o sconsigliato

- Orientare scelte tecniche per vantaggi personali o di terzi.
- Omettere informazioni che possano incidere su imparzialità e credibilità.

8. Integrità documentale, dichiarazioni e autocertificazioni

Comportamenti da tenere

- Mantenere coerenza tra fatti, evidenze contabili e documenti trasmessi; gestire versioni e aggiornamenti.
- Verificare requisiti “sensibili” (ammissibilità, cumulo, intensità, vincoli temporali) e documentare le fonti.

- In caso di dubbio sostanziale, applicare stop operativo e chiedere parere al RRSS (Responsabile di Servizio).

Vietato o sconsigliato

- Alterare date, importi, descrizioni o contenuti per rientrare nei requisiti.
- Produrre o utilizzare autocertificazioni non veritiere o non supportate da evidenze.

9. Gestione delle anomalie (Stop & Escalation)

Comportamenti da tenere

- Segnalare tempestivamente anomalie a IC (Istruttore Creditalia)/CC (Consulente Creditalia) e, se necessario, al RRSS con evidenze disponibili.
- Sospendere invii o attività critiche finché l'anomalia non è chiarita e risolta con decisione tracciata.
- Mantenere comunicazioni allineate verso il Cliente per evitare disallineamenti informativi.

Vietato o sconsigliato

- Ignorare segnali di incoerenza o “forzare” la prosecuzione per rispettare scadenze.
- Gestire autonomamente comunicazioni critiche senza coordinamento interno.

10. Anticorruzione, omaggi, ospitalità e spese

Comportamenti da tenere

- Accettare omaggi solo se modesti e non collegati a decisioni/istruttorie, in caso di dubbio, rifiutare e segnalare.
- Per gli RRSS, selezionare Partner/Consulenti/Tecnici con criteri trasparenti e contratti chiari (scopo, privacy, qualità, tempi).

Vietato o sconsigliato

- Accettare compensi per velocizzare una pratica, rimborsi fittizi, pagamenti indiretti impropri tramite terze parti.
- Effettuare regali, utilità o promesse a Soggetti pubblici o privati per ottenere vantaggi.

11. Riservatezza, privacy e sicurezza delle informazioni

Comportamenti da tenere

- Trattare i dati nel rispetto dei principi GDPR (minimizzazione, finalità, integrità e riservatezza).
- Condividere informazioni solo se necessario al lavoro e tramite canali aziendali autorizzati.
- Usare Archivio e sistemi aziendali per archiviazione e *versioning*; proteggere credenziali e accessi.

Vietato o sconsigliato

- Inviare documenti sensibili su canali non autorizzati o a destinatari errati.
- Conservare copie locali non protette quando previsto repository centrale.

12. Segnalazioni e protezione del segnalante

Comportamenti da tenere

- Segnalare violazioni o irregolarità con tempestività e in modo documentato.
- Tutelare la riservatezza del Segnalante con divieto di ritorsione, secondo la normativa applicabile.

Vietato o sconsigliato

- Non segnalare con tempestività violazioni o irregolarità di cui si viene a conoscenza.
- Ritorsioni o ostracismo verso chi segnala in buona fede.
- Ostruzione delle verifiche interne o distruzione/alterazione di evidenze.

13. Attuazione, formazione, controlli e aggiornamento

Comportamenti da tenere

- Diffusione del Codice ETICO a tutti i destinatari e inserimento nei contratti/accordi rilevanti.
- Formazione periodica su comportamenti, rischi e casi pratici; aggiornamento in caso di novità normative o operative.
- Controlli interni su aree sensibili (documentazione, rendicontazione, comunicazioni con PA, privacy).

Vietato o sconsigliato

- Considerare il Codice ETICO un documento “formale” senza applicazione concreta.

Allegato A – Checklist minima di conformità (per pratica agevolata)

1. Incarico/Mandato firmato e deleghe verso Enti/Soggetti gestori acquisite e archiviate.
2. Anagrafica cliente e dati di base completi; documentazione societaria aggiornata ove richiesta.
3. Perimetro costi e cronoprogramma coerenti con requisiti della misura; vincoli comunicati al cliente.
4. Tracciabilità pagamenti predisposta (conto dedicato/estratti conto/bonifici) ove necessario.
5. Controllo documenti: bozze, revisioni, approvazioni interne, invii e ricevute conservati.
6. Verifica requisiti sensibili (ammissibilità, cumulo, intensità aiuto, vincoli temporali, impresa in difficoltà se rilevante).
7. Piano rendicontazione: SAL/saldo con elenco documenti richiesti e responsabilità assegnate.
8. Gestione anomalie: registro anomalie e decisioni; escalation effettuate quando necessario.
9. Privacy: canali di scambio autorizzati, minimizzazione dati, accessi controllati.

Allegato B – Schema “Stop & Escalation” (testo operativo)

10. Rilevazione: l'operatore identifica un'anomalia (documentale, contabile, temporale, dichiarativa, o di condotta).
11. Blocco: sospensione invio/attività critica correlata all'anomalia.
12. Segnalazione: invio report sintetico con evidenze a IC/CC; se impatto elevato o trasversale, coinvolgere RS/Direzione.
13. Valutazione: analisi congiunta e decisione tracciata (correzione, integrazione, rinuncia, richiesta, parere specialistico).
14. Comunicazione: messaggio univoco al Cliente e, se applicabile, all'Ente, gestito in coordinamento interno.
15. Chiusura: registrazione esito e aggiornamento fascicolo/archivio digitale centralizzato.

Allegato C – Regole su omaggi, ospitalità e spese (sintesi)

- Divieto assoluto di utilità improprie verso PA/Soggetti Gestori; nessuna promessa o vantaggio in cambio di decisioni.
- Omaggi: consentiti solo simbolici e non correlati a istruttorie; in dubbio, rifiutare e segnalare.
- Ospitalità/spese: ammesse solo se giustificate, proporzionate, documentate e autorizzate secondo regole interne.
- Terze parti: vietato usare Consulenti/Partner per veicolare pagamenti impropri o “favori”.

Allegato D – “Do & Don't” (una pagina)

DO (sempre)

- Tracciare ogni invio e conservare evidenze (PEC/protocolli/receipts).

- Documentare fonti e versioni; usare repository e workflow aziendali.
- Bloccare informazioni false o incoerenti.
- Spiegare al Cliente vincoli, rischi e responsabilità (senza promesse).

DON'T (mai)

- Non garantire esiti o promuovere scorciatoie.
- Non alterare documenti, date o contenuti; non accettare mai autocertificazioni non veritiere.
- Non offrire regali o utilità a Soggetti pubblici o privati per vantaggi.
- Non condividere dati sensibili fuori dai canali autorizzati.