

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO EX D. LGS. 231/2001 DI

Parte Speciale I:

Delitti in materia di strumenti di pagamento diversi
dai contanti e trasferimento fraudolento di valori
ex art. 25 octies.1 D. Lgs. 231/2001

ESI S.p.A.

Tabella 1 - Riepilogo modifiche ed aggiornamenti

Versione	Approvato da	Motivo aggiornamento	Data validità
1.00	Consiglio di Amministrazione	Prima emissione	5 agosto 2024



Esi S.p.A.

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Parte Speciale I: Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori ex art. 25 octies.1 D. Lgs. 231/2001

INDICE DEI CONTENUTI

1.	DEFINIZIONI.....	3
2.	PREMESSA.....	5
3.	LE FATTISPECIE DI DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 25-OCTIES.1 DEL DECRETO).....	6
4.	PROCESSI SENSIBILI	7
5.	PRINCIPI GENERALI DI CONDOTTA E COMPORTAMENTO E DI ASSETTO DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO	8
6.	PRINCIPI SPECIFICI E COMPONENTI DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO..	10



1. DEFINIZIONI

“Appaltatori”: convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del Codice civile, nonché i subappaltatori, i somministranti, i lavoratori autonomi che abbiano stipulato un contratto d’opera con la Società e di cui questa si avvale nei Processi Sensibili.

“CCNL”: Contratto Collettivo Nazionale del Lavoro.

“Comitato delle Segnalazioni”: il Comitato incaricato di ricevere e gestire le segnalazioni delle violazioni ai sensi del D. Lgs. 24/2023 (Whistleblowing).

“Consulenti”: soggetti non dipendenti della Società che agiscono in nome e/o per conto di ESI S.p.A. sulla base di un mandato o di un altro rapporto di collaborazione.

“Decreto”: il Decreto Legislativo n. 231 dell’8 giugno 2001.

“Delega”: l’atto interno di attribuzione di funzioni e compiti nell’ambito dell’organizzazione aziendale.

“Destinatari”: tutti i soggetti cui è rivolto il Modello e, in particolare: gli organi societari ed i loro componenti, i dipendenti, i Fornitori, gli Appaltatori, gli agenti della Società, i Consulenti, i collaboratori a progetto e i lavoratori somministrati, coinvolti nei Processi Sensibili, nonché i membri dell’Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.

“Fornitori”: i fornitori di beni (merci e materiali per la produzione) e servizi (escluse le consulenze) di cui la Società si avvale nell’ambito dei Processi Sensibili.

“Modello”: il Modello di Organizzazione, Gestione e Controllo previsto dal Decreto.

“OdV”: l’Organismo di Vigilanza previsto dal Decreto.

“Organo Dirigente”: Consiglio d’Amministrazione di ESI S.p.A.

“Processo/i Sensibile/i” l’insieme di attività ed operazioni aziendali organizzate al fine di perseguire un determinato scopo o gestire un determinato ambito aziendale di Esi S.p.A., in aree potenzialmente a rischio di commissione di uno o più reati previsti dal Decreto, così come elencate nella Parte Speciale del Modello, indicate anche genericamente e complessivamente come area/e a rischio.

“ProcessOwner” il soggetto che per posizione organizzativa ricoperta o per le attività svolte è maggiormente coinvolto nel Processo Sensibile di riferimento o ne ha maggiore visibilità ai fini del Modello 231.

“Procura” il negozio giuridico unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

“Reati”: le fattispecie di reato considerate dal Decreto.

“Società”: ESI S.p.A.



Esi S.p.A.

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Parte Speciale I: Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori ex art. 25 octies.1 D. Lgs. 231/2001

“Società del Gruppo” tutte le società appartenenti al gruppo facente capo a Innovatec S.p.A. la quale le controlla ai sensi dell’art. 2359 c.c.

“Sistema di Whistleblowing”: sistema di segnalazione messo a disposizione dei dipendenti, nonché dei collaboratori e dei professionisti della società, finalizzato alla comunicazione di violazioni di leggi, violazioni del Modello rilevazioni di pericoli, frodi (reali o potenziali) o un qualunque altro rischio in grado di danneggiare l'azienda stessa, gli azionisti, i dipendenti, i clienti o la reputazione dell'ente.



