

PAYBACK ITALIA S.R.L.

CODICE ETICO



INDICE

1.	PREMESSA	3
2.	CODICE ETICO: OBIETTIVI, DESTINATARI E AMBITO APPLICAZIONE	DI 3
3.	PRINCIPI E VALORI DI RIFERIMENTO	5
4.	NORME DI CONDOTTA VERSO I SOGGETTI INTERNI	6
5.	PRINCIPI E NORME DI CONDOTTA VERSO SOGGETTI ESTERNI	7
	5.1Principi di Comportamento nelle Relazioni Istituzionali75.2Rapporti con la Pubblica Amministrazione85.3Autorità Giudiziarie e Autorità di Vigilanza85.4Rapporti con fornitori/consulenti95.5Regali e forme di intrattenimento10	
6.	USO E TUTELA DEI BENI DELLA SOCIETÀ	10
7.	CONFLITTO DI INTERESSE	11
	7.1Posizioni esterne117.2Impiego di un familiare127.3Opportunità commerciali12	
8.	USO E DIVULGAZIONE DELLE INFORMAZIONI	12
9.	TRASPARENZA NELLA CONTABILITÀ	13
	9.1Accuratezza e Trasparenza della Documentazione Ufficiale139.2Registrazione e Documentazione delle Transazioni139.3Trasparenza Contabile149.4Controlli interni149.5Rapporti con revisori e funzionari pubblici o autorità di vigilanza15	
10.	TUTELA DELLA SALUTE E DELLA SICUREZZA	15
11.	PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE E DEL INFORMAZIONI	LE 16
12.	PRIVACY	16
13.	RICICLAGGIO DI DENARO SPORCO	17
14.	CORRUZIONE	17
15.	DIFFUSIONE DEL CODICE ETICO, EFFICACIA E CONSEGUENZE DEL SUE VIOLAZIONI	
16.	DISPOSIZIONI FINALI	19



1. PREMESSA

I termini utilizzati nel presente Codice Etico hanno lo stesso significato loro attribuito nel Modello di Organizzazione, Gestione e Controllo adottato dalla Società.

Payback opera nel campo dell'organizzazione, gestione, promozione e sviluppo di programmi di fidelizzazione, compresi concorsi e operazioni a premio, nonché della prestazione di servizi di marketing, creazione e gestione di database per rivenditori, fornitori di prodotti e/o servizi e produttori di beni di largo consumo.

Payback, in qualità di società appartenente al gruppo American Express recepisce, nel presente Codice Etico, i principi illustrati nel Codice di Condotta del gruppo. Quest'ultimo fa riferimento, in particolare, ad elevati standard sostenuti in tutte le relazioni interne e con i partners, inclusi clienti, azionisti, venditori ed enti pubblici.

Pertanto, Payback ha ritenuto opportuno e necessario adottare ed emanare un Codice Etico (di seguito anche il "Codice") che espliciti i valori cui deve essere improntata la condotta di tutti coloro che, ai vari livelli di responsabilità, concorrono con i propri atti allo svolgimento della sua attività, compresi i consulenti e/o i fornitori e i collaboratori esterni comunque denominati.

2. CODICE ETICO: OBIETTIVI, DESTINATARI E AMBITO DI APPLICAZIONE

Al Codice sono attribuite le seguenti funzioni:

- preventiva: la codificazione dei principi etici di riferimento e delle regole di
 comportamento basilari cui tutti i portatori di interesse devono uniformarsi, costituisce
 l'espressa dichiarazione dell'impegno serio ed effettivo della Società a rendersi garante
 della legalità della propria attività, con particolare riferimento alla prevenzione degli
 illeciti;
- **cognitiva:** il Codice, attraverso l'enunciazione di principi astratti e generali e di regole di comportamento, consente di riconoscere i comportamenti non etici e di indicare le corrette modalità di esercizio delle funzioni e dei poteri attribuiti a ciascuno;
- di legittimazione: il Codice esplicita i doveri e le responsabilità della Società nei confronti dei portatori di interesse affinché questi ultimi possano ritrovare in esso un riconoscimento delle loro aspettative;
- **di incentivo**: il Codice, imponendo l'osservanza dei principi e delle regole in esso contenute, contribuisce allo sviluppo di una coscienza etica, rafforza la reputazione della Società ed il rapporto di fiducia con i portatori di interesse.



L'insieme dei principi etici e dei valori espressi nel Codice, dovrà ispirare l'attività di tutti coloro che operano all'interno della Società, tenendo conto dell'importanza dei ruoli, della complessità delle funzioni e delle responsabilità loro affidate per il perseguimento degli scopi della Società.

Il Codice è rivolto indistintamente a tutti i Destinatari del Modello; in particolare, a titolo esemplificativo e non esaustivo:

- ai componenti del Consiglio di Amministrazione della Società, che si ispirano ai principi del Codice nel fissarne gli obiettivi;
- al Presidente, che si conforma al Codice nell'esercizio della rappresentanza della Società, nel compito di sovraintendere al suo funzionamento e di dare esecuzione alle deliberazioni del Consiglio e dell'Assemblea;
- ai singoli dirigenti che:
 - assumono atteggiamenti leali e trasparenti e adottano un comportamento esemplare e imparziale nei rapporti con i colleghi, i collaboratori e i destinatari dell'azione della Società;
 - curano il benessere organizzativo della struttura a cui sono preposti, favorendo l'instaurarsi di rapporti cordiali e rispettosi tra i collaboratori;
 - assumono iniziative finalizzate alla costante condivisione delle informazioni, alla formazione e all'aggiornamento del personale, all'inclusione e al rispetto delle differenze di genere, di età e di condizioni personali. I dirigenti, inoltre, nei limiti delle loro possibilità, gestiscono le notizie riguardanti l'organizzazione, l'attività e i dipendenti della Società in modo trasparente e favoriscono la diffusione della conoscenza di buone prassi e buoni esempi al fine di rafforzare il senso di fiducia nei confronti della Società;
- ai dipendenti e i collaboratori esterni su base continuativa che, nel dovuto rispetto della legge e delle normative vigenti, adeguano le proprie azioni ed i propri comportamenti ai principi, agli obiettivi ed agli impegni previsti dal Codice Etico;
- ai fornitori, ai consulenti e, in generale, alle società terze con le quali la Società intrattiene rapporti.



Tutti i soggetti sopra elencati, nonché gli altri Organi Statutari della Società (Assemblea e Collegio Sindacale) e tutti coloro che operano per il conseguimento dello scopo e degli obiettivi della Società sono, pertanto, considerati Destinatari del Codice.

I Destinatari si impegnano a perseguire i propri obiettivi con lealtà, serietà, onestà, competenza e trasparenza, nel rispetto delle leggi e delle normative vigenti.

In questo quadro la Società si impegna a:

- favorire la massima diffusione del Codice Etico, provvedendo al suo approfondimento ed aggiornamento;
- assicurare e promuovere il rigoroso rispetto delle leggi e del Codice Etico;
- assicurare e promuovere un programma di formazione differenziato e di sensibilizzazione circa le problematiche attinenti al Codice Etico;
- svolgere tutte le necessarie verifiche in ordine ad ogni notizia inerente a possibili violazioni, applicando, in caso di accertamento delle stesse, adeguate sanzioni.

3. PRINCIPI E VALORI DI RIFERIMENTO

Tutti i Destinatari devono tenere fede ai seguenti valori:

- Legalità: ogni attività deve essere condotta nella consapevolezza della normativa primaria e secondaria applicabile e nel rispetto, tanto formale che sostanziale, di essa;
- **Integrità:** gli obiettivi della Società devono essere perseguiti con onestà, correttezza e responsabilità, nel rispetto delle regole dell'etica professionale;
- Trasparenza: relazionarsi in modo chiaro, completo e diligente al fine di consentire a tutti gli interlocutori di prendere le proprie decisioni consapevolmente e in via autonoma;
- Riservatezza: tutelare la riservatezza delle informazioni e dei dati dei quali si dovesse
 venire a conoscenza; non utilizzarli, salvi gli obblighi normativamente previsti, per finalità
 estranee all'espletamento del proprio compito; adoperarsi affinché siano osservati tutti gli
 adempimenti previsti dalla legge in materia di *privacy*, al fine di garantire la sicurezza nel
 trattamento delle informazioni attraverso l'utilizzo di sistemi e tecnologie affidabili;
- Rispetto e valorizzazione del personale: impegno al rispetto della dignità individuale e
 delle differenze di genere, età, etnia, religione ed appartenenza politica e sindacale, etc.;
 al rispetto dell'integrità psico-fisica, morale e culturale della persona, attraverso un
 ambiente di lavoro sicuro in cui i rapporti tra colleghi siano improntati alla lealtà,
 correttezza, collaborazione, rispetto reciproco e fiducia;



 Correttezza: seguire un comportamento che rispetti le buone regole della morale e dell'etica, provvedendo a garantire verifiche appropriate per il corretto svolgimento delle attività della Società.

4. NORME DI CONDOTTA VERSO I SOGGETTI INTERNI

La Società riconosce che il personale dipendente è elemento indispensabile per la propria esistenza e per il proprio sviluppo; ne riconosce la centralità, nella convinzione che il più rilevante fattore di successo della propria attività sia costituito dal contributo professionale di ciascuno, in un contesto di lealtà e reciproca fiducia.

A tal proposito, Payback offre a tutti i propri dipendenti pari opportunità di lavoro, in funzione delle rispettive caratteristiche professionali, competenze e conoscenze nonché delle capacità di rendimento, senza alcuna discriminazione.

La Società, pertanto, pone particolare attenzione alla valorizzazione, alla tutela ed allo sviluppo delle capacità e delle competenze di tutti i propri dipendenti, affinché essi possano esprimere al massimo livello, nell'ambito della mansione assegnata, il proprio potenziale e la propria professionalità.

La Società si impegna ad adottare criteri di imparzialità, merito, competenza e professionalità per qualunque decisione inerente ai rapporti con il personale di cui si avvale e con i collaboratori in genere. Non è consentita alcuna pratica discriminatoria nella selezione, assunzione, formazione, gestione, sviluppo e retribuzione del personale.

Payback, tra i suoi principali obiettivi, si propone quello di creare un ambiente di lavoro privo di molestie. Le molestie, nello specifico, si identificano nei comportamenti offensivi che mirano a creare un ambiente minaccioso, ostile e offensivo. Il comportamento si definisce molesto, a prescindere che sia fisico o verbale, sia se posto in essere di persona che con altri mezzi (lettere o e-mail).

A tale scopo l'Amministratore Delegato e i dirigenti, nel rispetto di tutte le leggi, regolamenti e politiche in vigore, si impegnano a:

- selezionare, assumere, retribuire, formare e valutare i dipendenti in base a criteri di merito, di competenza e professionalità, senza alcuna discriminazione politica, sindacale, religiosa, razziale, di lingua e di sesso;
- non assumere lavoratori provenienti da paesi esteri con permesso di soggiorno non valido e a richiedere ai propri fornitori/consulenti di osservare tale previsione;
- assicurare un ambiente di lavoro in cui i rapporti tra colleghi siano improntati alla lealtà, correttezza, collaborazione, rispetto reciproco e fiducia;



- offrire condizioni di lavoro adeguate dal punto di vista della sicurezza e della salute, nonché rispettose della personalità morale di tutti, in modo tale da favorire rapporti interpersonali liberi da pregiudizi;
- intervenire in caso di atteggiamenti non conformi ai principi sopra esposti;
- combattere, in particolare, qualsiasi forma di intimidazione, ostilità, isolamento, indebita interferenza o condizionamento, molestia sessuale.

Nell'evoluzione del rapporto di lavoro, Payback favorisce lo sviluppo del potenziale e la crescita professionale di ciascuna risorsa prevedendo programmi di formazione ed aggiornamento in relazione ai profili professionali ed alle potenzialità di ciascuno.

Al personale è richiesto di sollecitare l'acquisizione di nuove competenze e conoscenze, metodologie di lavoro, favorire lo scambio di conoscenze professionali tra colleghi e con i propri superiori o dirigenti, mentre a questi ultimi si richiede di prestare la massima attenzione alla valorizzazione delle potenzialità delle persone che gestiscono, richiedendo prestazioni coerenti con l'esercizio delle mansioni loro assegnate.

Costituisce abuso della posizione di autorità richiedere alle figure subordinate favori personali o qualunque comportamento che configuri una violazione al presente Codice Etico o alle disposizioni legislative applicabili.

5. PRINCIPI E NORME DI CONDOTTA VERSO SOGGETTI ESTERNI

5.1 Principi di Comportamento nelle Relazioni Istituzionali

Con riferimento ai rapporti che si instaurano con le istituzioni nazionali o internazionali, Payback si impegna ad evitare qualsiasi tipo di discriminazione e a comunicare con tutti gli interlocutori istituzionali a livello nazionale e territoriale.

Solo i referenti che abbiano ricevuto esplicito mandato dall'Amministratore Delegato potranno tenere i contatti con gli interlocutori istituzionali, al fine di garantire la massima chiarezza nei rapporti.

Analogamente, i rapporti con le Istituzioni Pubbliche volti al presidio degli interessi complessivi della Società e collegati all'attuazione dei suoi programmi che comportino impegni nei confronti delle Istituzioni Pubbliche, sono riservati esclusivamente ai soggetti a ciò delegati.

In virtù di questi principi, tutti i Destinatari devono perseguire i legittimi obiettivi della Società e rifiutare ogni accordo illecito con esponenti della Pubblica Amministrazione e/o di altre associazioni/società.



5.2 Rapporti con la Pubblica Amministrazione

Nell'espletamento dell'attività istituzionale la Società entra in contatto con la Pubblica Amministrazione (a titolo meramente esemplificativo: Agenzia delle Entrate, INPS, INAIL, etc.).

Nell'ambito di tali rapporti, è necessario ispirarsi alla più rigorosa osservanza delle disposizioni di legge applicabili, prestando particolare cura nel non porre in essere atti in violazione delle prescrizioni di legge, del Modello e del presente Codice Etico. In particolare, è fatto espresso divieto di:

- offrire, anche per interposta persona, denaro o altra utilità che può consistere anche in opportunità di lavoro o commerciali al funzionario pubblico coinvolto, ai suoi familiari o a soggetti in qualunque modo allo stesso collegati;
- ricercare o instaurare illecitamente relazioni personali di favore, influenza, ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto;
- indurre in errore, con artifici o raggiri, il funzionario pubblico al fine di ottenere un vantaggio per la Società;
- assecondare la condotta induttiva di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Atti di cortesia (come, a titolo di esempio, omaggi o forme di ospitalità) sono consentiti solo se non eccedono le normali pratiche di cortesia e se, in ogni caso, sono tali da non compromettere l'imparzialità e l'indipendenza di giudizio del rappresentante della Pubblica Amministrazione.

5.3 Autorità Giudiziarie e Autorità di Vigilanza

Payback opera nel rispetto della normativa vigente; a tal fine la Società svolge le proprie attività in modo lecito e corretto.

Nei rapporti con le Autorità Giudiziarie è espressamente vietato porre in essere pratiche corruttive di qualsiasi genere; nel caso in cui la Società sia coinvolta in procedimenti giudiziali o stragiudiziali in sede civile, penale, amministrativa e tributaria, il personale, o chiunque agisca in nome e/o per conto della Società (es. legali esterni all'uopo nominati), non dovrà in alcun modo adottare comportamenti nei confronti delle Autorità Giudiziarie per indurre tali soggetti ad adottare provvedimenti che rechino un ingiusto vantaggio per la Società.

La Società collabora con qualunque pubblico ufficiale che abbia poteri ispettivi e svolga indagini nei suoi confronti.



In occasione di un procedimento giudiziario e/o di un'indagine/ispezione da parte delle autorità pubbliche, nessuno deve:

- distruggere/alterare registrazioni, verbali, scritture contabili e qualsiasi altro tipo di documento,
- mentire o fare/intimare a fare dichiarazioni false alle autorità competenti.

Qualsiasi tentativo di estorsione o di concussione da parte di un pubblico ufficiale deve essere segnalato al proprio responsabile.

Nell'ambito dei rapporti con le Autorità di Vigilanza (es. Autorità garante per la protezione dei dati personali), Payback presta la massima collaborazione in maniera da non ostacolare in alcun modo lo svolgimento delle funzioni da parte dell'autorità stessa, ispirandosi ai principi di trasparenza, professionalità e piena collaborazione, conformemente al Modello.

Le comunicazioni e le segnalazioni, anche di carattere periodico, sono fornite in modo completo e tempestivo, nel pieno rispetto della normativa tempo per tempo vigente e delle procedure interne adottate dalla Società.

5.4 Rapporti con fornitori/consulenti

La Società riconosce il valore del ruolo del fornitore nell'ambito dei servizi erogati e per questo motivo ritiene necessario instaurare rapporti di fiducia reciproca, definendo contratti che possano contemperare l'interesse della Società ad un servizio efficiente ed economico con la giusta remunerazione del servizio stesso.

La scelta dei fornitori e la determinazione delle condizioni d'acquisto di beni e servizi è svolta sulla base di criteri obiettivi e imparziali, fondati in prevalenza sulla valutazione della serietà, affidabilità, qualità, efficienza ed economicità, nel rispetto dei processi di selezione descritti nelle policy di American Express.

La Società, nelle procedure di acquisto:

- assicura una concorrenza adeguata;
- fornisce un'informazione comprensibile e completa che consenta a tutti i concorrenti di presentare un'offerta congrua;
- adotta nella scelta dei fornitori criteri oggettivi e documentabili;
- seleziona i fornitori in base alla valutazione dei livelli di qualità ed economicità delle prestazioni, dell'idoneità tecnico-professionale, del rispetto dell'ambiente;



• verifica il rispetto della normativa in materia di lavoro e salute e sicurezza dei lavoratori.

Sono vietati favoritismi, comportamenti collusivi, corresponsione di benefici, materiali e immateriali, o altri vantaggi finalizzati ad influenzare o compensare rappresentanti di istituzioni o dipendenti o componenti degli Organi della Società.

Payback porta a conoscenza dei fornitori e dei consulenti il contenuto del presente Codice mediante la sua pubblicazione sul proprio sito internet.

5.5 Regali e forme di intrattenimento

Nel corso delle attività della Società occorre applicare criteri generali di correttezza, trasparenza e integrità. In particolare, da parte dei Destinatari, non devono essere:

- esaminate, proposte o promesse, opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della P.A. o fornitori a titolo personale;
- offerti in alcun modo omaggi, dazioni, benefici anche indiretti, beni, servizi e prestazioni non dovuti, favori che travalichino gli ordinari rapporti di cortesia;
- intraprese azioni volte a influenzare impropriamente le decisioni della controparte.

Inoltre, occorre prestare attenzione nell'offrire o nell'accettare regali o altre forme di intrattenimento con chiunque ha relazioni commerciali con la Società, nonché con attuali o potenziali clienti o altri partner aziendali. In particolare, non sarà concesso accettare o offrire regali omaggi o altre utilità nelle seguenti forme:

- oggetti che hanno un valore significativo;
- trattamenti di favore.

Inoltre, non sarà permesso accettare o offrire intrattenimento come omaggio che abbia:

- valore eccessivo;
- nessuna relazione con l'attività lavorativa svolta;
- con una forma non appropriata.

6. USO E TUTELA DEI BENI DELLA SOCIETÀ

Tutti i dipendenti ed i collaboratori devono ricordare che i beni materiali ed immateriali messi a loro disposizione da Payback sono da utilizzare:

- con il massimo scrupolo ed in modo proprio, anche al fine di evitare danni a cose o a
 persone;
- evitando, per quanto possibile, sprechi, manomissioni od impieghi che possano comprometterne lo stato di efficienza o accelerarne il normale deterioramento;



- esclusivamente per scopi connessi e strumentali all'esercizio dell'attività lavorativa;
- evitando assolutamente salvo quanto previsto da normative specifiche l'utilizzo da parte di terzi o la cessione dei beni stessi a terzi, anche temporaneamente.

Anche le dotazioni ed applicazioni informatiche devono essere utilizzate nel rispetto di quanto sopra ed in particolare:

- seguendo attentamente le politiche di sicurezza e riservatezza;
- evitando assolutamente l'acquisizione, l'utilizzo o la trasmissione, in particolar modo se massiva, di informazioni e contenuti non attinenti all'attività lavorativa;
- non alterando le configurazioni hardware e software fornite dalla Società.

Tutti i dipendenti devono anche operare al fine di ridurre il rischio di furti, danneggiamenti, intrusioni od altre minacce esterne alle risorse assegnate o presenti nella Società, informando tempestivamente le Funzioni preposte in caso di situazioni anomale.

7. CONFLITTO DI INTERESSE

Tutti i Destinatari e, in particolare, i Consiglieri di Amministrazione, l'Amministratore Delegato, i dipendenti ed i collaboratori a vario titolo devono evitare ogni situazione ed astenersi da ogni attività che possa contrapporre un interesse personale – diretto o indiretto – a quelli della Società o che possa interferire ed intralciare la capacità di assumere, in modo imparziale ed obiettivo, decisioni nell'interesse della Società stessa.

Il verificarsi di situazioni di conflitto d'interesse, oltre ad essere in contrasto con le norme di legge e con i principi fissati nel Codice Etico, risulta pregiudizievole per l'immagine e l'integrità della Società.

I Destinatari devono, quindi, escludere ogni possibilità di sovrapporre o comunque incrociare, strumentalizzando la propria posizione funzionale, le attività economiche rispondenti ad una logica di interesse personale e/o familiare e le mansioni che svolgono o ricoprono all'interno della Società.

Eventuali situazioni di conflitto, ancorché potenziale, dovranno essere tempestivamente e dettagliatamente comunicate alla Funzione *Compliance*, anche per il tramite del proprio superiore gerarchico.

7.1 Posizioni esterne

I dipendenti non devono svolgere attività esterne che interferiscono con la capacità di svolgere il proprio lavoro presso la Società. In particolare, è fatto divieto di accettare lavori da società esterne che agiscono in qualità di fornitori, partner commerciali o competitor della Società, senza la previa approvazione dell'Ufficio *Compliance*. Allo stesso modo, potrebbe sorgere un



conflitto di interessi nel caso in cui un parente o un familiare di un dipendente lavori per una società concorrente o per un partner commerciale della Società.

Infine, non è ammesso assumere la funzione di direttore, amministratore, membro del consiglio di amministrazione, o consulente in società diverse da American Express o in una delle sue consociate senza previa autorizzazione dell'Ufficio *Compliance*.

7.2 Impiego di un familiare

Per evitare conflitti di interesse, prima di assumere un familiare di un dipendente, sarà necessario consultare l'Ufficio *Compliance* ed evitare che il dipendente lavori direttamente, o nello stesso reparto del familiare, o che prenda decisioni che lo coinvolgono.

7.3 Opportunità commerciali

Non è consentito accettare opportunità commerciali, pagamenti, commissioni o accordi finanziari vantaggiosi da un partner, cliente, fornitore, concorrente della Società.

Inoltre, non è consentito acquistare per uso personale beni o servizi dei fornitori della Società a condizioni diverse da quelle normalmente offerte al pubblico o stabilite dalla politica aziendale.

8. USO E DIVULGAZIONE DELLE INFORMAZIONI

Payback considera la diffusione di informazioni corrette, complete e veritiere su tutti i fatti – ed il mantenimento della dovuta riservatezza sugli stessi, quando necessario – quale presupposto per creare e conservare un rapporto di trasparenza e di fiducia con tutti i suoi interlocutori.

Conseguentemente, nella gestione delle informazioni, i dipendenti devono:

- conservare scrupolosamente e con il massimo riserbo tutte le informazioni riguardanti la Società di qualunque tipologia apprese nell'esercizio delle proprie funzioni;
- richiedere, ove previsto, il consenso al trattamento dei dati personali, per le finalità comunicate.

In relazione alle informazioni in genere, i dipendenti devono:

- evitare un uso improprio o strumentale di quelle riservate in proprio possesso, né utilizzarle a proprio vantaggio e/o di quello dei familiari, dei conoscenti e dei terzi in genere;
- proteggerle dall'accesso di terzi non autorizzati, impedirne la diffusione a meno di specifiche autorizzazioni del Titolare;



- non ricercare, o cercare di ottenere da altri, quelle non attinenti la propria sfera di competenza o funzioni;
- classificarle ed organizzarle in modo che sia possibile, per i soggetti autorizzati, accedervi in maniera agevole e traendone un quadro completo.

Ai dipendenti non espressamente autorizzati, nelle forme e nei termini previsti dalla normativa in tema di privacy di cui al Regolamento UE 2016/679, avente per oggetto la tutela dei dati personali, è vietato conoscere, registrare, trattare e divulgare i dati personali dei dipendenti o di terzi.

9. TRASPARENZA NELLA CONTABILITÀ

9.1 Accuratezza e Trasparenza della Documentazione Ufficiale

Tutti i documenti ufficiali volti ad illustrare la situazione gestionale della Società, devono essere redatti con la massima cura al fine di garantirne l'accuratezza e la veridicità. Devono, inoltre, essere redatti in conformità delle leggi e normative vigenti.

Nella redazione dei predetti documenti, il personale di Payback deve prestare la dovuta attenzione e mantenere quei comportamenti improntati a principi di correttezza, onestà e integrità che devono uniformare lo svolgimento delle attività professionali di propria competenza.

In ogni caso non sarà giustificata né giustificabile la tenuta/redazione di documentazione deliberatamente falsa o artefatta in modo da alterare significativamente la rappresentazione veritiera della situazione di Payback.

9.2 Registrazione e Documentazione delle Transazioni

I fatti di gestione vengono rilevati con la massima tempestività nel sistema contabile di Payback, in base al tipo di operazioni cui afferiscono, mentre il personale preposto provvede a registrare extracontabilmente tutte le movimentazioni bancarie e di cassa (entrate/uscite) secondo le tempistiche previste dalla funzione competente. Il sistema contabile di Payback registra le operazioni inerenti la gestione della Società, mediante: scritture contabili rilevate e contabilizzate in automatico attraverso i sistemi informatizzati delle società convenzionate; scritture contabili rilevate e contabilizzate manualmente, generate mediante imputazione diretta ad opera del personale addetto.

Ogni operazione, azione e transazione della Società deve essere adeguatamente registrata e documentata in modo da consentirne la verifica dei processi di decisione, autorizzazione e svolgimento.



È necessario assicurare che i dati da fornire per la preparazione dei bilanci siano conformi a tutti i principi di contabilità applicabili e alle procedure interne di controllo della Società.

Ogni atto od operazione svolta dal personale dovrà essere supportata da documentazione adeguata, chiara e completa da conservare agli atti, in modo da consentire in ogni momento il controllo sulle motivazioni, le caratteristiche dell'operazione e l'individuazione dei soggetti che hanno eseguito l'operazione, che hanno concesso le autorizzazioni e che hanno effettuato le verifiche.

Va precisato, inoltre, che non sarà possibile distruggere, nascondere o modificare documenti o registri che ostacolino investigazioni, azioni legali, verifiche o ispezioni.

9.3 Trasparenza Contabile

Tutte le funzioni di Payback sono tenute a prestare la massima collaborazione al fine di garantire registrazioni contabili corrette e tempestive. Le registrazioni contabili fondate su valutazioni economico-patrimoniali devono rispettare i criteri di ragionevolezza e prudenza.

Per ogni registrazione contabile deve essere conservata agli atti un'adeguata documentazione.

Tale documentazione deve consentire di individuare il motivo dell'operazione che ha generato la rilevazione e la relativa autorizzazione. La documentazione di supporto deve essere archiviata e facilmente consultabile.

Chiunque venga a conoscenza di possibili omissioni, falsificazioni o irregolarità nella tenuta della contabilità deve darne immediata comunicazione al proprio superiore.

Inoltre, nello svolgimento delle attività di verifica e controllo da parte della società di revisione e del Collegio Sindacale, è necessario agire con trasparenza e prestare la massima collaborazione.

9.4 Controlli interni

Payback diffonde a tutti i livelli una cultura basata sulla responsabilizzazione delle persone e sull'attività di controllo, in considerazione del contributo positivo che questi possano dare in termini di efficienza.

La Società, pertanto, presta ogni collaborazione improntando i propri comportamenti alla massima correttezza e trasparenza e trasmettendo in maniera puntuale le informazioni e i dati idonei a consentire un corretto esercizio delle funzioni di controllo.

Tutti gli attori della Società (dai dirigenti ai collaboratori) sono quindi responsabili, nell'ambito delle proprie attività, in relazione alla definizione e al corretto funzionamento del sistema di controllo interno.



9.5 Rapporti con revisori e funzionari pubblici o autorità di vigilanza

I dipendenti devono collaborare con i revisori esterni e interni, con i funzionari pubblici o con l'Autorità di Vigilanza in relazione a qualsiasi verifica della Società. Inoltre, non è consentito influenzare illecitamente un revisore dei conti o un membro dell'Autorità durante il controllo sui bilanci. Pertanto, non è permesso fornire informazioni fuorvianti, l'offerta di denaro od oggetti di valore per il buon esito della verifica.

10. TUTELA DELLA SALUTE E DELLA SICUREZZA

Payback attribuisce grande importanza all'integrità fisica e morale dei propri dipendenti e collaboratori, a condizioni di lavoro rispettose della dignità individuale e ad ambienti di lavoro sicuri e salubri; la Società cura, pertanto, la diffusione e il consolidamento di una cultura della sicurezza e della salute dei lavoratori sul luogo di lavoro, sviluppando la consapevolezza dei rischi e promuovendo comportamenti responsabili da parte di tutto il personale.

In particolare, i principi che influiscono sulla salute e la sicurezza sul posto di lavoro sono i seguenti:

- a) eliminare i rischi e ridurli al minimo in relazione alle conoscenze acquisite in base al progresso tecnologico;
- b) valutare i rischi che non possono essere evitati;
- c) rispettare i principi di salubrità dei luoghi di lavoro nell'organizzazione dello stesso e nella scelta degli strumenti e dei metodi di lavoro utilizzati;
- d) tener conto del grado di evoluzione della tecnica;
- e) sostituire ciò che è pericoloso con ciò che non lo è o risulta più sicuro;
- f) programmare le misure opportune per garantire il miglioramento dei livelli di sicurezza;
- g) programmare la prevenzione, mirando a integrare la tecnica, l'organizzazione, le condizioni del lavoro;
- h) dare la priorità alle misure di protezione collettiva rispetto a quelle di protezione individuale;
- i) impartire adeguate istruzioni ai lavoratori.

Il Datore di Lavoro e le altre figure dotate di poteri gerarchici e funzionali devono curare, o fare in modo che i terzi che agiscono per conto della Società curino il rispetto delle disposizioni vigenti ed in generale le prescrizioni contenute nel D.Lgs. n. 81/2008.

Gli organi statutari e il Datore di Lavoro devono assicurare che la Società disponga di una struttura organizzativa tale da assicurare una chiara suddivisione di compiti e obblighi in



materia di salute e sicurezza sul lavoro, definiti formalmente in coerenza con lo schema organizzativo e funzionale della Società e con le prescrizioni regolamentari e di legge, a partire dal Datore di Lavoro e dai Dirigenti fino al singolo lavoratore.

Tutti i soggetti destinatari degli obblighi in materia di salute e sicurezza sul lavoro devono rispettare le procedure e le misure generali di tutela previste dalla Società.

11. PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE E DELLE INFORMAZIONI

Payback, ai sensi del presente Codice, rivendica la protezione della Proprietà Intellettuale, comprensiva di ogni creazione dell'intelletto umano quali copyright, brevetti, marchi registrati, segreti commerciali, diritti sul design, loghi, know-how e altri tipi di proprietà industriale o commerciale.

Con riferimento alle informazioni riservate della Società, quali segreti industriali, Payback impone il divieto di divulgarle al di fuori se non per scopi d'affari. Nel caso in cui vi sia una necessità dettata dal business, è possibile divulgare tali informazioni a terze parti solo previa predisposizione di un accordo di riservatezza.

I suddetti obblighi si applicano durante il periodo lavorativo e anche dopo la terminazione del contratto di impiego. Quando un dipendente lascia la Società, dovrà restituire tutto il materiale contente informazioni riservate o segreti industriali in suo possesso.

12. PRIVACY

Payback non condivide le informazioni personali identificabili di clienti o dipendenti con terze parti, senza prima verificare che il ricevente sia stato autorizzato a riceverle per una legittima ragione di business, nonché senza prima assicurarsi che la persona sia vincolata da specifici accordi di confidenzialità e dai contratti.

A tal proposito, nell'*Open Network Confidentiality Operating Principles (ONCOP)*, vengono illustrati i seguenti principi a garanzia della corretta gestione delle informazioni confidenziali:

- Obbligazioni legali e contrattuali: le informazioni devono essere condivise in conformità alle norme contrattuali e legali. La Società protegge le informazioni confidenziali dei partner emittenti e di coloro che acquisiscono esercizi commerciali. Le leggi Antitrust e per il commercio equo, inoltre, proibiscono di condividere i prezzi e le altre informazioni commerciali con i competitors e altre terze parti.
- 2. **Condivisione delle informazioni**: le informazioni commerciali (strategie di business o di prezzi; piani di Marketing; dettagli relativi a contratti o accordi con partner del



Network, ecc.) di un emittente o di un soggetto che acquisisce esercizi commerciali all'interno del Network non devono essere utilizzate da nessun altro emittente o acquisitore di esercizi.

3. **Supporto del Network**: alcuni gruppi a supporto dell'American Express Global Network possono avere accesso ad informazioni confidenziali relative agli emittenti con il solo scopo di supportare il Network.

Come dipendenti, inoltre, si può avere accesso a informazioni riguardanti più di un emittente o il Network quando:

- il ruolo è necessario a supporto del Network e c'è un evidente bisogno di acquisire informazioni su più di un emittente o sul Network nel suo complesso;
- il ruolo richiede che venga fatta consulenza e assistenza in diversi settori e non è circoscritto ad un singolo emittente;
- si è a supporto di più di un emittente o acquisitore e quindi si deve avere accesso a informazioni su tutto il Network per il quale si opera.

13. RICICLAGGIO DI DENARO SPORCO

Il riciclaggio di denaro sporco rappresenta il processo con cui i proventi di attività criminali vengono fatti passare attraverso il sistema finanziario per nascondere ogni traccia della loro origine criminale. Per evitare di incorrere nel suddetto reato, la Società deve prendere ogni precauzione al fine di scegliere i partner aziendali che non usino il marchio, i prodotti o i servizi di American Express per intraprendere azioni illegali. Inoltre, qualora un dipendente venga contattato da un ente pubblico per indagini relative a riciclaggio di denaro sporco dovrà informare immediatamente l'Ufficio *Compliance*.

14. CORRUZIONE

Non è ammessa alcuna forma di corruzione, compresa l'offerta o l'accettazione di oggetti di valore, al fine di ottenere o conservare rapporti d'affari o servizi.

In particolare, nel corso di una trattativa d'affari, richiesta o rapporto commerciale con la Pubblica Amministrazione, non vanno intraprese le seguenti azioni:

- esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione;
- offrire o fornire omaggi;
- sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti.



È altresì necessario evitare di incorrere nel reato di corruzione nella gestione dei rapporti con funzionari pubblici, di organizzazioni internazionali e partiti politici, nonché con dipendenti di aziende pubbliche. Inoltre, non è consentito offrire beni di valore, al fine di influenzare le azioni o le decisioni, o ottenere un vantaggio improprio da funzionari o organismi pubblici. Infine, è proibito pagare tangenti a impiegati governativi, indipendentemente dal luogo in cui svolgono il loro lavoro.

15. DIFFUSIONE DEL CODICE ETICO, EFFICACIA E CONSEGUENZE DELLE SUE VIOLAZIONI

15.1 Diffusione ed efficacia

Il Codice Etico costituisce uno degli elementi fondanti del sistema preventivo ed è parte integrante del Modello in ottemperanza al D.Lgs. n. 231/2001.

Il sistema di controllo interno, orientato all'adozione di strumenti e metodologie di monitoraggio, è volto a contrastare i potenziali rischi al fine di determinare una ragionevole garanzia circa il rispetto delle leggi e di tutte le disposizioni e procedure interne della Società.

La Società si impegna ad assicurare:

- la massima diffusione del presente Codice Etico, mediante pubblicazione sul sito internet della Società;
- la predisposizione di strumenti conoscitivi, esplicativi, di informazione e sensibilizzazione con riferimento ai contenuti del Codice Etico;
- lo svolgimento di verifiche periodiche allo scopo di monitorare il grado di osservanza delle disposizioni contenute nel Codice Etico;
- il costante aggiornamento del Codice Etico, in relazione all'evoluzione dell'attività della Società, a eventuali mutamenti nella sua struttura organizzativa o gestionale, nonché in rapporto alle tipologie di violazioni riscontrate nell'ambito dell'attività di vigilanza;
- la previsione di adeguati strumenti di prevenzione, l'attuazione di idonee misure sanzionatorie, nonché la tempestiva applicazione delle stesse in caso di accertata violazione delle disposizioni del Codice Etico.

Ove richiesto, una copia del Codice Etico sarà consegnata a tutti i soggetti che intrattengono relazioni con la Società. Ai dipendenti viene trasmesso inizialmente con specifica mail o consegnato all'atto dell'assunzione. Il Codice viene inoltre pubblicato nella intranet aziendale.

15.2 Violazioni e whistleblowing



È fatto obbligo a chiunque entri in relazione con la Società di osservare e di fare osservare il presente Codice.

L'osservanza delle norme contenute nel presente Codice deve considerarsi parte essenziale delle obbligazioni contrattuali previste per i dipendenti della Società, ai sensi dell'articolo 2104 del Codice Civile, nonché per i collaboratori dello stesso.

La violazione delle suddette norme costituirà inadempimento alle obbligazioni derivanti dal rapporto di lavoro e/o illecito disciplinare, con ogni conseguenza di legge, anche in ordine alla conservazione del rapporto di lavoro.

La Società s'impegna a prevedere ed irrogare, con coerenza, imparzialità ed uniformità, sanzioni proporzionate alle rispettive violazioni del Codice e conformi alle vigenti disposizioni in materia di regolamentazione dei rapporti di lavoro.

Payback incoraggia i Destinatari a riferire tempestivamente all'Organismo di Vigilanza condotte illecite o, comunque, contrarie al Codice, delle quali vengano a conoscenza in ragione dei propri rapporti con la Società. A tal fine, Payback si è dotata di un sistema interno di segnalazione delle violazioni (c.d. *whistleblowing*), finalizzato a rafforzare i presidi di legalità e trasparenza.