2. PREMESSA

La presente Parte Speciale, dedicata alla prevenzione Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori disciplina dei comportamenti ed attività che potrebbero astrattamente configurarli, è strutturata nelle seguenti sezioni:

- illustrazione delle **fattispecie di reato** ascrivibili alla famiglia dei Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori e disciplina dei comportamenti ed attività che potrebbero astrattamente configurarli, è strutturata nelle seguenti sezioni, astrattamente configurabili nella realtà ESI;
- identificazione dei processi ed attività aziendali di ESI a rischio di potenziale commissione dei suddetti reati e derivanti dalle attività di risk assessment condotte (c.d. **Processi Sensibili**);
- **Per ciascun Processo Sensibile** viene inoltre fornita la **descrizione sintetica delle attività riconducibili al Processo Sensibile**, nonché illustrate le **esemplificazioni più significative delle fattispecie di reato potenzialmente associabili alla realtà ESI**;
- delineazione dei **principi di comportamento e regole di condotta** applicabili nella realizzazione delle attività entro i Processi Sensibili, ad integrazione del sistema etico e delle regole di comportamento delineati al Capitolo 4.3 della Parte Generale del presente Modello;
- per **ciascun Processo Sensibile, o per categorie omogenee di processi**, viene infine fornita la previsione di **principi specifici di comportamento e di controllo**, coerentemente con i principi ispiratori definiti all'interno del Capitolo 4 della Parte Generale, ed al fine di rappresentare aspetti peculiari delle componenti del sistema di controllo interno rilevanti ai fini della disciplina del/i Processo/i.



3. LE FATTISPECIE DI DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 25-OCTIES.1 DEL DECRETO)

Tra i reati nei confronti della di ricettazione, riciclaggio ed impiego di denaro, beni ed utilità di provenienza illecita, nonché autoriciclaggio previsti dal Decreto si indicano di seguito quelli astrattamente configurabili nell'ambito delle attività svolte da ESI S.p.A.:

- **Indebito utilizzo e falsificazione di carte di credito e di pagamento (art. 493-ter c.p.)** – La norma punisce chi si avvale di carte di credito di cui non è titolare, al fine di trarne profitto (e dunque senza averla rubata, ma anche semplicemente avendola trovata) e chi tali falsifichi le carte, o dopo la falsificazione le ceda, sempre al fine di trarne profitto. Inoltre, il reato si configura anche quando le stesse condotte si compino con qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o servizi”, ma, più in generale, di quelle riguardanti anche “ogni altro mezzo di pagamento diverso dal contante”.
- **Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)** – La norma punisce, chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.
- **Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)** – Tale ipotesi di reato si configura nel caso di alterazione, da parte di un dipendente o di un rappresentante della Società, in qualsiasi modo effettuata, del funzionamento di un sistema informatico o telematico o di intervento, senza averne diritto, su dati, informazioni, programmi, finalizzata al trasferimento di denaro, di valore monetario o di valuta virtuale, commessa in danno anche di privati. Tale reato era già stato previsto nel D. Lgs. 231/2001 come presupposto dell'illecito amministrativo di cui all'art. 24, ma con una rilevanza per l'ente limitata alle sole ipotesi di frode informatica commessa in danno dello Stato o di altro Ente pubblico
- **Trasferimento fraudolento di valori (art. 512-bis) [articolo introdotto dalla L. n. 137/2023]** – Il reato si configura quando vengano attribuite a terzi soggetti fittiziamente la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter .



4. PROCESSI SENSIBILI

I Processi identificati come a rischio di commissione dei Reati ai sensi del Decreto sono emersi dall'analisi di risk assessment (cfr. Capitolo 2 Parte Generale "Processo di redazione e implementazione del Modello").

Con riferimento specifico ai delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, ai fini della presente Parte Speciale, le aree potenzialmente a rischio sono riconducibili ai seguenti Processi Sensibili:

1. Gestione dei flussi finanziari– pagamenti;
2. Gestione dei sistemi informatici
3. Gestione delle Carte di credito aziendali
4. Gestione circolazione dei dati informatici
5. Gestione utilizzo di informazioni, dati e programmi informatici
6. Gestione Operazioni societarie.

Eventuali integrazioni dei suddetti Processi Sensibili a rischio potranno essere richieste a cura dell'Organismo di Vigilanza della Società, al quale viene dato mandato di identificare le relative ipotesi e di definire gli opportuni provvedimenti operativi affinché l'Organo Dirigente della Società provveda a modificare e/o integrare conseguentemente il Modello.

Di seguito, per ciascun Processo Sensibile, verranno fornite in particolare:

- la descrizione sintetica del Processo Sensibile;
- la delineazione dei reati che potrebbero essere astrattamente commessi nell'ambito del Processo."



5. PRINCIPI GENERALI DI CONDOTTA E COMPORTAMENTO E DI ASSETTO DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

La presente sezione illustra le regole di condotta generali e di comportamento, nonché di assetto del sistema di organizzazione, gestione e controllo che, unitamente ai principi definiti al Capitolo 4 della Parte Generale in materia di componenti del sistema di controllo preventivo ed ai principi specifici sanciti nel paragrafo 6 dovranno essere seguite dai Destinatari al fine di prevenire il verificarsi dei Reati descritti nel Paragrafo 3.