A tal proposito, chiunque commetta un'azione di ritorsione contro una persona, che in buona fede effettui una segnalazione o collabori a un'indagine, sarà soggetto a un'azione disciplinare che potrà includere anche il licenziamento.

Fuori dai casi di responsabilità a titolo di calunnia e diffamazione, ovvero per lo stesso titolo ai sensi dell'art. 2043 c.c., nessun Destinatario che comunichi in buona fede un sospetto può essere esposto a ritorsioni sulla base della comunicazione effettuata, anche qualora il sospetto si riveli infondato.

Le segnalazioni vanno inoltrate utilizzando l'indirizzo e-mail dedicato o tramite deposito nell'apposita cassetta messa a disposizione a tal fine.

Le segnalazioni possono essere effettuate anche in forma anonima. L'Organismo di Vigilanza agisce in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone coinvolte, nonché la reputazione dei segnalanti.

16. DISPOSIZIONI FINALI

Il Codice è approvato dal Consiglio di Amministrazione della Società e costituisce parte integrante del Modello di Organizzazione Gestione e Controllo adottato da Payback.



Eventuali futuri aggiornamenti, dovuti ad adeguamenti normativi o all'evoluzione/modifica dell'attività della Società, saranno approvati dal Consiglio di Amministrazione e diffusi tempestivamente a tutti i Destinatari.



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

DI

PAYBACK ITALIA S.R.L.

Ai Sensi Del Decreto Legislativo n. 231/2001

"Responsabilità amministrativa della Società"

PAYBACK ITALIA S.R.L.

SEDE LEGALE IN VIALE ALEXANDRE GUSTAVE EIFFEL 15, 00148 ROMA

CODICE FISCALE E REGISTRO IMPRESE ROMA N. 07643140960 - N. ISCRIZIONE AL REA 1331503



INDICE

LA PARTE GENERALE DEL MODELLO	4
1. LA NORMATIVA IN MATERIA DI RESPONSABILITÀ AMMINISTRATIVA D	<u>EGLI</u>
ENTI: IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 E S.M.I.	4
1.1 IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA A CARICO DELLE PERSO	
GIURIDICHE, DELLE SOCIETÀ E DELLE ASSOCIAZIONI (ENTI)	4
1.2 I REATI-PRESUPPOSTO SUI QUALI SI FONDA LA RESPONSABILITÀ DELL'E.	<u>NTE</u> 6
1.3 LE SANZIONI APPLICABILI	7
1.4 L'ADOZIONE DEL MODELLO QUALE ESIMENTE DELLA RESPONSABILITÀ	<u>DEGLI</u>
<u>ENTI</u>	8
2. L'ADOZIONE DEL MODELLO DA PARTE DI PAYBACK ITALIA	11
2.1 OBIETTIVI PERSEGUITI CON L'ADOZIONE DEL MODELLO	11
2.2 PAYBACK ITALIA NEL GRUPPO AMERICAN EXPRESS E RELATIVO MODEL.	LO DI
<u>GOVERNANCE</u>	11
2.3 I PRINCIPI ISPIRATORI E LE LINEE GUIDA PER L'ADOZIONE DEL MODEL	<i>LO</i> 13
2.4 LA STRUTTURA DEL MODELLO E DESTINATARI	15
2.5 LA PROCEDURA DI ADOZIONE E AGGIORNAMENTO DEL MODELLO	16
3. PRINCIPI GENERALI DI COMPORTAMENTO E VALORI ETICI	18
3.1 LE LINEE GUIDA DI CONFINDUSTRIA	18
4. FORMAZIONE E COMUNICAZIONE	19
4.1 SELEZIONE E FORMAZIONE DEL PERSONALE	19
5. IL SISTEMA DISCIPLINARE E I MECCANISMI SANZIONATORI	20
5.1 PRINCIPI GENERALI	20



5.2 MISURE NEI CONFRONTI DEI LAVORATORI DIPENDENTI	21
5.3 MISURE NEI CONFRONTI DEI DIRIGENTI	22
5.4 MISURE NEI CONFRONTI DI PARTNER COMMERCIALI, AGENTI, CONSU COLLABORATORI, FORNITORI, ECC.	
6. L'ORGANISMO DI VIGILANZA	22
6.1 L'INDIPENDENZA E LA STRUTTURA DELL'ORGANISMO DI VIGILANZA	22
6.2 LA NOMINA, DURATA E REVOCA DEI MEMBRI DELL'ORGANISMO DI VIGI	<i>LANZA</i> 23
6.3 I COMPITI E I REQUISITI DELL'ORGANISMO DI VIGILANZA	23
6.4 I POTERI DELL'ORGANISMO DI VIGILANZA	24
6.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO	24
6.6 REPORTING DELL'ORGANISMO NEI CONFRONTI DEGLI ORGANI SOCI	E <i>TARI</i> 26
7. WHISTLEBLOWING	26
ALLEGATO 1 – elenco reati attualmente inclusi nel D.lgs. n. 231/2001	28



La Parte Generale del Modello

1. LA NORMATIVA IN MATERIA DI RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI: IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 E S.M.I.

1.1 IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA A CARICO DELLE PERSONE GIURIDICHE, DELLE SOCIETÀ E DELLE ASSOCIAZIONI (ENTI)

In data 8 giugno 2001 è stato emanato – in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 – il Decreto Legislativo n. 231 (di seguito denominato anche il "**Decreto**" o "**D.Lgs. 231/2001**"), entrato in vigore il 4 luglio successivo, che ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito, ed in particolare:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione anch'essa firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione di funzionari della Comunità Europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Il Decreto recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" per gli illeciti dipendenti da reato.

Il regime di responsabilità si applica a tutti gli Enti con o senza responsabilità giuridica che ispirano la propria gestione a finalità di lucro.

A titolo esemplificativo:

- persone fisiche;
- società di persone, associazioni, enti ed organismi aventi carattere personale;
- società di capitali.

Sono, invece, esclusi dal regime di responsabilità amministrativa:

- gli enti privi di personalità giuridica che svolgono funzioni di rilievo costituzionale;
- lo Stato, gli enti pubblici territoriali e gli enti ed organizzazioni associative che svolgono un pubblico servizio.

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta tuttavia taluni caratteri propri della responsabilità penale, essendo ad esempio rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare ed essendo estese all'ente le garanzie del processo penale.

La responsabilità amministrativa dell'ente stabilisce che:

1. l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:



- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a);
- 2. l'ente non risponde se le persone indicate nel punto 1 hanno agito nell'interesse esclusivo proprio o di terzi.

Oltre all'esistenza degli elementi oggettivi e soggettivi sopra descritti, il D.Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è in definitiva riconducibile ad una "colpa di organizzazione", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione dei reati elencati al successivo paragrafo, da parte dei soggetti individuati nel Decreto.

La responsabilità amministrativa dell'ente è quindi ulteriore e diversa da quella della persona fisica che ha materialmente commesso il reato e sono entrambe oggetto di accertamento nel corso del medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'ente permane anche nel caso in cui la persona fisica autrice del reato non sia identificata o non risulti punibile e nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

La responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma di tentativo (ai sensi dell'art. 26 del D.Lgs. 231/2001), vale a dire quando il soggetto agente compie atti idonei in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica.

In forza dell'articolo 4 del Decreto, l'ente può essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati. In particolare, l'art. 4 del Decreto prevede che gli enti aventi la sede principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, l'ente è perseguibile quando:

- in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica);
- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità ex art. 6 del codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".



In seguito all'entrata in vigore della Legge n. 291 del 14 dicembre 2017 (Legge sul *Whistleblowing*), sono stati inseriti all'interno dell'art. 6 del Decreto tre nuovi commi (comma 2-bis, 2-ter e 2-quater) in virtù dei quali il Modello di Organizzazione, Gestione e Controllo dovrà prevedere:

- uno o più canali che consentano, ai soggetti apicali ed ai loro sottoposti, di presentare segnalazioni circostanziate riguardanti condotte illecite rilevanti ai sensi del Decreto, oppure violazioni del Modello di Organizzazione e Gestione dell'ente di cui siano venuti a conoscenza in ragione delle funzioni svolte;
- almeno un canale alternativo di segnalazione idoneo a garantire con modalità informatiche la riservatezza dell'identità del segnalante;
- il divieto di compiere atti di ritorsione e/o discriminatori diretti e/o indiretti nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- un sistema disciplinare di sanzioni da irrogarsi nei confronti di chi violi le misure predisposte ai fini della tutela del segnalante nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate;
- la possibilità di denunciare all'Ispettorato Nazione del Lavoro l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni;
- la nullità del licenziamento ritorsivo o discriminatorio del soggetto segnalante, nonché la nullità del demansionamento o di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti dello stesso, purché siano ascrivibili a ragioni connesse alla segnalazione stessa.

1.2 I REATI-PRESUPPOSTO SUI QUALI SI FONDA LA RESPONSABILITÀ DELL'ENTE

I reati, dal cui compimento può derivare la responsabilità amministrativa dell'ente, sono quelli espressamente richiamati dal D.Lgs. 231/2001 e successive modifiche ed integrazioni.

Si elencano di seguito le "famiglie di reato" attualmente ricomprese nell'ambito di applicazione del D.Lgs. 231/2001, per il cui testo si rimanda all'Allegato 1 del presente documento:

- 1. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (Art. 24)
- 2. Delitti informatici e trattamento illecito di dati (Art. 24-bis)
- 3. Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009]
- 4. Concussione, induzione indebita a dare o promettere altra utilità e corruzione (Art. 25)
- 5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis)
- 6. Delitti contro l'industria e il commercio (Art. 25-bis.1)
- 7. Reati societari (Art. 25-ter)



- 8. Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater)
- 9. Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1,)
- 10. Delitti contro la personalità individuale (Art. 25-quinquies)
- 11. Reati di abuso di mercato (Art. 25-sexies)
- 12. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-septies)
- 13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies)
- 14. Delitti in materia di violazione del diritto d'autore (Art. 25-novies)
- 15. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies)
- 16. Reati ambientali (Art. 25-undecies)
- 17. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies)
- 18. Reati transnazionali (L. n. 146/2006)

1.3 LE SANZIONI APPLICABILI

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale, che la esercita con le garanzie proprie del procedimento penale. L'accertamento della responsabilità può concludersi con l'applicazione di sanzioni gravi e pregiudizievoli per la vita dell'ente stesso, quali:

- a) sanzioni pecuniarie;
- b) sanzioni interdittive;
- c) confisca;
- d) pubblicazione della sentenza.

La sanzione pecuniaria è sempre applicabile, si prescrive nel termine di 5 anni dalla consumazione del reato – presupposto e non può essere inferiore a 25.882 euro né superiore a 1.549.371 euro.

In particolare le sanzioni interdittive, che si applicano in relazione ai reati per i quali sono espressamente previste, possono comportare importanti restrizioni all'esercizio dell'attività di impresa dell'ente, quali:

- a) interdizione dall'esercizio dell'attività;
- b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;



- c) divieto di contrattare con la Pubblica Amministrazione, salvo che per le prestazioni del pubblico servizio;
- d) esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- e) divieto di pubblicizzare beni o servizi.

Tali misure possono essere applicate all'ente anche in via cautelare, e dunque prima dell'accertamento nel merito in ordine alla sussistenza del reato e dell'illecito amministrativo che da esso dipende, nell'ipotesi in cui si ravvisi l'esistenza di gravi indizi tali da far ritenere la responsabilità dell'ente, nonché il pericolo di reiterazione dell'illecito.

Nell'ipotesi in cui il giudice ravvisi l'esistenza dei presupposti per l'applicazione di una misura interdittiva a carico di un ente che svolga attività di interesse pubblico ovvero abbia un consistente numero di dipendenti, lo stesso potrà disporre che l'ente continui a operare sotto la guida di un commissario giudiziale.

Le diverse tipologie di sanzioni previste ai sensi del Decreto sono applicabili quando:

- il reato è commesso da un soggetto in posizione apicale e l'ente abbia tratto dal reato un profitto di rilevante entità:
- il reato è commesso da un soggetto sottoposto all'altrui direzione e la commissione del reato sia stata cagionata da gravi carenze organizzative.

Con la pronuncia della sentenza di condanna il giudice dispone la confisca del prezzo o del profitto del reato.

Ai sensi dell'art. 26 del Decreto, nell'ipotesi di commissione del reato nella forma del tentativo:

- le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà;
- l'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

1.4 L'ADOZIONE DEL MODELLO QUALE ESIMENTE DELLA RESPONSABILITÀ DEGLI ENTI

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da soggetti apicali, non risponda a titolo di responsabilità amministrativa qualora dimostri che:

- a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (c.d. "Organismo di Vigilanza", nel seguito anche "**Organismo**" o "**OdV**");
- c) le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.



Nel caso in cui il reato sia stato commesso da soggetti sottoposti alla direzione o alla vigilanza del personale apicale, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, è esente da responsabilità se risultano integrate le condizioni di cui all'art. 6 del Decreto.

In tal senso il Decreto fornisce specifiche indicazioni in merito alle esigenze cui i Modelli Organizzativi devono rispondere:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
- prevedere specifici "protocolli" diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'OdV.;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Tuttavia la mera adozione di un Modello Organizzativo, non è di per sé sufficiente ad escludere detta responsabilità, essendo necessario che il modello sia effettivamente ed efficacemente attuato. In particolare ai fini di un efficace attuazione del Modello, il Decreto richiede una serie di interventi organizzativi, quali:

- definizione dei reati;
- redazione di un codice etico (di seguito anche il "Codice Etico" o il "Codice");
- mappatura delle aree e delle attività soggette al rischio di commissione dei rati previsti dal Decreto:
- evidenziazione dei processi sensibili, che necessitino di adeguati presidi, e relativa graduazione secondo la diversa esposizione al rischio di reato;
- disciplina dei processi sensibili e dei meccanismi di controllo, nonché definizione delle modalità di segnalazione e formazione, da parte del personale, di eventuali criticità;
- informazione al proprio personale del contenuto del Codice Etico e del Modello;
- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso;
- costituzione di un apposito Organismo che vigili sul corretto funzionamento del Modello.



Nel caso in cui il reato sia commesso dai soggetti apicali, il Decreto prevede l'applicazione del meccanismo di inversione dell'onere della prova, per cui la responsabilità dell'Ente si presume, salvo che questo dia prova della sua estraneità al reato e di aver attuato il Modello di Organizzazione e Gestione.

Nel caso in cui si tratti di soggetti sottoposti, invece, gli organi accertatori dovranno provare che la commissione del reato derivi dall'inosservanza degli obblighi di direzione e vigilanza da parte dei vertici aziendale, nonché la mancata adozione e attuazione del Modello.



2. L'ADOZIONE DEL MODELLO DA PARTE DI PAYBACK ITALIA

2.1 OBIETTIVI PERSEGUITI CON L'ADOZIONE DEL MODELLO

Payback Italia S.r.l. (di seguito "Payback Italia" o la "Società") si dota del presente Modello di organizzazione, gestione e controllo (di seguito anche "Modello 231" o "Modello") con l'obiettivo di prevenire la commissione – nell'interesse o a vantaggio della stessa – dei reati riconducibili al Decreto (cd. reati presupposto) da parte di esponenti della Società, apicali o sottoposti all'altrui direzione.

Scopo del Modello è quello di sensibilizzare tutti i soggetti che operano in nome e per conto della Società, con la finalità di costruire un sistema strutturato e organico di procedure e di attività di controllo, volte a prevenire la commissione dei reati presupposto.

In particolare, il Modello si propone di:

- creare la consapevolezza di poter incorrere in un illecito passibile di sanzioni, sul piano penale e amministrativo, sia nei confronti di coloro che operano in nome e per conto della Società, sia nei confronti dell'azienda stessa;
- ribadire che le suddette forme di comportamento illecito sono contrarie alle disposizioni di legge, nonché ai principi etico-sociali;
- consentire alla Società di intervenire tempestivamente, al fine di prevenire e contrastare la commissione dei reati.

Nella predisposizione del presente documento la Società ha opportunamente tenuto presente, oltre le prescrizioni del Decreto, le Linee Guida predisposte da Confindustria.

2.2 PAYBACK ITALIA NEL GRUPPO AMERICAN EXPRESS E RELATIVO MODELLO DI GOVERNANCE

Payback Italia, con sede legale a Roma, fa parte del Gruppo American Express (il "**Gruppo**"), gruppo globale che opera prevalentemente nei servizi finanziari di pagamento e di viaggio e, in particolare, la Società è affiliata ad American Express Services Europe Limited (AESEL). Nello specifico, la Società risulta partecipata al 100% dalla Loyalty Partner Holdings B.V., con sede in Olanda, società a sua volta partecipata al 100% dalla American Express Continental LLC, sita negli Stati Uniti.

La Società opera, con decorrenza dal 2013, nel campo dell'organizzazione, gestione, promozione e sviluppo, in Italia, nella Repubblica di San Marino e nello Stato della Città del Vaticano, di programmi di fidelizzazione, compresi concorsi e operazioni a premio, anche in combinazione tra loro, nonché della prestazione di servizi di marketing, creazione e gestione di *database* per rivenditori, fornitori di prodotti e/o servizi e produttori di beni di largo consumo. La Società svolge inoltre tutte quelle attività accessorie e strumentali a quelle principali ritenute utili per il conseguimento dello scopo sociale. ¹

-

¹ Lo Statuto di Payback dispone che: "La società ha altresì per oggetto l'attività di creazione e gestione di piattaforme informatiche a servizio di programmi di fidelizzazione e/o promozionali; la fornitura, anche per via telematica, di servizi di informazione economica e commerciale a favore delle imprese e dei consumatori; la fornitura di servizi di pubblicità commerciale a mezzo reti telematiche ed ogni altro mezzo di comunicazione; la fornitura a favore di qualsivoglia soggetto di servizi di marketing connessi o non connessi ai programmi di fidelizzazione della Società anche attraverso lo svolgimento di attività di "tele-marketing" e "tele-selling", nonché di servizi di consulenza correlati; la fornitura a favore di qualsivoglia



La *corporate governance* di Payback Italia, essenzialmente basata sul modello tradizionale di gestione, è così articolata:

Assemblea dei soci, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo statuto; a tal riguardo l'Assemblea è chiamata a deliberare:

- sulle decisioni relative alle modificazioni dell'atto costitutivo ivi comprese fusioni e scissioni (salvo, nei casi consentiti, la competenza del Consiglio di Amministrazione nelle ipotesi di cui agli artt. 2505 e 2505-bis c.c., quali richiamati anche dall'art. 2506-ter c.c., e 2481 c.c.);
- sulle decisioni di compiere operazioni che comportano una sostanziale modificazione dell'oggetto sociale e una rilevante modificazione dei diritti dei soci nonché l'assunzione di partecipazioni da cui derivi responsabilità illimitata per le obbligazioni delle società partecipate;
- sulle decisioni in merito allo scioglimento anticipato della Società, alla nomina o revoca dei liquidatori ed alla determinazione dei relativi poteri;
- su ogni altra determinazione di competenza dei soci riservata in via inderogabile dalla legge o dal presente statuto alla assemblea, ovvero ogni altra determinazione per la quale uno o più amministratori o tanti soci che rappresentino almeno un terzo del capitale richiedano la forma assembleare.

Consiglio di Amministrazione, composto da 5 membri compreso il Presidente, è investito dei più ampi poteri per l'amministrazione ordinaria e straordinaria della Società, con facoltà di compiere tutti gli atti opportuni per l'attuazione ed il raggiungimento degli scopi sociali, ad esclusione di quelli che la legge o lo statuto riserva alla preventiva approvazione dell'Assemblea, o comunque dei soci.

Presidente del Consiglio di Amministrazione e Amministratore Delegato ai quali spetta, in via disgiunta, la rappresentanza legale della Società di fronte ai terzi e in giudizio;

Collegio Sindacale o Sindaco Unico cui, ai sensi dell'art. 2403 c.c., spetta il compito di vigilare: a) sull'osservanza della legge e dallo statuto nonché sul rispetto dei principi di corretta amministrazione; b) sull'adeguatezza della struttura organizzativa della Società, del sistema di controllo interno e del

soggetto di servizi o strumenti per l'analisi dati connessi o non connessi ai programmi di fidelizzazione della Società, nonché di servizi di consulenza correlati; la fornitura a favore di qualsivoglia soggetto di ricerche di mercato e analisi del comportamento di acquisto del consumatore; la fornitura a favore di qualsivoglia soggetto di servizi di gestione di programmi o iniziative volte ad incentivare la clientela; la fornitura a favore di qualsivoglia soggetto in "outsourcing" di iniziative e/o programmi di fidelizzazione nonché ogni attività di "e-commerce" di beni e servizi attraverso reti telematiche e la prestazione di servizi correlati.

La società potrà inoltre svolgere tutte quelle attività accessorie e strumentali a quelle principali ritenute utili per il conseguimento dello scopo sociale.

La società potrà inoltre: (i) effettuare qualsiasi operazione monetaria, immobiliare, commerciale, industriale, finanziaria, di credito, di leasing e ipotecaria che gli amministratori o i soci possano ritenere necessaria e utile per il conseguimento dell'oggetto sociale; (ii) ottenere finanziamenti e prestiti, anche garantiti da ipoteca, al fine di finanziare le attività della società; (iii) acquisire e possedere, direttamente e/o indirettamente, in Italia e all'estero, azioni, quote e partecipazioni in imprese industriali, finanziarie o commerciali nonché in altre società, consorzi, associazioni in partecipazione, gruppi di imprese, associazioni; e (iv) prestare garanzie in favore di altri enti o persone.

Il tutto con esclusione comunque dell'attività di concessione di finanziamenti nei confronti del pubblico e di ogni altra attività riservata per legge a differenti categorie di soggetti."



sistema amministrativo contabile, anche in riferimento all'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione.

Società di revisione, incaricata a svolgere l'attività di revisione legale dei conti.

2.3 I PRINCIPI ISPIRATORI E LE LINEE GUIDA PER L'ADOZIONE DEL MODELLO

L'adozione del Modello e la sua implementazione contribuiscono a migliorare la gestione del sistema di controllo interno, favorendo il consolidarsi di una cultura aziendale che valorizzi i principi di trasparenza, eticità, correttezza anche a beneficio dell'immagine del Gruppo.

In particolare, il Modello è stato adottato tenendo conto:

- del Codice di condotta American Express;
- delle linee di condotta e procedure American Express;
- delle procedure locali;
- del sistema di controllo e gestione dei rischi in essere;
- delle indicazioni delle Linee guida Confindustria;
- delle best practices in materia di costruzione dei Modelli 231;
- della normativa penale applicabile in materia di responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

A tal fine, devono essere perseguiti i seguenti presidi organizzativo-gestionali di carattere generale:

Norme comportamentali

I codici comportamentali devono descrivere le regole generali di condotta a presidio delle attività svolte.

Definizioni di ruoli e responsabilità

- La regolamentazione interna deve declinare ruoli e responsabilità delle strutture organizzative a tutti i livelli, descrivendo in maniera omogenea, le attività proprie di ciascuna struttura.
- Tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Protocolli e norme interne

- Le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso gli strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato.
- Deve essere individuato e formalizzato un Responsabile per ciascuna attività sensibile, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa.

Segregazione dei compiti



- All'interno di ogni processo aziendale rilevante, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla.
- Non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano l'evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

Poteri autorizzativi e di firma

- Deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando l'impresa e manifestando la sua volontà.
- I poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate.
- Le procure devono essere coerenti con il sistema interno delle deleghe.
- Devono essere previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni.
- Il processo di attribuzione delle deleghe deve identificare, tra l'altro:
 - o i requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
 - o l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;
 - o le modalità operativa di gestione degli impegni di spesa;
- Le deleghe sono attribuite secondo i principi di:
 - o autonomia decisionale e finanziaria del delegato;
 - o idoneità tecnico-professionale del delegato;
 - o disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- Nell'ambito dei protocolli o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità). La descrizione dei controlli deve, inoltre, esplicitare:
 - o l'input, che rappresenta l'informazione chiave da sottoporre al controllo;
 - o lo standard di riferimento, ossia l'elemento di raffronto dell'input che consente di identificare situazioni anomale e di attivare gli opportuni processi di correzione (es. tempistiche, politiche, normative, ecc.);
 - o l'attività di controllo, che rileva l'input e lo confronta con uno o più standard di riferimento;
 - o l'attività di correzione, che viene eseguita in caso di rilevazione di anomalie;
 - o l'output, del processo di controllo.



- La documentazione afferente alle attività sensibili deve essere adeguatamente formalizzata e riportare la data di compilazione, presa visione del documento e la firma riconoscibile del compilatore/supervisore; la stessa deve essere archiviata in luogo idoneo alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti.
- Devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate.
- Il responsabile dell'attività deve produrre e mantenere adeguati report di monitoraggio che contengano evidenza dei controlli effettuati e di eventuali anomalie.
- Deve essere prevista, laddove possibile, l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano. Il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni.
- I documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili sono archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza.
- L'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne o a loro delegato, al Collegio Sindacale od organo equivalente o ad altri organi di controllo interno, alla Società di Revisione e all'Organismo di Vigilanza.

2.4 LA STRUTTURA DEL MODELLO E DESTINATARI

Il presente Modello è costituito da una Parte Generale che contiene:

- una sintetica descrizione del quadro normativo, integrata dal dettaglio delle fattispecie di reato (Allegato 1);
- una sintetica descrizione del contesto organizzativo di Payback Italia e del processo di definizione del Modello;
- i principi generali di comportamento e i valori etici;
- le modalità di selezione e formazione del personale;
- le sanzioni applicabili in caso di violazioni delle regole e delle prescrizioni contenute nel Modello;

e una Parte Speciale che:

- individua, previa descrizione delle diverse fattispecie di reato-presupposto, le attività aziendali nel cui ambito possono essere commessi i reati rilevanti ai sensi del Decreto;
- evidenzia i comportamenti che possono comportare l'applicazione delle sanzioni previste dal Decreto;



• definisce i principi comportamentali e di controllo a presidio dei rischi individuati.

In particolare, il Modello si articola in:

- o Parte Generale
- Codice Etico
- Allegato alla Parte Generale (Allegato 1)
- o Regolamento dell'Organismo di Vigilanza
- o una Parte Speciale, composta dalle seguenti sedici Sezioni:
- Sezione A: indebita percezione di erogazioni, truffa in danno dello Stato o di un Ente Pubblico
 o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un
 Ente Pubblico;
- Sezione B: delitti informatici;
- Sezione C: delitti di criminalità organizzata;
- Sezione D: reati contro la pubblica amministrazione;
- Sezione E: reati contro la fede pubblica;
- Sezione F: delitti contro l'industria e il commercio;
- Sezione G: reati societari;
- Sezione H: i reati contro la personalità individuale;
- Sezione I: reati connessi alla violazione delle norme in materia di salute e sicurezza sul lavoro;
- Sezione J: reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di illecita provenienza e autoriciclaggio;
- Sezione K: delitti in materia di violazioni del diritto della proprietà intellettuale;
- Sezione L: reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria;
- Sezione M: reati ambientali;
- Sezione N: reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare;
- Sezione O: reati di razzismo e xenofobia;

Si considerano soggetti destinatari delle prescrizioni del Modello, ai sensi del Decreto e nell'ambito delle rispettive competenze, i componenti degli organi sociali, il management e i dipendenti di Payback Italia, nonché tutti coloro che operano per il conseguimento dello scopo e degli obiettivi della Società (di seguito, i "**Destinatari**").

2.5 LA PROCEDURA DI ADOZIONE E AGGIORNAMENTO DEL MODELLO

Il processo di costruzione del Modello può essere strutturato nelle seguenti fasi:



a) Mappatura preliminare delle attività sensibili

Ai sensi dell'art. 6, comma 2, lettera a) del D.Lgs. 231/2001, il Modello deve garantire l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati di cui al suddetto Decreto, conseguentemente definiti come "sensibili".

Nello specifico, sono state svolte le seguenti attività:

- raccolta della documentazione relativa alla struttura societaria e organizzativa;
- analisi della suddetta documentazione, al fine di approfondire il modello di *governance* e di *business*;
- *case history* di eventuali procedimenti penali, civili, o amministrativi connessi alla normativa ex d.lgs. 231/2001;
- definizione delle relative responsabilità a ciascuna funzione anche attraverso interviste con i principali responsabili delle funzioni aziendali/business unit;
- individuazione preliminare dei processi e delle attività sensibili ai sensi del decreto;
- definizione preliminare delle funzioni/business unit responsabili dei processi sensibili individuati.

b) Identificazione dei key officer (process owner e co-work) e analisi dei processi e delle attività sensibili

La fase operativa di cui sopra mira a identificare le risorse che abbiano una conoscenza approfondita dei processi e delle attività sensibili, nonché dei relativi meccanismi di controllo in essere.

In particolare, i *key officer* vengono a coincidere con le persone di più alto livello organizzativo, in grado di fornire informazioni dettagliate sui processi e le attività afferenti le singole unità, al fine di definire al meglio il sistema di controlli e di gestione dei rischi in essere.

In particolare, la presente fase operativa ha previsto la predisposizione di una serie di interviste con i *key officer*, volte a carpire le informazioni necessarie a comprendere:

- i processi e le attività svolte;
- le unità, i soggetti interni ed esterni coinvolti (process owner e co-work);
- i relativi ruoli e responsabilità;
- il sistema dei controlli esistenti;
- i rischi di *compliance*;
- la valutazione dei rischi di compliance.

In seguito, sono state condivise con i *key officer* le risultanze delle relative interviste e, tramite la sintetizzazione delle informazioni acquisite e delle criticità individuate, è stata formalizzata la mappa dei processi e delle attività sensibili (di seguito anche "Matrice di analisi di rischio 231" o "Matrice 231").

Per quanto concerne la rilevazione del sistema di controllo, sono stati individuati i seguenti principi:



- applicazione delle policy di American Express;
- tracciabilità ex post delle transazioni tramite adeguati supporti documentali;
- segregazione dei compiti;
- esistenza delle deleghe formalizzate coerenti con le responsabilità organizzative.

c) Gap analysis

La fase di cui sopra prevede, attraverso una comparazione del sistema organizzativo e di controllo esistente e un modello astratto fondato sulla disciplina di cui al Decreto, l'individuazione:

- dei requisiti organizzativi idonei a prevenire i reati previsti ai sensi del Decreto;
- delle eventuali azioni di miglioramento del Modello.

d) Definizione del Modello

La suddetta fase, supportata dai risultati delle fasi precedenti, ha previsto la definizione del Modello, personalizzandolo rispetto alla realtà aziendale.

L'eventuale aggiornamento del Modello compete al Consiglio di Amministrazione, che lo eserciterà mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D.Lgs. 231/2001.

L'Organismo di Vigilanza, invece, dovrà verificare l'eventuale necessità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio di Amministrazione.

In ogni caso, il Modello deve essere tempestivamente modificato ed integrato dal Consiglio di Amministrazione, anche su proposta e previa consultazione dell'Organismo di Vigilanza, quando siano intervenute:

- violazioni ed elusioni delle prescrizioni in esso contenute che ne abbiano evidenziato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- significative modificazioni all'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa;
- modifiche normative ed evoluzioni giurisprudenziali.

3. PRINCIPI GENERALI DI COMPORTAMENTO E VALORI ETICI

3.1 LE LINEE GUIDA DI CONFINDUSTRIA

Il Modello di Payback Italia è stato strutturato sulla base delle "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001" elaborate da Confindustria, oltre che sulla base del Codice di Condotta di American Express.



I principi etici previsti dalle suddette Linee guida prevedono:

- il rispetto delle norme del codice penale, in materia di tutela della concorrenza, delle attività di intermediario finanziario, della salute e sicurezza sul lavoro, dell'ambiente;
- ogni operazione e transazione deve essere correttamente registrata, autorizzata, legittima, coerente e congrua;
- divieto di fornire doni o denaro a dirigenti, funzionari o dipendenti della Pubblica Amministrazione o a loro parenti, salvo che siano di modico valore;
- divieto di proporre opportunità di impiego o commerciali che possano avvantaggiare dipendenti della Pubblica Amministrazione;
- divieto di offrire omaggi, salvo quelli previsti dalle procedure aziendali;
- divieto di sollecitare la comunicazione di informazioni riservate idonee a compromettere l'integrità di entrambe le parti.

4. FORMAZIONE E COMUNICAZIONE

4.1 SELEZIONE E FORMAZIONE DEL PERSONALE

La fase di selezione del personale viene svolta tenendo conto di uno specifico sistema di valutazione del personale ispirato a criteri di imparzialità, merito e professionalità, che tenga altresì conto delle esigenze aziendali in relazione all'applicazione del Decreto 231.

In particolare, nella lettera di assunzione viene inserita idonea informativa illustrante il Modello Organizzativo adottato ai sensi del Decreto.

La formazione del personale, finalizzata all'attuazione del Modello ed alla sua diffusione nel contesto aziendale, prevede dei corsi di formazione a frequenza obbligatoria la cui qualità è monitorata e accertata dall'Organismo di Vigilanza.

La formazione del personale viene articolata su tre livelli di seguito elencati:

- a) Organismo di Vigilanza: seminario iniziale volto alla illustrazione delle procedure aziendali interne e alla descrizione della struttura e delle dinamiche aziendali;
- b) personale direttivo e con funzioni di rappresentanza della Società: seminario iniziale esteso ai neo assunti con relativo aggiornamento annuale;
- c) altro personale: con cadenza periodica, la Società propone un piano di formazione dell'Organismo di Vigilanza, che ne verifica la qualità e i contenuti.

Il suddetto piano di formazione prevede diverse tipologie di interventi, predisposti a seconda della collocazione aziendale degli esponenti aziendali. Il mancato rispetto dei citati obblighi da parte degli esponenti aziendali con funzione di vigilanza comporta l'applicazione di sanzioni parametrate alla posizione ricoperta all'interno della Società.



Infine, i soggetti esterni che intrattengono rapporti contrattuali di qualsiasi natura con la Società vengono informati che Payback Italia si è dotata di un Modello Organizzativo e di specifiche procedure in tema di Decreto 231, nonché di un Codice Etico rivolto anche ai fornitori e ai collaboratori esterni.

5. IL SISTEMA DISCIPLINARE E I MECCANISMI SANZIONATORI

5.1 PRINCIPI GENERALI

La definizione di un sistema sanzionatorio, applicabile in caso di violazione delle disposizioni del presente Modello, costituisce condizione necessaria per garantire l'efficace attuazione del Modello stesso, nonché presupposto imprescindibile per consentire alla Società di beneficiare dell'esimente dalla responsabilità amministrativa (ex art. 6, comma 2, lettera e) del Decreto).

L'applicazione delle sanzioni disciplinari prescinde dall'instaurazione e dagli esiti di un procedimento penale eventualmente avviato nei casi in cui la violazione integri un'ipotesi di reato rilevante ai sensi del D.Lgs. 231/2001.

Il sistema disciplinare costituisce parte integrante del Modello e, ai sensi dell'art. 2106 c.c., integra il Contratto Collettivo Nazionale.

Le sanzioni comminabili sono diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché del rilievo e gravità della violazione commessa e del ruolo e responsabilità dell'autore. Più in particolare, le sanzioni comminabili sono diversificate tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

In generale, le violazioni possono essere ricondotte ai seguenti comportamenti:

- a) comportamenti che integrano una mancata attuazione colposa delle prescrizioni del Modello e/o del Codice Etico ivi comprese direttive, procedure o istruzioni aziendali;
- b) comportamenti che integrano una trasgressione dolosa delle prescrizioni del Modello e/o del Codice Etico tale da compromettere il rapporto di fiducia tra l'autore e la Società in quanto preordinata in modo univoco a commettere un reato.

nonché classificate come segue:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, delle previsioni del Modello o delle procedure stabilite per l'attuazione del medesimo e del Codice Etico;
- la redazione, eventualmente in concorso con altri, di documentazione alterata o non veritiera;
- l'agevolazione, mediante condotta omissiva, di violazioni del Modello e del Codice Etico e della redazione da parte di altri, di documentazione alterata o non veritiera;
- l'omessa redazione della documentazione prevista dal Modello o dalle procedure stabilite per l'attuazione dello stesso



Le sanzioni specifiche saranno applicate in base ai seguenti criteri generali:

- a. elemento soggettivo della condotta;
- b. rilevanza degli obblighi violati;
- c. gravità dei pericoli creati;
- d. entità del danno creato alla società dall'eventuale applicazione delle sanzioni;
- e. livello di responsabilità gerarchica e/o tecnica;
- f. circostanze aggravanti o attenuanti
- g. condivisione di responsabilità con altri lavoratori.

5.2 MISURE NEI CONFRONTI DEI LAVORATORI DIPENDENTI

In relazione al personale dipendente, la Società si attiene alle prescrizioni di cui all'art. 7 della Legge 300/1970 (Statuto dei lavoratori) ed alle previsioni contenute nel Contratto Collettivo Nazionale di Lavoro applicabile, sia con riguardo alle sanzioni comminabili che alle modalità di esercizio del potere disciplinare.

L'inosservanza - da parte del personale dipendente - delle disposizioni del Modello e/o del Codice Etico, nonché di tutta la documentazione che di essi forma parte, costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro *ex* art. 2104 cod. civ. ed illecito disciplinare.

Alla notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. Una volta accertata la violazione, sarà irrogata all'autore una sanzione disciplinare proporzionata alla gravità della violazione commessa.

Sulla base del suddetto principio di proporzionalità, occorre valutare:

- l'intenzionalità del comportamento;
- il grado di negligenza, imprudenza o imperizia;
- la posizione funzionale e le mansioni del lavoratore;
- il comportamento del lavoratore e l'eventuale reiterazione della condotta da censurare.

Al personale dipendente possono essere comminate le sanzioni previste dall'art. 225 del CCNL, quali:

- i) rimprovero verbale;
- ii) ammonizione scritta;
- iii) multa in misura non superiore a quattro ore di retribuzione;
- iv) sospensione dal lavoro e dalla retribuzione fino ad un massimo di dieci giorni;
- v) licenziamento senza preavviso.