La presente Parte Speciale “I” prevede l’espresso divieto – a carico dei Destinatari del presente Modello - di porre in essere comportamenti:

- tali da integrare le fattispecie di reato sopra considerate (art. 25-octies.1 del Decreto);
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarle;
- non in linea o non conformi con i principi e le prescrizioni contenute nel presente Modello e nel Codice Etico;

Agli Organi Sociali e ai Dirigenti di ESI, in via diretta, nonché ad eventuali lavoratori Dipendenti, Collaboratori e i Consulenti, soggetti a vigilanza, è fatto divieto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge, con particolare riferimento alle attività finalizzate alla gestione anagrafica e alla qualifica di Fornitori/Clienti/Consulenti/Appaltatori/Agenti anche stranieri;
- alterare/manomettere/danneggiare il funzionamento di sistemi informatici o telematici anche finalizzato al trasferimento di denaro, di valore monetario o di valuta virtuale, al fine di procurare un vantaggio o un interesse per la società;
- installare nella rete aziendale un proprio software che non rientri nello scopo per cui il sistema informatico è stato assegnato all’utente, per evitare che possa interrompere, danneggiare, manomettere, o impedire le comunicazioni informatiche aziendali;
- Prestare o cedere a terzi qualsiasi apparecchiatura informatica senza la preventiva autorizzazione del Responsabile interno;
- trasferire all’esterno dell’azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà dell’azienda stessa o di altra società collegata ESI, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del Responsabile interno;
- effettuare copie non autorizzate di dati o di software;
- di utilizzare password di altri utenti aziendali, neanche per l’accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile dei Sistemi Informatici;



Esi S.p.A.

IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Parte Speciale I: Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori ex art. 25 octies.1 D. Lgs. 231/2001

- Utilizzare le carte di credito o di debito o di ogni altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque di ogni altro strumento di pagamento diverso dei contanti, nei limiti delle proprie funzioni responsabilità e delle autorizzazioni;
- effettuare operazioni che, anche solo potenzialmente, siano idonee a determinare l'indebito utilizzo e /o la falsificazione di carte di credito e di pagamento sottoporre all'attenzione del superiore gerarchico e/o dell'OdV eventuali situazioni di incertezza in ordine ai comportamenti da tenere, all'interpretazione della normativa vigente;
- intrattenere rapporti economici con soggetti terzi al fine di trasferire valori o beni suscettibili di valutazione economica appartenenti alla Società con l'intento di evitare o limitare gli effetti e le conseguenze derivanti dall'applicazione di misure di prevenzione personali e patrimoniali;
- effettuare operazioni fittizie o di comodo, in contanti, o mediante trasferimenti, costituzione di trust, cessione di crediti, trasferimenti di proprietà e di diritti reali sui beni dell'impresa, o anche mediante locazioni, leasing ed altri diritti di godimento, relativi ai beni della Società al solo fine di sottrarre tali beni all'applicazione di misure di prevenzione personali e patrimoniali.



6. PRINCIPI SPECIFICI E COMPONENTI DEL SISTEMA DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Ai fini dell'attuazione delle regole e dei divieti elencati nel precedente capitolo, oltre che dei principi già contenuti nella Parte Generale del presente Modello di organizzazione, gestione e controllo, con riferimento ai processi sensibili indicati, la società dovrà prevedere:

- la verifica dei dispositivi idonei a ricevere e disporre pagamenti attraverso procedimenti telematici ed informatici, con l'uso di codici identificativi e parole chiave per l'accesso da cambiare periodicamente.
- una vigilanza periodica sui sistemi informatici e telematici per verificarne il corretto funzionamento e l'eventuale presenza di indebite manomissioni;
- una verifica sulle condotte dei terzi contraenti e degli operatori ai fini della prevenzione dei delitti in materia di strumenti di pagamento diversi dai contanti e richiedere, mediante la clausola 231, un impegno specifico in tal senso nei contratti;
- un'individuazione puntuale delle funzioni competenti al processo di incasso/pagamento secondo l'organizzazione gerarchica aziendale.

Ad integrazione di quanto definito nella Parte Speciale A e nella Parte Speciale E, e con riferimento specifico alla prevenzione dei reati oggetto della presente Parte Speciale, si prevede quanto segue:

- non devono essere utilizzati conti correnti, carte di credito o carte prepagato o altri mezzi di pagamento diversi dai contanti in forma anonima o con intestazione fittizia, né in Italia né presso altri Stati esteri;
- tutti i rapporti infragruppo devono essere regolati nell'ambito di contratti formalizzati, autorizzati e firmati coerentemente con il sistema di poteri e deleghe vigenti;
- la tracciabilità nell'ambito della gestione dei rapporti infragruppo deve essere garantita:
 - a) dal flusso documentale generato nell'ambito dei rapporti stessi (tra i servizi aziendali e tra le Società del Gruppo coinvolte);
 - b) dall'esistenza di contratti formalizzati e della documentazione amministrativo-contabile;
- inoltre, al fine di prevenire le condotte potenzialmente illecite riconducibili alle fattispecie delittuose oggetto del presente paragrafo, si ritiene che le prescrizioni specifiche previste nel precedente paragrafo debbano essere applicate anche con riferimento alla gestione dei flussi finanziari generati da operazioni infragruppo.