È inteso che saranno seguite tutte le disposizioni e le garanzie previste dal CCNL in materia di procedimento disciplinare; in particolare si rispetterà:

- l'obbligo della previa contestazione dell'addebito al dipendente con indicazione dei fatti costitutivi dell'infrazione e del termine dal ricevimento della contestazione entro cui il dipendente potrà presentare le proprie giustificazioni e dell'audizione di quest'ultimo in ordine alla sua difesa;
- l'obbligo di non adottare il provvedimento disciplinare, se più grave del rimprovero verbale, prima che sia trascorso il termine minimo previsto dall'art. 7 dello Statuto dei Lavoratori dalla contestazione per iscritto dell'addebito, nel corso del quale il lavoratore può presentare le proprie giustificazioni;
- il lavoratore può presentare le proprie giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'Associazione sindacale cui aderisce o conferisce mandato, ovvero di un componente la RSU.
- l'obbligo di comunicazione dell'adozione del provvedimento disciplinare per iscritto entro e non oltre i termini massimi previsti dai rispettivi CCNL dalla scadenza del termine assegnato al dipendente per la presentazione delle sue giustificazioni. In caso contrario, il procedimento disciplinare è definito con l'archiviazione.

5.3 MISURE NEI CONFRONTI DEI DIRIGENTI

In caso di violazione, da parte di Dirigenti, delle procedure interne previste dal presente Modello o di adozione, nell'espletamento di attività nelle aree a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti Industriali. Laddove la violazione sia tale da far venir meno il rapporto di fiducia, la sanzione è individuata nel licenziamento per giusta causa.

5.4 MISURE NEI CONFRONTI DI PARTNER COMMERCIALI, AGENTI, CONSULENTI, COLLABORATORI, FORNITORI, ECC.

Nei contratti stipulati con i soggetti di cui sopra, devono essere inserite specifiche clausole in base alle quali la violazione delle disposizioni e delle regole di comportamento previste dal Decreto, dal Codice Etico e dal Modello potrà determinare la risoluzione del rapporto contrattuale.

6. L'ORGANISMO DI VIGILANZA

6.1 L'INDIPENDENZA E LA STRUTTURA DELL'ORGANISMO DI VIGILANZA

L'art. 6, comma 1, del Decreto prevede che la funzione di vigilare e di curare l'aggiornamento del Modello sia affidata ad un Organismo di Vigilanza (di seguito, anche "**OdV**" o l'"**Organismo**") interno alla Società che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

Il Modello predisposto deve garantire che l'Organismo assicuri:



- autonomia;
- indipendenza;
- professionalità;
- continuità di azione

Payback Italia considera necessaria la presenza di un OdV collegiale, composto da tre membri, con relativo affidamento della carica di presidente ad un membro esterno, a tutela dell'autonomia e dell'indipendenza dell'Organo stesso.

6.2 LA NOMINA, DURATA E REVOCA DEI MEMBRI DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione della Società e dura in carica per un periodo di un anno dalla nomina.

Costituiscono cause di ineleggibilità e decadenza dei componenti dell'OdV:

- aver ricoperto funzioni di amministratore esecutivo, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
- aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero di applicazione della pena su richiesta (cosiddetto "patteggiamento"), in Italia o all'estero, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex Decreto 231;
- aver riportato una sentenza di condanna, anche non passata in giudicato, ovvero di "patteggiamento" a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

È altresì motivo di decadenza con effetto immediato il venir meno, nel corso del periodo di carica, dei requisiti che hanno determinato l'individuazione dei componenti stessi all'atto delle nomine in virtù della carica societaria o del ruolo organizzativo rivestito.

Costituiscono cause di revoca dei componenti dell'OdV:

- l'omessa o insufficiente vigilanza da parte dell'OdV risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del Decreto 231 ovvero da sentenza di applicazione della pena su richiesta (c.d. patteggiamento);
- il grave inadempimento delle funzioni e/o dei poteri dell'Organismo di Vigilanza.

In caso di revoca, sostituzione, dimissioni di uno dei componenti dell'OdV, il Consiglio di Amministrazione provvede tempestivamente alla sua sostituzione.

6.3 I COMPITI E I REQUISITI DELL'ORGANISMO DI VIGILANZA

Le attività dell'OdV ricomprendono:

- vigilanza sul funzionamento del Modello Organizzativo e sull'osservanza da parte dei Destinatari:
- disamina in merito all'adeguatezza del Modello;



- analisi circa il mantenimento dei requisiti di funzionalità del Modello;
- vigilanza sulla diffusione all'interno della Società della conoscenza, comprensione e dell'osservanza del Modello:
- aggiornamento del Modello in relazione all'evolversi della struttura organizzativa, attraverso proposte di adeguamento del Modello e relativo *follow-up*, mirato a verificare la funzionalità delle proposte.

Per garantire lo svolgimento delle attività di cui sopra, l'Amministratore Delegato dispone affinché l'OdV abbia accesso alle procedure aziendali ogni volta che esse vengono emanate, nonché alle delibere di delega delle attribuzioni del Consiglio di Amministrazione a suoi componenti.

Quando lo ritiene opportuno, l'OdV si avvale anche di professionisti esterni per l'accertamento di fatti che sono potenzialmente idonei a costituire violazione del Modello Organizzativo, dandone preventiva informazione al Presidente e all'Amministratore Delegato.

6.4 I POTERI DELL'ORGANISMO DI VIGILANZA

Per l'esecuzione delle attività di propria competenza l'Organismo di Vigilanza può procedere a:

- atti di ispezione;
- atti di controllo;
- accesso ad atti aziendali;
- accesso ad informazioni o dati;
- accesso a procedure e protocolli operativi;
- accesso a dati contabili;
- accesso ad ogni altro dato, atto o informazione ritenuti utili.

Al fine di coadiuvare la definizione e lo svolgimento delle attività di competenza, l'OdV si avvale delle Funzioni *Internal Audit, Compliance, Operational Risk*, nonché dei Delegati in materia di Sicurezza sul lavoro e della funzione preposta per la gestione dei rischi ambientali. Con riferimento alle attività concernenti il monitoraggio, il controllo e la consulenza, l'OdV può servirsi del personale della Società o di consulenti specialistici.

6.5 FLUSSI INFORMATIVI NEI CONFRONTI DELL'ORGANISMO

Il Decreto enuncia (art. 6 comma 2 lettera d.), tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza.

Il personale dipendente è tenuto ad informare, mediante apposite segnalazioni, l'OdV delle possibili violazioni e/o dei comportamenti non conformi a quanto stabilito dal Modello Organizzativo, mediante i seguenti canali di comunicazione:

- casella di posta elettronica dedicata;
- posta tradizionale, all'indirizzo Organismo di Vigilanza 231, in Italia Viale Alexandre Gustave Eiffel 15 00148 Roma.



Le segnalazioni avverranno come di seguito:

- se un esponente aziendale desidera effettuare una segnalazione, deve riferire al suo diretto superiore, il quale canalizza la segnalazione all'OdV;
- l'OdV valuta le segnalazioni ricevute, motivando per iscritto eventuali rifiuti di procedere ad un'indagine interna;
- l'OdV non è tenuto a prendere in considerazione le segnalazioni anonime che appaiano irrilevanti o non circostanziate;
- le segnalazioni potranno essere in forma scritta e l'OdV garantirà i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza del segnalante;
- i terzi, i collaboratori e i fornitori potranno fare segnalazioni direttamente all'OdV;
- è prevista l'istituzione di un canale informativo dedicato da parte dell'OdV di Payback Italia, con l'obiettivo di facilitare il flusso di segnalazioni e di risolvere eventuali situazioni dubbie circa l'ambito di applicazione del Modello.

L'Organismo di Vigilanza deve obbligatoriamente ricevere tutte le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, tributaria o da qualsiasi altra autorità, anche amministrativa, che vedano il coinvolgimento della Società o di soggetti apicali, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto, fatti salvi gli obblighi di riservatezza e segretezza legalmente imposti;
- richieste di informazioni o invio di prescrizioni, relazioni o lettere da parte delle Autorità di Vigilanza (es. Banca d'Italia, Consob, Autorità per la protezione dei dati personali), ed ogni altra documentazione che scaturisce da attività di ispezione delle stesse svolte e rientranti negli ambiti di pertinenza del D.Lgs. 231/2001;
- comunicazioni all'Autorità Giudiziaria che riguardano potenziali o effettivi eventi illeciti che possono essere riferiti alle ipotesi di cui al D.Lgs. 231/2001;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- esiti delle attività di controllo svolte dai responsabili delle diverse funzioni aziendali dalle quali siano emersi fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto o del Modello:
- modifiche nel sistema delle deleghe e delle procure, modifiche statutarie o modifiche dell'organigramma aziendale;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- segnalazione di infortuni gravi (incidenti mortali o con prognosi superiore a 40 giorni) occorsi a dipendenti, appaltatori e/o collaboratori presenti nei luoghi di lavoro della Società.



Tutte le informazioni, la documentazione e le segnalazioni raccolte nell'espletamento dei compiti istituzionali devono essere archiviate e custodite, per almeno cinque anni, dall'Organismo di Vigilanza, avendo cura di mantenere riservati i documenti e le informazioni acquisite, anche nel rispetto della normativa sulla privacy.

6.6 REPORTING DELL'ORGANISMO NEI CONFRONTI DEGLI ORGANI SOCIETARI

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello 231, all'emersione di eventuali aspetti critici e comunica l'esito delle attività svolte nell'esercizio dei compiti assegnati. Sono previste le seguenti linee di riporto:

- continuativa, nei confronti dei legali rappresentanti, il quale informa il Consiglio di Amministrazione nell'ambito dell'informativa sull'esercizio delle deleghe conferite;
- semestrale, nei confronti dei legali rappresentanti e del Collegio Sindacale; a tale proposito è predisposta una relazione semestrale relativa all'attività svolta, con evidenza dell'esito delle attività di vigilanza effettuate e delle eventuali innovazioni legislative in materia di responsabilità amministrativa degli enti registratesi nel periodo; in tale occasione, sono organizzati incontri per discutere dei temi trattati nella relazione e di eventuali ulteriori argomenti di comune interesse;
- immediata, ove risultino accertati fatti di particolare materialità o significatività, nei confronti dei legali rappresentanti e del Collegio Sindacale.

Inoltre, è previsto che:

- nel caso in cui la violazione del Modello sia commessa da parte di uno dei legali rappresentanti, l'OdV informa l'altro legale rappresentante e il Collegio Sindacale;
- nel caso in cui la violazione del Modello sia commessa da parte di entrambi i legali rappresentanti, l'OdV informa il Consiglio di Amministrazione e il Collegio Sindacale;
- nel caso in cui la violazione del Modello sia commessa da parte di uno o più dei componenti del Collegio Sindacale, l'OdV informa tutti gli altri membri del Collegio e i legali rappresentanti.

7. WHISTLEBLOWING

Conformemente alle previsioni dell'art. 6 del Decreto 231, Payback Italia intende incentivare la collaborazione dei lavoratori per favorire l'emersione di eventuali fenomeni corruttivi all'interno della Società e, a tal fine, ha istituito tre canali alternativi di segnalazione, tutti protetti da assoluta riservatezza, costituiti da:

- 1. apposito indirizzo di posta elettronica dedicato;
- 2. apposito indirizzo di posta elettronica dell'OdV;
- 3. casella per segnalazioni in cartaceo presso la sede aziendale.

Ricevuta la segnalazione, il destinatario della stessa, applicando le misure di tutela della riservatezza del segnalante previste dalle policy American Express, seguirà le procedure stabilite per la valutazione



della segnalazione e ne stabilirà la fondatezza, informando, se del caso, le funzioni aziendali e gli organi societari responsabili dell'applicazione del sistema disciplinare.

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano segnalazioni può essere denunciata all'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.



ALLEGATO 1 – elenco reati attualmente inclusi nel D.lgs. n. 231/2001

Art. D. Lgs. n. 231/2001	Disposizione richiamata	Rubrica/Contenuto	
Art. 24	Art. 316 bis c.p.	Malversazione a danno dello Stato	
Indebita percezione di erogazioni, truffa in	Art. 316 ter c.p	Indebita percezione di erogazioni a danno dello Stato	
danno dello Stato o di un ente pubblico o per il conseguimento di	Art. 640 comma 2 n. 1 c.p.	Truffa aggravata a danno dello Stato o di un altro ente pubblico	
erogazioni pubbliche e frode informatica in	Art. 640 bis c.p.	Truffa aggravata per il conseguimento di erogazioni pubbliche	
danno dello Stato o di un ente pubblico	Art. 640 <i>ter</i> c.p.	Frode informatica in danno dello Stato o di altro ente pubblico	
	Art. 491 bis c.p.	Documenti informatici	
	Art. 615 <i>ter</i> c.p.	Accesso abusivo ad un sistema informatico o telematico	
	Art. 615 quater c.p.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici	
	Art. 615 quinquies c.p.	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	
Art. 24 <i>bis</i> Delitti informatici e trattamento illecito	Art. 617 quater c.p.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	
dei dati	Art. 617 quinquies c.p.	Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	
	Art. 635 bis c.p.	Danneggiamento di informazioni, dati e programmi informatici	
	Art. 635 <i>ter</i> c.p.	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	
	Art. 635 quater c.p.	Danneggiamento di sistemi informatici o telematici	



	Art. 635 quinquies c.p.	Danneggiamento di sistemi informatici o telematici di pubblica utilità	
	Art. 640 quinquies c.p.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	
	Art. 416 c.p.	Associazione per delinquere	
	Art. 416 bis c.p.	Associazioni di tipo mafioso anche straniere	
	Art. 416 <i>ter</i> c.p.	Scambio elettorale politico-mafioso	
	Art. 630 c.p.	Sequestro di persona a scopo di estorsione	
	Art. 378 c.p.	Favoreggiamento personale	
Art. 24 <i>ter</i> Delitti di criminalità organizzata	Art. 407, comma 2, lett. a), n. 5 c.p.p.	Delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo	
	Art. 74 D.P.R. 309/1990 (T.U. Stupefacenti)	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	
Art. 25	Art. 317 c.p.	Concussione	
Concussione, induzione indebita a	Art. 318 c.p.	Corruzione per l'esercizio della funzione	
dare o promettere utilità e corruzione	Art. 319 c.p.	Corruzione per un atto contrario ai doveri di ufficio	
	Art. 319 bis c.p.	Circostanze aggravanti	
	Art. 319 ter c.p.	Corruzione in atti giudiziari	
	Art. 319 quater c.p.	Induzione indebita a dare o promettere utilità	
	Art. 320 c.p.	Corruzione di persona incaricata di un pubblico servizio	
	Art. 321 c.p.	Pene per il corruttore	
	Art. 322 c.p.	Istigazione alla corruzione	



	Art. 322 <i>bis</i> c.p.	Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri	
	Art. 453 c.p.	Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate	
Art. 25 <i>bis</i>	Art. 454 c.p.	Alterazione di monete	
Falsità in monete, in carte di pubblico credito, in valori di	Art. 455 c.p.	Spendita e introduzione nello Stato, senza concerto, di monete falsificate	
bollo e in strumenti o segni di	Art. 457 c.p.	Spendita di monete falsificate ricevute in buona fede	
riconoscimento	Art. 459 c.p.	Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati	
	Art. 460 c.p.	Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo	
	Art. 461 c.p.	Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata	
	Art. 464 c.p.	Uso di valori di bollo contraffatti o alterati	
	Art. 473 c.p.	Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni	
	Art. 474 c.p.	Introduzione nello Stato e commercio di prodotti con segni falsi	
	Art. 513 c.p.	Turbata libertà dell'industria o del commercio	
Art. 25 <i>bis</i> 1	Art. 513 bis c.p.	Illecita concorrenza con minaccia o violenza	



Delitti contro	Art. 514 c.p.	Frodi contro le industrie nazionali		
l'industria e il- commercio	Art. 515 c.p.	Frode nell'esercizio del commercio		
Commercio	Art. 516 c.p.	Vendita di sostanze alimentari non genuine come genuine		
	Art. 517 c.p.	Vendita di prodotti industriali con segni mendaci		
	Art. 517 ter c.p.	Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale		
	Art. 517 quater c.p.	Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari		
	Art. 2621 c.c.	False comunicazioni sociali		
	Art. 2621 bis c.c.	Fatti di lieve entità		
	Art. 2622 c.c.	False comunicazioni sociali delle società quotate		
	Art. 2625 c.c.	Impedito controllo		
	Art. 2626 c.c.	Indebita restituzione dei conferimenti		
	Art. 2627 c.c.	Illegale ripartizione degli utili e delle riserve		
	Art. 2628 c.c.	Illecite operazioni sulle azioni o quote sociali o della società controllante		
Art. 25 ter	Art. 2629 c.c.	Operazioni in pregiudizio dei creditori		
Reati societari	Art. 2629 bis c.c.	Omessa comunicazione del conflitto di interessi		
	Art. 2632 c.c.	Formazione fittizia del capitale		
	Art. 2633 c.c.	Indebita ripartizione dei beni sociali da parte dei liquidatori		
	Art. 2635 c.c.	Corruzione tra privati		
	Art. 2635 bis c.c.	Istigazione alla corruzione tra privati		
	Art. 2636 c.c.	Illecita influenza sull'assemblea		
	Art. 2637 c.c.	Aggiotaggio		
	Art. 2638 c.1 e 2 c.c.	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza		



	Art. 270 c.p.	Associazioni sovversive	
	Art. 270 bis c.p.	Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico	
	Art. 270 ter c.p.	Assistenza agli associati	
	Art. 270 quater c.p.	Arruolamento con finalità di terrorismo anche internazionale	
	Art. 270 quater 1 c.p.	Organizzazione di trasferimenti per finalità di terrorismo	
	Art. 270 quinquies c.p.	Addestramento ad attività con finalità di terrorismo anche internazionale	
	Art. 270 quinquies 1 c.p.	Finanziamento di condotte con finalità di terrorismo	
	Art. 270 quinquies 2 c.p.	Sottrazione di beni o denaro sottoposti a sequestro	
Art. 25 <i>quater</i> Delitti con finalità di	Art. 270 sexies c.p.	Condotte con finalità di terrorismo	
terrorismo o di eversione dell'ordine democratico	Art. 280 c.p.	Attentato per finalità terroristiche o di eversione	
	Art. 280 bis c.p.	Atto di terrorismo con ordigni micidiali o esplosivi	
	Art. 280 ter c.p.	Atti di terrorismo nucleare	
	Art. 289 bis c.p.	Sequestro di persona a scopo di terrorismo o di eversione	
	Art. 302 c.p.	Istigazione a commettere alcuno dei delitti preveduti dai capi primo e secondo	
	Art. 304 c.p.	Cospirazione politica mediante accordo	
	Art. 305 c.p.	Cospirazione politica mediante associazione	
	Art. 306 c.p.	Banda armata: formazione e partecipazione	
	Art. 307 c.p.	Assistenza ai partecipi di cospirazione o di banda armata	



	Art. 1 D.L. 625/1979 - mod.	Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica	
	in L. 15/1980	democratico e dena sicurezza pubblica	
	Art. 5 D.L. 625/1979 - mod. in L. 15/1980	Pentimento operoso	
	Art. 1 L. 342/1976	Impossessamento, dirottamento e distruzione di un aereo	
	Art. 2 L. 342/1976	Danneggiamento delle installazioni a terra	
	Art. 3 L. 422/1989	Disposizioni in materia di reati diretti contro la sicurezza della navigazione marittima e la sicurezza delle istallazioni fisse sulla piattaforma continentale	
	Art. 2 Convenzione di New York del 9 Dicembre 1999	Convenzione internazionale per la repressione del finanziamento del terrorismo	
Art. 25 quarter 1 Pratiche di mutilazione degli organi genitali femminili	Art. 583 bis c.p.	Pratiche di mutilazione degli organi genitali femminili	
	Art. 600 c.p.	Riduzione o mantenimento in schiavitù o in servitù	
	Art. 600 bis c.p.	Prostituzione minorile	
	Art. 600 ter c.p.	Pornografia minorile Detenzione di materiale pornografico	
Art. 25 <i>quinquies</i> Delitti contro la	Art. 600 quater c.p.		
personalità individuale	Art 600 quater 1 c.p.	Pornografia virtuale	
	Art. 609 undecies c.p.	Adescamento di minorenni	
	Art. 600 quinquies c.p.	Iniziative turistiche volte allo sfruttamento della prostituzione minorile	



	Art. 601 c.p.	Tratta di persone	
-	Art. 602 c.p.	Acquisto e alienazione di schiavi	
		Intermediazione illecita e sfruttamento	
	Art. 603 <i>bis</i> c.p.	del lavoro	
Art. 25 sexies	Art. 184 T.U.F. (D. Lgs. 58/1998)	Abuso di informazioni privilegiate	
Reati di abuso di mercato	Art. 185 T.U.F. (D. Lgs. 58/1998)	Manipolazione del mercato	
Art. 25 septies	Art. 589 c.p.	Omicidio colposo	
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	Art. 590 c.p.	Lesioni personali colpose	
Art. 25 octies	Art. 648 c.p.	Ricettazione	
Ricettazione,	Art. 648 bis c.p.	Riciclaggio	
riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	Art. 648 <i>ter</i>	Impiego di denaro, beni o utilità di provenienza illecita	
nonché autoriciclaggio	Art. 648 ter. 1	Autoriciclaggio	
	Art. 171 L. 633/1941	Divulgazione di opere dell'ingegno attraverso rete telematica	
	Art. 171 bis L. 633/1941	Reati in materia di software e banche dati	
Art. 25 <i>novies</i> Delitti in materia di violazione del diritto d'autore	Art. 171 ter L. 633/1941	Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche	
u autore	Art. 171 septies L. 633/1941	Violazioni nei confronti della SIAE	
	Art. 171 octies L. 633/1941	Manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato	



Art. 25 decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Art. 377 <i>bis</i> c.p.	Reato di induzione a non render dichiarazioni o a rendere dichiarazion mendaci all'autorità giudiziaria	
	Art. 452 bis c.p. Art. 452 quater c.p. Art. 452	Inquinamento ambientale Disastro ambientale Delitti colposi contro l'ambiente	
	quinquies c.p. Art. 452 sexies c.p. Art. 452 octies	Traffico e abbandono di materiale ad alta radioattività Circostanze aggravanti	
	c.p. Art. 727 bis c.p.	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette	
Art. 25 <i>undecies</i> Reati ambientali	Art. 733 bis c.p.	Distruzione o deterioramento di habitat all'interno di un sito protetto	
Reati ambientali	Art. 137 c. 2, 3, 5,11, 13 D.Lgs. 152/2006	Scarichi di acque contenenti sostanze pericolose, in assenza di autorizzazione o dopo che la stessa sia stata sospesa o revocata e scarico nelle acque del mare, da parte di navi o aeromobili, di sostanze o materiali per i quali vige il divieto assoluto di sversamento	
	Art. 256 c. 1 lettere a) b), 3, 4, 5 e 6 D.Lgs. 152/2006	Reati in materia di gestione non autorizzata di rifiuti (attività di gestione di rifiuti non autorizzata)	
	Art. 257 c. 1 e 2 D.Lgs. 152/2006	Reati in materia di bonifica dei siti (omessa bonifica dei siti in conformità del progetto approvato dall'autorità competente)	



Art. 258 c. 4 D.Lgs. 152/2006	Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari
Art. 259 c. 1 D.Lgs. 152/2006	Traffico illecito di rifiuti
Art. 260 D.Lgs. 152/2006	Attività organizzate per il traffico illecito di rifiuti
Art. 260 bis c. 6, 7 e 8 D.Lgs. 152/2006	Falsità ideologica del certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione, e falsità ideologica e materiale della scheda SISTRI – Area Movimentazione
Art. 279 c. 5 D.Lgs. 152/2006	Reati in materia di tutela dell'aria e di riduzione delle emissioni in atmosfera (Superamento di valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria)
	Reati in materia di tutela di specie animali e vegetali in via di estinzione
Art. 6 L. 150/1992	Detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e l'incolumità pubblica
Art. 3 L. 549/1993	Cessazione e riduzione dell'impiego di sostanze lesive
Art. 8 c. 1 e 2 D.Lgs. 202/2007	Inquinamento doloso di nave battente qualsiasi bandiera
Art. 9 c. 1 e 2 D.Lgs. 202/2007	Inquinamento colposo di nave battente qualsiasi bandiera



Art. 25 duodecies Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	D. Lgs. 109/2012	Secondo l'art. 22 comma 12 bis del D. Lgs. 25 luglio 1998, n. 286, l'impiego di cittadini di Paesi terzi il cui soggiorno è irregolare aggravato da: - numero di lavoratori irregolari superiore a tre; - impiego di minori in età non lavorativa; - sottoposizione a condizioni lavorative di particolare sfruttamento, quali l'esposizione a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro	
	Art. 12 c. 3, 3 bis, 3 ter e 5 D. Lgs. 286/1998	Disposizioni contro le immigrazioni clandestine	
Art. 3, c. 1 L. 654/1975 Art. 25 terdecies Art. 3, c. 3 bis L. 654/1975		Propaganda di idee fondate sulla superiorità o sull'odio razziale o etnico, e istigazione a commettere o commissione di atti di discriminazione per motivi razziali, etnici, nazionali o religiosi	
		Propaganda ovvero istigazione e incitamento, da cui derivi un concreto pericolo di diffusione, fondato in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra	
L. 146/2006	Art. 12 c. 3, 3 bis, 3 ter e 5 D. Lgs. 286/1998	Disposizioni contro le immigrazioni clandestine	
309/1990 il		Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	



Art. 291 quater D.P.R. 43/1973	Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri
Art. 377 bis c.p.	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
Art. 378 c.p.	Favoreggiamento personale
Art. 416 c.p.	Associazione per delinquere
Art. 416 bis c.p.	Associazioni di tipo mafioso anche straniere





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - A

INDEBITA PERCEZIONE DI EROGAZIONI, TRUFFA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO O PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE E FRODE INFORMATICA IN DANNO DELLO STATO O DI UN ENTE PUBBLICO



INDICE

<u>- P</u>	ARTE SPECIALE - A	41
PR	EMESSA	41
<u>1.</u>	LE TIPOLOGIE DI REATO	41
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	42
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	43
4	PRINCIPI CENERALI DI COMPORTAMENTO	13



- PARTE SPECIALE - A -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "A", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24 del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 24 ex D.lgs. n. 231/2001. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.

I reati di truffa e frode informatica tutelano il patrimonio e, con specifico riferimento ai reati rilevanti ai sensi del D.Lgs. n. 231/2001, ad essere tutelato è il patrimonio dello Stato.

Fermo restando quanto di seguito dettagliato in riferimento alle singole attività sensibili, i rapporti con la Pubblica Amministrazione che potrebbero dare luogo alla commissione dei reati di truffa e frode informatica sono stati identificati, principalmente, in quelli con l'INPS, INAIL e con l'Agenzia delle Entrate in relazione alle attività di gestione degli adempimenti connessi all'applicazione delle leggi, regolamenti e provvedimenti delle Autorità pubbliche in materia di sicurezza e igiene sul lavoro e di previdenza e assistenza dei lavoratori.

Truffa aggravata a danno dello Stato, di altro ente pubblico (art. 640, comma 2, n. 1 c.p.)

"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da 6 mesi a 3 anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da 1 a 5 anni e della multa da euro 309 a euro 1.549, 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare (...)".



La fattispecie di cui al comma 1 dell'art. 640 c.p. descrive un reato comune che può essere commesso da chiunque, con artifizi e raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. Nella fattispecie richiamata dall'art. 24 del D.Lgs. n. 231/2001 (i.e. art. 640 comma 2, n. 1 c.p.), il reato di truffa è preso in considerazione con esclusivo riferimento al caso in cui il fatto sia commesso a danno dello Stato o di un altro ente pubblico.

Per "artificio" o "raggiro" si intende la simulazione o dissimulazione della realtà, atta ad indurre in errore una persona per effetto della percezione di una falsa apparenza. Il silenzio può integrare la condotta della truffa se mantenuto in presenza di un obbligo giuridico di comunicazione, anche di carattere extra-penale.

L'atto di disposizione del soggetto indotto in errore può comprendere ogni comportamento dotato di un'efficacia in fatto; tale può essere considerata anche la semplice inerzia.

Il "profitto" si ravvisa anche nella mancata diminuzione del patrimonio e, quindi, anche in assenza di un aumento effettivo di ricchezza; può anche non essere di natura patrimoniale, potendo consistere nel soddisfacimento di un interesse di natura morale.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.)

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da 6 mesi a 3 anni e con la multa da euro 51 a euro 1.032.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

Tale ipotesi di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, si procura un ingiusto profitto per sé o altri, con danno altrui.

In concreto, può integrarsi il reato in esame qualora, ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Ai fini dell'applicabilità del D.Lgs. n. 231/01, tale reato assume rilevanza solo nei casi in cui il titolare del sistema informatico sia rappresentato dallo Stato o altro ente pubblico.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]



3. IL SISTEMA DI CONTROLLO

- A) Gestione dei rapporti con le autorità di vigilanza/autorità pubbliche in sede di verifiche e accertamenti [OMISSIS]
- B) Gestione dei rapporti con le autorità competenti

[OMISSIS]

C) Gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti con la Pubblica Amministrazione (compresi i pubblici ufficiali e gli incaricati di pubblico servizio) per conto o nell'interesse della Società ovvero a coloro che possano avere rapporti diretti o indiretti con l'Autorità Giudiziaria, in relazione a circostanze oggetto di attività processuale comunque attinenti l'Ente stesso.

In via generale, a tali soggetti è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 24 del D.Lgs. 231/2001.

In particolare, coerentemente con i principi deontologici aziendali espressi nel Codice Etico e nel Codice di Condotta American Express, ai quali si rimanda ad ulteriore integrazione di quanto non espressamente disciplinato nella Parte Generale del presente Modello, è fatto divieto di:

- fornire alla Pubblica Amministrazione/Autorità di Vigilanza documentazione non veritiera, occultare notizie e informazioni rilevanti e, più in generale, ostacolare l'attività di controllo della medesima;
- esibire documenti negligentemente incompleti e/o comunicare dati falsi o alterati alla Pubblica Amministrazione;
- alterare il funzionamento di sistemi telematici pubblici;
- alterare dati contenuti in documenti/comunicazioni elettroniche aventi natura certificativa e/o efficacia probatoria inviata ai funzionari pubblici competenti;
- fornire informazioni o dichiarazioni non veritiere al fine dell'ottenimento di erogazioni, contributi, sovvenzioni o finanziamenti ovvero destinare erogazioni, contributi, sovvenzioni o finanziamenti a finalità diverse da quelle per le quali sono stati ottenuti.



In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente Payback) o il referente interno (in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - B
DELITTI INFORMATICI



INDICE

- P	ARTE SPECIALE B	47
<u>PR</u>	REMESSA	47
<u>1.</u>	LE TIPOLOGIE DI REATO	47
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	51
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	51
4.	PRINCIPI GENERALI DI COMPORTAMENTO	52



- PARTE SPECIALE B-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "B", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24 bis del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno di Payback Italia S.r.l. (di seguito anche la "Società" o l'"Ente") in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 24 bis ex D.lgs. n. 231/2001. Delitti informatici e trattamento illecito di dati

Falsità riguardanti un documento informatico (art. 491-bis c.p.)

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici."

Tale reato si realizza quando le condotte di falsità di cui agli articoli individuati al Capo III del Codice Penale trovano applicazione rispetto a un documento informatico (pubblico o privato) cui la legge attribuisce efficacia probatoria.

Pertanto, a prescindere da un supporto cartaceo, il legislatore prevede la consumazione dei reati di falsità sin dal momento in cui i documenti, sia che siano un atto pubblico che una scrittura privata, vengano inseriti in un registro informatico, o comunque trasmessi telematicamente.

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)



"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

Tale reato si realizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo.

L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema stesso (password).

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, nonostante sia entrato legittimamente in un sistema, si sia trattenuto contro la volontà del titolare oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615-quater c.p.)

"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater."



Il suddetto reato si realizza nel caso in cui un soggetto acquisisca i mezzi necessari ad accedere al sistema informatico altrui, sia se procura ad altri i mezzi o le informazioni idonei ad eludere le barriere di protezione.

Il reato si consuma nel momento in cui il soggetto agente acquisisce la disponibilità del codice di accesso, ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o la consegna dei suddetti mezzi.

Il bene giuridico oggetto di tutela è la riservatezza informatica e la indisturbata fruizione del sistema informatico da parte del gestore.

Viene ad ogni modo richiesto il dolo specifico costituito dal fine di procurasi un profitto, di danneggiare o di permettere il danneggiamento o comunque il non funzionamento (anche temporaneo) di un sistema informatico.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329."

Il reato di cui sopra si realizza sia nel caso in cui il soggetto procuri strumenti dannosi sia qualora li metta in circolazione.

Nello specifico, con riferimento alla produzione, questa è integrata dall'effettiva creazione di nuovi strumenti, non essendo sufficiente la mera progettazione.

Con riferimento all'importazione, questa consiste nell'introduzione dall'estero di strumenti sul territorio nazionale, mentre la diffusione viene intesa come la messa a disposizione dello strumento ad un numero indeterminato di individui.

La condotta della messa a disposizione di altri, quale formula di chiusura, è finalizzata a reprimere tutte le ipotesi di messa in circolazione di carattere residuale.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617quater c.p.)

"Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.



I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;
- 3) da chi esercita anche abusivamente la professione di investigatore privato."

Il suddetto reato può concretizzarsi in una condotta volta ad intercettare fraudolentamente una comunicazione informatica o telematica, ovvero che miri ad impedirla o interromperla, eludendo eventuali sistemi di protezione della trasmissione in corso o in modo tale da non rendere percepibile a terzi l'intromissione abusiva.

Il secondo comma prevede la medesima pena nei confronti di chi riveli pubblicamente il contenuto delle comunicazioni captate fraudolentemente da altri.

Il comma 4 prevede alcune circostanze aggravanti specifiche, qualora il fatto sia commesso in danno di un sistema informatico dello Stato, oppure sia commesso da un pubblico ufficiale con abuso dei poteri o con abuso della qualità di operatore del sistema, o se commesso da chi eserciti, anche abusivamente, la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

"Chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617quater."

La condotta con cui si realizza tale reato consiste nell'installazione di apparecchiature idonee a intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico.

Il reato si consuma nel momento in cui è stata completata l'installazione delle suddette apparecchiature. In particolare, la disposizione punisce fatti prodromici alla commissione del delitto di cui all'articolo precedente (617 quater), indicando infatti come penalmente rilevante l'installazione di apparecchiature atte a captare o impedire comunicazioni relative ad un sistema informatico o tra sistemi telematici.

Il secondo comma prevede una circostanza aggravante specifica, qualora il fatto sia commesso in danno di un sistema informatico dello Stato, oppure sia commesso da un pubblico ufficiale con abuso dei poteri o con abuso della qualità di operatore del sistema, o se commesso da chi eserciti, anche abusivamente, la professione di investigatore privato.



Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime

 $informazioni,\ dati\ o\ programmi\ informatici\ altrui\ punito,\ a\ quere la\ della\ persona\ offesa,\ con\ la\ reclusione\ da\ sei$

mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del

sistema, la pena è della reclusione da uno a quattro anni."

Tale disposizione mira a tutelare il bene giuridico del patrimonio, in relazione a dati o programmi informatici

altrui.

Ad essere incriminata è la condotta di chi distrugge, cancella, deteriora o altera dati, informazioni o programmi

informatici altrui. Inoltre, se il fatto è commesso con violenza o minaccia, oppure abusando della propria qualità

di operatore informatico, si applica un aggravamento di pena ai sensi del secondo comma.

La condotta idonea ad integrare il reato, si identifica con quella del fatto illecito in materia aquiliana (art. 2043),

stante la differenza riguardante la delimitazione dell'oggetto del danno (che nel delitto in esame deve

necessariamente essere un programma informatico o suoi dati) e l'elemento soggettivo, limitato al dolo e non anche

alla colpa.

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 bis, ovvero

attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in

tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è

punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del

sistema, la pena è della reclusione da uno a quattro anni."

Tale reato punisce il soggetto a cui è imputabile la condotta prevista ai sensi dell'articolo precedente (art. 635-bis

c.p.), qualora ne derivi una compromissione irreversibile di un sistema informatico, e non di semplici dati o

informazioni.

Se il fatto è commesso con violenza o minaccia, oppure abusando della propria qualità di operatore informatico,

si applica un aggravamento di pena ai sensi del secondo comma.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

51



4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle Attività Sensibili rispetto ai delitti informatici e al trattamento illlecito di dati e, in particolare, a tutte le risorse che utilizzano sistemi informativi (avuto soprattutto riguardo a linee di comunicazione dei dati e server) per l'espletamento della propria attività lavorativa in favore dell'Ente.

In via generale, a tali soggetti è richiesto di:

- osservare rigorosamente tutte le norme poste dalla legge, dalle procedure e dalle linee di condotta aziendali interne (di Gruppo e locali) in merito alla sicurezza dei sistemi informativi dell'Azienda e al trattamento di qualsivoglia dato personale;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi
 individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di delitti informatici
 e trattamento illecito di dati.

In particolare, è vietato:

- connettere ai sistemi informatici, personal computer, periferiche e altre apparecchiature o installare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
- modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire, possedere o utilizzare strumenti software e/o hardware se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali che potrebbero essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate;
- divulgare, cedere o condividere con personale interno o esterno e alle altre Società del Gruppo le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere abusivamente ad un sistema informatico altrui ovvero nella disponibilità di altri Dipendenti o terzi
 nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;



- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici
 aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati
 ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o
 sistemi;
- accedere abusivamente al sito Internet dell'Ente al fine di manomettere o alterare abusivamente qualsiasi dato
 ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, infografica, video,
 ecc.) in violazione della normativa sul diritto d'autore e delle procedure e linee di condotta aziendali
 applicabili;
- comunicare a persone non autorizzate, interne o esterne, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti Virus o altri programmi in grado di danneggiare o intercettare dati;
- lo Spamming come pure ogni azione di risposta al medesimo;
- inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

È, inoltre, previsto l'espresso obbligo a carico dei Destinatari di:

- impegnarsi a non rendere pubbliche tutte le informazioni loro assegnate per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password, anche se superata, necessaria per l'accesso ai sistemi dell'Azienda);
- attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso
 allo stesso in caso di allontanamento dalla postazione (es.: uscita dal sistema o blocco dell'accesso tramite
 password);
- accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e
 provvedere, entro le scadenze indicate dal Responsabile della sicurezza informatica, alla modifica periodica
 della password;
- astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;
- non intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- non utilizzare connessioni alternative rispetto a quelle messe a disposizione da parte dell'Azienda al dipendente per l'espletamento della propria attività lavorativa;
- non accedere in maniera non autorizzata ai sistemi informativi di terzi, né alterarne in alcun modo il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;



assicurare la veridicità delle informazioni contenute in qualsivoglia atto e/o documento informatico.

Ferme tutte le altre prescrizioni e regole aziendali, in caso di dubbi circa la corretta attuazione dei principi eticocomportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente dell'ente) o referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

L'Ente inoltre per evitare per quanto possibile il proprio coinvolgimento in attività suscettibili di concretizzare uno o più delitti informatici o di trattamento illecito di dati, verifica che i fornitori esterni implementino presidi di controllo specifici al fine di garantire la sicurezza dei propri sistemi informativi, quali ad esempio:

- accesso ai sistemi informativi solo previa opportuna identificazione da parte dell'utente, a mezzo username e password assegnati originariamente dall'Azienda;
- periodicità di modifica della suddetta password, a seconda della frequenza di utilizzo e della criticità dei dati cui si accede per mezzo di quella password;
- verifica periodica della coincidenza tra i poteri assegnati al profilo utente e le sue mansioni all'interno dell'Azienda, sia nei casi in cui un soggetto venga adibito a differenti attività, sia in caso di conclusione del rapporto di lavoro con l'ente;
- adeguata formazione ai Dipendenti, nonché gli altri soggetti come ad esempio i Collaboratori Esterni –
 eventualmente autorizzati all'utilizzo dei Sistemi Informativi, dell'importanza di:
- mantenere le proprie Credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
- utilizzare correttamente i software e banche dati in dotazione;
- non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse dell'ente, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a
 comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti
 dal Decreto);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della



normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti conformi al dettato della norma;

• contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es. clausole risolutive espresse, penali).



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - C

DELITTI DI CRIMINALITÀ ORGANIZZATA



INDICE

- P	PARTE SPECIALE - C	58
PR	REMESSA	47
<u>1.</u>	LE TIPOLOGIE DI REATO	58
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	59
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	59
4.	PRINCIPI GENERALI DI COMPORTAMENTO	59



- PARTE SPECIALE - C-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "C", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 24 ter del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 24 ter ex D.lgs. n. 231/2001. Delitti di criminalità organizzata

Associazione per delinquere (Art. 416 c.p.)

"Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni.

Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.

I capi soggiacciono alla stessa pena stabilita per i promotori.

Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni.

La pena è aumentata se il numero degli associati è di dieci o più.

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601 e 602, nonché all'articolo 12, comma 3 bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma.



Se l'associazione è diretta a commettere taluno dei delitti previsti dagli articoli 600 bis, 600 ter, 600 quater, 600quater1, 600 quinquies, 609 bis, quando il fatto è commesso in danno di un minore di anni diciotto, 609 quater, 609 quinquies, 609 octies, quando il fatto è commesso in danno di un minore di anni diciotto, e 609 undecies, si applica la reclusione da quattro a otto anni nei casi previsti dal primo comma e la reclusione da due a sei anni nei casi previsti dal secondo comma."

Con riferimento alla fattispecie di reato sopra considerata, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) del reato che costituisce il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un soggetto apicale e/o sottoposto della Società potrebbe determinare la responsabilità amministrativa della Società stessa, sempre che la partecipazione o il concorso all'associazione risultasse strumentale al perseguimento anche dell'interesse o del vantaggio della Società medesima.

È tuttavia richiesto che il vincolo associativo si esplichi attraverso un minimo di organizzazione a carattere stabile nel tempo e la condivisione di un programma di realizzazione di una serie indeterminata di delitti. Non basta pertanto l'occasionale accordo per la commissione di uno o più delitti determinati.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle Attività Sensibili rispetto ai delitti di cui all'art. 24-ter, D.Lgs. n. 231/2001 per l'espletamento della propria attività lavorativa in favore della Società.

In relazione ai reati in esame, fermo quanto previsto dalle altre Sezioni della Parte Speciale del Modello, l'Ente adotta i seguenti principi generali di comportamento:

- preferire come partner commerciali/controparti coloro che hanno adottato un Modello di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001;
- svolgere verifiche preventive delle controparti contrattuali attraverso documentazione disponibile al pubblico e utilizzando tutte le informazioni di cui si sia in possesso;
- ove ritenuto opportuno in relazione alla natura e alle circostanze delle operazioni aziendali, chiedere alle controparti contrattuali e ai candidati per l'assunzione i certificati del casellario giudiziario e i carichi pendenti aggiornati;
- verificare l'adozione di specifiche cautele nell'attività di selezione e assunzione del personale da parte della funzione di AESEL a cui è esternalizzata l'attività di gestione del personale;



- osservare la massima trasparenza nei processi di approvvigionamento;
- svolgere adeguate attività formative e informative, mediante la diffusione di notizie sulle forme di criminalità presenti sul territorio;
- monitorare costantemente i flussi di denaro in uscita.

In particolare, è fatto divieto ai soggetti destinatari della presente Parte Speciale di:

- fornire, direttamente o indirettamente, fondi a favore di soggetti utilizzabili per porre in essere condotte integranti reati di associazione per delinquere;
- fornire compensi in favore dei fornitori di beni e servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale.

Ferme tutte le altre prescrizioni e regole aziendali, in caso di dubbi circa la corretta attuazione dei principi eticocomportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente dell'Ente) o referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a
 comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti
 dal Decreto);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di
 cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della
 normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti
 ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti
 conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. n. 231/2001 e del Modello (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti rientranti nell'ambito di applicazione del Decreto) (es. clausole risolutive espresse, penali).





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - D

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE



INDICE

<u>- P</u>	ARTE SPECIALE - D	63	
<u>PR</u>	PREMESSA		
<u>1.</u>	LE TIPOLOGIE DI REATO	63	
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	66	
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	66	
4.	PRINCIPI GENERALI DI COMPORTAMENTO	66	



- PARTE SPECIALE - D -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "D", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25 ex D.lgs. n. 231/2001. Reati di Corruzione

I reati di corruzione mirano a tutelare l'imparzialità e la correttezza dell'agire della Pubblica Amministrazione, andando a sanzionare tutti quei comportamenti volti a mercificare l'azione, le decisioni e gli orientamenti della Pubblica Amministrazione. Fermo restando quanto di seguito dettagliato in riferimento alle singole attività "sensibili", i rapporti con la Pubblica Amministrazione che potrebbero dare luogo alla commissione dei reati di corruzione di seguito elencati sono stati identificati in quelli con l'Agenzia delle Entrate e/o con la Guarda di Finanza, con le Autorità Amministrative indipendenti (es. AGCM, Garante *Privacy*) e con l'Autorità Giudiziaria, nonché con le Autorità di controllo ed enti pubblici (es. INPS, INAIL, ASL, etc.).

Con riferimento alla Società, tali reati verrebbero sanzionati ai sensi dell'art. 321 c.p. (rubricato "*Pene per il Corruttore*"), che, richiamando l'applicabilità degli articoli 318, 319-ter e 320 c.p., estende la punibilità dell'attività corruttiva al corruttore, dell'art. 319-quater, II comma c.p. ("*Induzione indebita a dare o a ricevere denaro*") e dell'art. 322, commi I e II c.p. ("*Istigazione alla corruzione*").

Tra gli strumenti a disposizione della Società per la commissione dei reati di corruzione si sono individuati, oltre alla mera dazione di danaro, anche la concessione di benefici di varia natura, in particolar modo con riferimento alla gestione del personale, relativamente ad assunzioni e/o alle elargizioni nei confronti di soggetti riconducibili



al funzionario pubblico di volta in volta interessato, ovvero al conferimento di omaggi o regalie quali contropartita dell'attività corruttiva.

Corruzione per l'esercizio della funzione (art. 318 c.p.)

"Il pubblico ufficiale, che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da 1 a 6 anni".

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

La disposizione prevede la punibilità di qualsiasi comportamento, attivo od omissivo, anche non espressamente in contrasto con specifiche norme giuridiche o con istruzioni di servizio, che si concretizzi - o si sia concretizzato - nella violazione dei doveri di fedeltà, imparzialità ed onestà, alla cui osservanza è chiamato il pubblico ufficiale.

Ai fini della configurabilità di tale reato, è necessario che il pubblico ufficiale percepisca, o accetti la promessa, per sé o per altri, di un indebito compenso, senza necessaria proporzionalità tra la prestazione del soggetto attivo e quanto dato o promesso.

Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)

"Il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri d'ufficio, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa, è punito con la reclusione da 6 a 10 anni".

L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri d'ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa (c.d. corruzione propria).

Corruzione in atti giudiziari (art. 319-ter c.p.)

"Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da 6 a 12 anni.

Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da 5 a 12 anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni".

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p. sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari nell'ambito di procedimenti pendenti tra la Società e il personale dipendente, al fine di ottenere illecitamente provvedimenti favorevoli.



Induzione indebita a dare o promettere utilità (319-quater c.p.)

"Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da 6 a 10 anni e 6 mesi.

Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a 3 anni".

Tale ipotesi di reato si configura, salvo che il fatto costituisca più grave reato, nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.)

"Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

In ogni caso, le pene sono ridotte in misura non superiore ad un terzo".

Le disposizioni di cui agli artt. 318 e 319 c.p. si applicano anche all'incaricato di pubblico servizio.

Pene per il corruttore (art. 321 c.p.)

"Le pene stabilite nel primo comma dell'articolo 318, nell' articolo 319, nell'articolo 319-bis, nell' art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità".

Le pene stabilite nel primo comma dell'art. 318, nell'art. 319, nell'art. 319-*bis*, nell'art. 319-*ter* e nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi (i.e. corruttore/Società) dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio denaro o altra utilità.

Istigazione alla corruzione (art. 322 c.p.)

"Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel comma 1 dell'articolo 318, ridotta di un terzo.

Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo [...]".

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a compiere un atto contrario ai propri doveri, qualora l'offerta o la promessa non sia accettata.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione dei rapporti con le autorità di vigilanza/autorità pubbliche in sede di verifiche e accertamenti

[OMISSIS]

A) Gestione dei rapporti con le autorità competenti

[OMISSIS]

B) Gestione dei rapporti con soggetti pubblici per l'ottenimento di autorizzazioni e licenze ed il successivo invio di dati/informazioni di carattere gestionale

[OMISSIS]

C) Gestione dei rapporti con l'amministrazione finanziaria

[OMISSIS]

D) Gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata

[OMISSIS]

E) Gestione del processo di selezione e assunzione del personale

[OMISSIS]

F) Gestione dei flussi monetari e finanziari

[OMISSIS]

G) Gestione degli acquisti di beni e servizi

[OMISSIS]

H) Gestione di omaggi e liberalità

[OMISSIS]

I) Gestione del contenzioso

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti con la Pubblica Amministrazione (compresi i pubblici ufficiali e gli incaricati di pubblico servizio) per conto o nell'interesse della Società ovvero a coloro che possano avere rapporti



diretti o indiretti con l'Autorità Giudiziaria, in relazione a circostanze oggetto di attività processuale comunque attinenti l'Ente stesso.

In particolare, coerentemente con i principi deontologici aziendali espressi nel Codice Etico e nel Codice di Condotta American Express, cui si rimanda ad ulteriore integrazione di quanto non espressamente disciplinato nella parte generale del presente modello, è fatto divieto di:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della Pubblica Amministrazione, italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni normative e delle procedure e linee di condotta aziendali.
- distribuire omaggi e regali al di fuori di quanto previsto dalle specifiche procedure e linee di condotta aziendali (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri, o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore, la cui quantificazione è prevista dalle specifiche procedure e linee di condotta aziendali.
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione) in favore di rappresentanti della Pubblica Amministrazione, italiana o straniera, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda.
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale e comunque non conformi alle specifiche procedure e linee di condotta aziendali.
- effettuare prestazioni o pagamenti di compensi in favore di collaboratori, fornitori, consulenti, partner o altri
 soggetti terzi che operino per conto dell'Ente, che non trovino adeguata giustificazione nel contesto del
 rapporto contrattuale costituito con gli stessi.
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da rappresentanti della Pubblica Amministrazione, italiana o straniera, come condizione per lo svolgimento di successive attività.
- ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico ufficiale
 o di altro rappresentante della Pubblica Amministrazione/Autorità di Vigilanza, tali da influenzare le
 conclusioni dell'attività amministrativa di propria competenza;
- omettere gli obblighi ed i presidi di controllo previsti dalla Società in ambito della gestione dei flussi finanziari in conformità ai principi di correttezza professionale e contabile, al fine di orientare in proprio favore decisioni della Pubblica Amministrazione;



• adottare comportamenti e azioni tali da impedire materialmente, o comunque ostacolare, mediante l'occultamento di documenti o l'utilizzo di altri mezzi fraudolenti, lo svolgimento delle attività ispettive.

I divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti (attraverso parenti, affini ed amici) con i rappresentanti della Pubblica Amministrazione, italiana o straniera.

È inoltre fatto obbligo ai Destinatari dei presenti principi etico-comportamentali di attenersi alle seguenti prescrizioni:

- in caso di tentata concussione da parte di un pubblico funzionario il soggetto interessato deve: (i) non dare seguito alla richiesta; (ii) fornire tempestivamente informativa al proprio Responsabile (in caso di dipendente Payback) o al referente interno (in caso di soggetti terzi) ed attivare formale informativa verso l'Organismo di Vigilanza.
- in caso di conflitti di interesse che sorgano nell'ambito dei rapporti con la Pubblica Amministrazione o con l'Autorità Giudiziaria, il soggetto interessato deve fornire tempestivamente informativa al proprio Responsabile (in caso di dipendente Payback) o al referente interno (in caso di soggetto terzo) ed attivare formale informativa verso l'Organismo di Vigilanza.
- in caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente Payback) o il referente interno (in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura, che operano con la Pubblica Amministrazione e l'amministrazione della giustizia per conto o nell'interesse di Payback, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a
 comportamenti configuranti ipotesi corrispondenti alla corruzione e alla truffa ai danni di enti pubblici ovvero
 di ostacolo all'amministrazione della giustizia);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. 231/2001 e di aver attuato un idoneo modello di organizzazione, gestione e controllo (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti alla corruzione e alla truffa ai danni di enti pubblici ovvero di ostacolo all'amministrazione della giustizia) e di impegnarsi a tenere comportamenti conformi al dettato della norma;



contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui
al D.Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa
internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti alla
corruzione e alla truffa ai danni di enti pubblici ovvero di ostacolo all'amministrazione della giustizia) (es.
clausole risolutive espresse, penali).





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - E

REATI CONTRO LA FEDE PUBBLICA



INDICE

- P/	PARTE SPECIALE - E	72
PR]	REMESSA	72
1.	LE TIPOLOGIE DI REATO	72
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	74
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	74
4.	PRINCIPI GENERALI DI COMPORTAMENTO	74



- PARTE SPECIALE - E-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "E", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 bis del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25-bis ex D.lgs. n. 231/2001. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento

Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)

"Chiunque, non essendo concorso nella contraffazione o nell'alterazione, fa uso di valori di bollo contraffatti o alterati, è punito con la reclusione fino a tre anni e con la multa fino a cinquecentosedici euro.

Se i valori sono stati ricevuti in buona fede, si applica la pena stabilita nell'articolo 457, ridotta di un terzo."

Tale reato si realizza nell'ipotesi in cui l'uso, che non deve accompagnarsi a comportamenti idonei a configurare un concorso nella fattispecie di cui all'articolo 459 c.p. ("Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati"), abbia ad oggetto valori bollati contraffatti o alterati.

Nello specifico, l'uso di valori di bollo contraffatti è punito come reato autonomo se l'uso è quello conforme alla naturale destinazione dei valori. Non rientra pertanto il trasferimento ad altri di valori contraffatti, che dà luogo al più grave delitto di messa in circolazione di cui all'art. 459 c.p.



Il presupposto essenziale ai fini dell'applicazione del primo comma si ravvisa nella ricezione in mala fede, sanzionabile solamente ove sia seguita dall'uso.

La ricezione in buona fede è invece sanzionata dal secondo comma, che punisce il successivo utilizzo, stante l'acquisita susseguente consapevolezza della falsità del valore di bollo.

Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)

"Chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali, ovvero chiunque, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.500 a euro 25.000.

Soggiace alla pena della reclusione da uno a quattro anni e della multa da euro 3.500 a euro 35.000 chiunque contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati.

I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale."

La norma in oggetto tutela una versione commerciale della fede pubblica, la cui violazione porta con sé una potenziale lesione della fiducia dei consumatori riposta in quei mezzi simbolici di pubblico riconoscimento che, come il marchio, contraddistinguono i prodotti industriali e le opere dell'ingegno nella loro circolazione.

Per quanto riguarda la contraffazione, essa consiste nella riproduzione abusiva di un marchio o di altri segni distintivi, nei propri elementi essenziali, in modo idoneo a confondere i consumatori circa la provenienza del prodotto.

Con riferimento all'alterazione, questa si identifica come modifica del significato rappresentativo del marchio, nonché come la riproduzione parziale degli elementi emblematici del marchio, tale da generare confusione con il marchio originario.

L'uso di marchi contraffatti o alterati, invece, rappresenta un'ipotesi residuale che ricomprenda i casi di impiego commerciale e industriale di marchi, da altri falsificati, purché non sia riconducibile a quanto previsto all'art. 474 c.p.

Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

"Fuori dei casi di concorso nei delitti preveduti dall'articolo 473, chiunque introduce nel territorio dello stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati è punito con la reclusione da uno a quattro anni e con la multa da euro 3.500 a euro 35.000.



Fuori dei casi di concorso nella contraffazione, alterazione, introduzione nel territorio dello stato, chiunque detiene per la vendita, pone in vendita o mette altrimenti in circolazione, al fine di trarne profitto, i prodotti di cui al primo comma è punito con la reclusione fino a due anni e con la multa fin a euro 20.000.

I delitti previsti dai commi primo e secondo sono punibili a condizione che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale."

Tale reato si configura ove, al di fuori delle ipotesi di concorso nel reato di cui all'articolo 473 c.p., vengano introdotti nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o segni distintivi contraffatti o alterati.

La mera detenzione per la vendita, che si consuma non appena il soggetto sia entrato in possesso della merce contrassegnata, rappresenta invece una figura autonoma di reato, punita dal legislatore in maniera più lieve.

Con riferimento alla messa in vendita, questa si ravvisa anche qualora venga esclusivamente accertata la giacenza dei prodotti nei luoghi destinati all'esercizio del commercio.

Infine, la messa in circolazione comprende tutte le altre ipotesi di immissione sul mercato dei prodotti falsamente contrassegnati, che comportino la messa in contatto della merce con i consumatori.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione degli acquisti di beni e servizi

B) Gestione indiretta del reward shop

[OMISSIS]

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto alla commissione dei delitti in tema di falsità in strumenti o segni di riconoscimento, per conto o nell'interesse dell'Ente.

In via generale, a tali soggetti è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dagli articoli 25 bis, del D. Lgs. 231/2001.



Sempre in via generale, a tali soggetti è richiesto di:

- osservare rigorosamente tutte le norme poste dalla legge e dalle procedure aziendali interne in merito a limiti,
 condizioni e modalità con cui svolgere l'attività economico-commerciale dell'Ente;
- tenere condotte tali da garantire il libero e corretto svolgimento del commercio nonché di una lecita concorrenza nel rispetto della fede pubblica;
- astenersi da condotte commerciali finalizzate o comunque idonee a ledere la buona fede del consumatore/cliente ovvero il lecito affidamento del cittadino;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi
 individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di delitto in tema di
 falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

In particolare, è fatto divieto di:

- alterare ovvero contraffare attraverso qualsivoglia tipo di riproduzione marchi o segni distintivi nazionali ed esteri depositati/registrati ovvero fare uso di marchi o segni distintivi alterati oppure contraffatti;
- effettuare la vendita o comunque mettere in altro modo in circolazione, anche attraverso l'immagazzinamento finalizzato alla distribuzione, opere o prodotti con nomi, marchi o segni distintivi alterati o contraffatti, che possano produrre un danno per l'industria;
- effettuare la vendita o comunque mettere in altro modo in circolazione, anche attraverso l'immagazzinamento finalizzato alla distribuzione, opere o prodotti con nomi, marchi o segni distintivi altrui, anche se non registrati, al fine di trarre in inganno il consumatore/cliente.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile e referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano per conto o nell'interesse dell'Ente, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di falsità
 in strumenti o segni di riconoscimento, industria e commercio nonché in materia di diritto d'autore e dei diritti
 connessi);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della



normativa internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento) e di impegnarsi a tenere comportamenti conformi al dettato della norma;

• contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento - es. clausole risolutive espresse, penali).





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - F

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO



INDICE

<u>- P</u>	ARTE SPECIALE - F	<u> 79</u>
PR.	REMESSA	79
1.	LE TIPOLOGIE DI REATO	79
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	80
<u>3.</u>	IL SISTEMA DI CONTROLLO [OMISSIS]	80
4.	PRINCIPI GENERALI DI COMPORTAMENTO	80



- PARTE SPECIALE - F -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "F", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 bis 1 del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25 bis 1 ex D.lgs. n. 231/2001. Delitti contro l'industria e il commercio

Frodi contro le industrie nazionali (art. 514 c.p.)

"Chiunque, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagiona un nocumento all'industria nazionale, è punito con la reclusione da uno a cinque anni e con la multa non inferiore a cinquecentosedici euro.

Se per i marchi o segni distintivi sono state osservate le norme delle leggi interne o delle convenzioni internazionali sulla tutela della proprietà industriale, la pena è aumentata e non si applicano le disposizioni degli articoli 473 e 474."

Tale reato consiste nel mettere in vendita o in circolazione prodotti industriali falsamente contrassegnati, coincidendo pertanto, nei suoi elementi essenziali, con la condotta descritta all'art. 474 c.p. ("Introduzione nello Stato e commercio di prodotti con segni falsi"). Tuttavia, un elemento distintivo è ravvisabile nell'oggetto materiale, dal momento che l'art. 514 c.p. fa esclusivo riferimento ai prodotti industriali, in quanto si qualificherebbero come gli unici idonei ad arrecare nocumento per l'industria nazionale.



Un ulteriore elemento caratterizzante si ravvisa nel fatto che la tutela penale si estende alle falsità materiali riguardanti i nomi, ovvero tutti gli elementi di identificazione dei prodotti industriali che non fanno parte del marchio.

Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)

"Chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a due anni e con la multa fino a ventimila euro."

Il reato di cui sopra si realizza qualora vengano messi in vendita o in circolazione opere dell'ingegno o prodotti industriali con nomi, marchi o segni distintivi atti ad indurre in inganno il consumatore.

Per quanto riguarda la messa in circolazione, essa comprende un significato più ampio di messa in vendita, comprendendo tutte le forme, anche gratuite, di potenziale contatto del prodotto con il mercato dei consumatori, con l'inclusione delle attività di movimentazione della merce finalizzate alla vendita.

Il reato in esame si differenzia da quello previsto all'articolo 473 c.p. ("Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni") per la diversa connotazione del fatto tipico, dato che tale ultima disposizione richiede la sussistenza di una contraffazione tale da potersi confondere con il marchio originario.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione indiretta del reward shop

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto alla commissione dei delitti di cui all'articolo 25 bis 1, del D. Lgs. 231/2001, per conto o nell'interesse dell'Ente.

A tali soggetti è richiesto di:

• osservare rigorosamente tutte le norme poste dalla legge e dalle procedure e linee di condotta aziendali interne in merito a limiti, condizioni e modalità con cui svolgere l'attività economico-commerciale dell'Ente;



• astenersi da condotte commerciali finalizzate o comunque idonee a ledere la buona fede del consumatore/cliente ovvero il lecito affidamento del cittadino;

In particolare, è fatto divieto di:

- alterare ovvero contraffare attraverso qualsivoglia tipo di riproduzione marchi o segni distintivi nazionali ed esteri depositati/registrati ovvero fare uso di marchi o segni distintivi alterati oppure contraffatti;
- effettuare la vendita o comunque mettere in altro modo in circolazione opere o prodotti con nomi, marchi o segni distintivi alterati o contraffatti, che possano produrre un danno per l'industria;
- effettuare la vendita o comunque mettere in altro modo in circolazione opere o prodotti con nomi, marchi o segni distintivi altrui, anche se non registrati, al fine di trarre in inganno il consumatore/cliente.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile e referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano per conto o nell'interesse dell'Ente, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di falsità
 in strumenti o segni di riconoscimento, industria e commercio nonché in materia di diritto d'autore e dei diritti
 connessi);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di
 cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della
 normativa internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento)
 e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui
 al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa
 internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento es.
 clausole risolutive espresse, penali).



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - G
REATI SOCIETARI



INDICE

- PA	PARTE SPECIALE - G	<u> 84</u>
PR	REMESSA	84
1.	LE TIPOLOGIE DI REATO	<u> 84</u>
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	<u> 90</u>
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	<u> 90</u>
4.	PRINCIPI GENERALI DI COMPORTAMENTO	90



- PARTE SPECIALE - G-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "G", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati nell'art. 25 ter del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società, in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. n. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività e dell'attività della Società.

Art. 25 ter ex D.lgs. n. 231/2001. Reati societari.

I reati di seguito riportati tutelano la "trasparenza societaria" ed il patrimonio sociale. Fermo restando quanto di seguito dettagliato in riferimento alle singole attività sensibili, i rapporti con società private che potrebbero dare luogo alla commissione dei reati di corruzione di seguito elencati, sono stati identificati in quelli con tutti i soggetti privati che a vario titolo intrattengono relazioni con la Società (ad es. fornitori, aziende contributrici, etc.). Tra gli strumenti a disposizione della Società per la commissione dei reati di corruzione tra privati sono stati individuati, oltre alla mera dazione di danaro, anche la concessione di favori/benefici di qualsivoglia natura, in particolar modo in riferimento alla gestione del personale, a soggetti vicini ai soggetti apicali o al controllore della società interessata.

False comunicazioni sociali (art. 2621 c.c.)

"Fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica,



patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni.

La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi."

La contravvenzione di cui al presente articolo risulta strettamente connessa al delitto previsto all'art. 2622 c.c. ("False comunicazioni sociali in danno della società, dei soci o dei creditori"), che risulta integrato qualora la condotta punita come contravvenzione arrechi un danno ai soci e ai creditori.

Nello specifico, la contravvenzione di cui sopra viene posta a tutela del patrimonio societario, nonché della fiducia riposta da parte dei destinatari circa la veridicità dei bilanci e delle comunicazioni della società.

La falsità deve avere ad oggetto la situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene.

Infine, la suddetta contravvenzione può essere posta in essere sia attraverso una condotta commissiva ovvero tramite l'esposizione di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, oppure mediante l'omissione di informazioni imposte dalla legge.

Fatti di lieve entità (art. 2621-bis c.c.)

"Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942, n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale."

Impedito controllo (art. 2625 secondo comma c.c.)

"Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro.

Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione Europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58."



Il reato di cui all'art. 2625, comma 2 del codice civile, si verifica nell'ipotesi in cui gli amministratori impediscano od ostacolino, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali, procurando un danno ai soci.

Indebita restituzione dei conferimenti (art. 2626 c.c.)

"Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno."

Tale reato si realizza, *in primis*, attraverso la restituzione dei conferimenti ai soci, tale da determinare uno svuotamento del capitale sociale. La restituzione è idonea ad integrare il reato sia che avvenga in modo diretto, sia indirettamente tramite la compensazione con un debito del socio nei confronti della società.

La seconda modalità di realizzazione del reato è attraverso la liberazione dall'obbligo di eseguire i conferimenti, impedendo la regolare costituzione del capitale.

L'illecito di cui sopra costituisce un reato di danno, il cui evento è rappresentato dalla diminuzione del patrimonio netto, il quale deve scendere ad un valore inferiore del capitale nominale.

Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)

"Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno.

La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato."

Il reato di cui sopra, stante la genericità della ripartizione, può configurarsi anche tramite compensazioni, prestiti, anticipazioni, premi, compensi per prestazioni lavorative o professionali.

La consumazione del reato coincide con il momento in cui la società riceve un concreto pregiudizio economico.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

"Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno.

La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto."



Tale reato consiste nell'acquisto, riferibile ad ogni negozio che determini il trasferimento della titolarità delle azioni, ovvero nella sottoscrizione delle azioni stesse.

In entrambi i casi, la condotta deve comportare una lesione all'integrità del capitale sociale o delle riserve non distribuibili.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)

"Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Il risarcimento del danno ai creditori prima del giudizio estingue il reato."

Il suddetto reato si realizza tramite la riduzione del capitale sociale, la fusione con un'altra società oppure la scissione effettuate da parte degli amministratori.

Il reato è punibile ove sia idoneo ad arrecare un pregiudizio economico apprezzabile nei confronti dei creditori, la cui realizzazione rappresenta il momento consumativo del reato.

Formazione fittizia del capitale (art. 2632 c.c.)

"Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno."

Tale reato si può configurare tramite tre specifiche tipologie di condotta, tra cui, *in primis*, l'attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale, idonea a precludere l'integrale copertura del capitale nominale.

La seconda forma di condotta consiste nella sottoscrizione reciproca di azioni o quote, qualificata come ipotesi esemplare di creazione fittizia del capitale, la cui reciprocità non richiede la contestualità delle sottoscrizioni ma solamente la definizione di un previo accordo.

La terza condotta consiste nella sopravvalutazione rilevante dei conferimenti o del patrimonio della società in caso di trasformazione. In particolare, risulterà rilevante la sopravvalutazione che sia al di fuori della prassi di mercato, mentre la rilevanza risulta strettamente connessa al bene giuridico tutelato.

Per quanto riguarda la sopravvalutazione del patrimonio in caso di trasformazione, questa si può realizzare sia attraverso una sovrastima delle componenti attive, sia tramite una sottostima delle componenti passive. Inoltre, si fa riferimento esclusivamente alla trasformazione da società di persone in società di capitali o da società di capitali in altra dello stesso tipo, con l'esclusione della trasformazione da società di capitali a società di persone, dal momento che a quest'ultime la relativa sanzione non risulta applicabile.



Corruzione tra privati (art. 2635 c.c.)

"Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla Direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi.

Fermo quanto previsto dall'articolo 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date o promesse."

Tale ipotesi di reato rileva ai fini della responsabilità amministrativa dell'ente qualora i soggetti apicali e/o sottoposti, anche per interposta persona, offrano, diano o promettano denaro o altra utilità non dovuti a:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti privati²;
- coloro che, nell'ambito organizzativo della società o dell'ente privato, esercitino funzioni direttive diverse da quelle proprie dei soggetti di cui al punto che precede;
- coloro che siano sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui ai punti che precedono.

Si fa presente che l'ente risponderà del reato ai sensi del comma 3 dell'articolo in esame, quando i predetti soggetti agiscano come corruttori, non anche quando siano stati corrotti.

Istigazione alla corruzione tra privati (art. 2635 bis c.c.)

"Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta

² L'art 2635 c.c. punisce tali comportamenti anche quando l'accettazione dell'offerta, della dazione o della promessa da parte dei soggetti sopraelencati avviene per interposta persona.



un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo. La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per se' o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata. Si procede a querela della persona offesa."

Tale ipotesi di reato rileva ai fini della responsabilità amministrativa dell'ente qualora i soggetti apicali e/o sottoposti, offrano o promettano denaro o altra utilità non dovuti a:

- amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci
 e ai liquidatori di società o enti privati;
- coloro che svolgono un'attività lavorativa con l'esercizio di funzioni direttive di società o enti privati e
 l'offerta o la promessa non sia dagli stessi accettata.

Illecita influenza sull'assemblea (art. 2636 c.c.)

"Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno."

Tale reato si configura, *in primis*, nell'ipotesi in cui gli amministratori e i soci conferenti determinino la maggioranza assembleare con atti simulati, intesi come qualsiasi operazione in grado di alterare la formazione delle maggioranze richieste per l'approvazione delle delibere assembleari, al fine di conseguire risultati vietati dalla legge o dallo statuto della società.

Pertanto, risulta rilevante anche un'interposizione reale, e non fittizia, per l'esercizio del diritto di voto, poiché si dovrà verificare in concreto la sussistenza di un'eventuale situazione fittizia che abbia favorito il conseguimento di risultati vietati dalla legge o dallo statuto, attraverso un'indebita influenza sull'assemblea.

In secundis, la maggioranza assembleare può essere determinata anche mediante atti fraudolenti, consistenti in dichiarazioni mendaci tali da indurre in errore circa la convenienza della delibera del socio, oppure in una convocazione maliziosa dell'assemblea che impedisca una integrale partecipazione.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.1 e 2)

"Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al



vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Agli effetti della legge penale, le autorità e le funzioni di risoluzione di cui al decreto di recepimento della direttiva 2014/59/UE sono equiparate alle autorità e alle funzioni di vigilanza."

La fattispecie in esame è volta a tutelare le funzioni di controllo affidate alle Autorità di Vigilanza. La prima modalità di commissione del reato descritta al comma 1 consiste nell'esporre fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza.

La seconda modalità viene integrata qualora i soggetti non adempiano, in tutto o in parte, agli obblighi di comunicazione cui sono tenuti ed occultino informazioni relative alla predetta situazione.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

4. Principi generali di comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle attività "sensibili" rispetto ai delitti di cui all'art. 25 ter, D.Lgs. n. 231/2001 per l'espletamento della propria attività lavorativa in favore della Società.

In relazione ai reati in esame, fermo quanto previsto dalle altre Sezioni della Parte speciale del Modello, l'Ente adotta i seguenti principi generali di comportamento:

 assicurare l'osservanza dei principi di verità e correttezza con riferimento a qualunque documento giuridicamente rilevante nel quale si evidenzino elementi economici, patrimoniali e finanziari della società (o del Gruppo al quale appartiene);



 tenere (nello svolgimento di tutte le attività finalizzate alla formazione del bilancio) un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e regolamentari nonché delle policy/linee di condotta aziendali interne.

In particolare, è fatto divieto di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria dell'Ente;
- omettere di comunicare dati e informazioni richiesti dalla normativa e dalle policy/linee di condotta in vigore riguardo alla situazione economica, patrimoniale e finanziaria dell'Ente;
- adottare procedure e comportamenti in contrasto con i principi e le prescrizioni delle norme di legge e delle regole contabili dell'Ente;
- assumere comportamenti che possano integrare la fattispecie criminosa prevista dall'articolo 377-bis del codice penale (al riguardo si rinvia all'apposita Sezione della Parte Speciale del Modello: Sezione dedicata al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria);
- osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del
 patrimonio e agire sempre nel rispetto delle policy/linee di condotta aziendali che su tali norme si fondano,
 al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo;
- assicurare il regolare funzionamento dell'Ente e degli Organi Sociali garantendo ed agevolando ogni
 forma di controllo interno sulla gestione sociale previsto dalla legge o dalle policy/linee di condotta di
 controllo aziendale;
- astenersi dal porre in essere comportamenti che possano costituire "corruzione tra privati" (ex dell'art. 2635, c.c.).

In particolare, con riferimento a quest'ultima ipotesi delittuosa è fatto divieto di:

- promettere o effettuare dazioni indebite di denaro o riconoscimenti indebiti di altra utilità (es.: contratti di consulenza/collaborazione con finalità corruttive);
- distribuire omaggi e regalie in contrasto con le regole aziendali;
- effettuare promesse di assunzione o assunzioni in favore di soggetti segnalati dall'interlocutore/referente privato al fine di ottenere indebiti benefici o vantaggi derivanti da comportamenti scorretti dell'interlocutore.



Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001

PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - H

REATI CONTRO LA PERSONALITÀ INDIVIDUALE



INDICE

<u>- P</u>	PARTE SPECIALE - H	94
PREMESSA		94
<u>1.</u>	LE TIPOLOGIE DI REATO	94
<u>2.</u>	LE ATTIVITÀ SENSIBILI <i>[OMISSIS]</i>	95
<u>3.</u>	IL SISTEMA DI CONTROLLO [OMISSIS]	95
4	PRINCIPI GENERALI DI COMPORTAMENTO	96



- PARTE SPECIALE - H -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "H", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 quinquies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Il reato di intermediazione illecita e sfruttamento del lavoro, inserito nella sezione del codice penale diretta alla repressione dei delitti contro la personalità individuale, punisce, non tanto la privazione dello *status libertatis* quanto piuttosto la dignità di essere umano. Fermo restando quanto di seguito dettagliato in riferimento alle singole attività sensibili, i rapporti che potrebbero dare luogo alla commissione del reato *de quo* sono stati identificati in tutti quelli che concernono la gestione degli acquisti.

Art. 25-quinquies ex D.lgs. n. 231/2001. Delitti contro la personalità individuale.

Intermediazione illecita e sfruttamento del lavoro (Art. 603 bis c.p.)

"Salvo che il fatto costituisca più grave reato, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:

1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;

2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.



Se i fatti sono commessi mediante violenza o minaccia, si applica la pena della reclusione da cinque a otto anni e la multa da 1.000 a 2.000 euro per ciascun lavoratore reclutato.

Ai fini del presente articolo, costituisce indice di sfruttamento la sussistenza di una o più delle seguenti condizioni:

1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;

2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;

3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;

4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Costituiscono aggravante specifica e comportano l'aumento della pena da un terzo alla metà:

1) il fatto che il numero di lavoratori reclutati sia superiore a tre;

2) il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;

3) l'aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro"

Il reato si configura quando l'attività di mediazione tra domanda e offerta di lavoro che presenti il requisito dell'organizzazione sia volta o al reclutamento della manodopera o all'organizzazione di un'attività caratterizzata dallo sfruttamento dei lavoratori. Tale attività di mediazione deve, inoltre, essere condotta con le modalità della violenza, della minaccia o dell'intimidazione oppure approfittando dello stato di bisogno o di necessità del lavoratore.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione degli acquisti di beni e servizi

[OMISSIS]



4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto alla commissione dei delitti di cui all'articolo 25 quinquies del D. Lgs. 231/2001, per conto o nell'interesse dell'Ente.

In relazione alla suddetta attività sensibile:

- si deve richiedere l'impegno dei collaboratori esterni e dei fornitori al rispetto degli obblighi di legge in tema di tutela del lavoro minorile e delle donne, condizioni igienicosanitarie e di sicurezza, diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del paese in cui essi operano;
- la selezione delle controparti destinate a fornire particolari servizi (quali ad esempio le imprese con alta incidenza di manodopera non qualificata), siano essi partner o fornitori, deve essere svolta con particolare attenzione e in base ad apposita procedura. In particolare, l'affidabilità di tali partner o fornitori deve essere valutata anche attraverso specifiche indagini *ex ante*;
- nel processo di assunzione diretta di personale, deve essere verificato il rispetto delle norme giuslavoristiche e degli accordi sindacali per l'assunzione e il rapporto di lavoro in generale;
- nei contratti con i collaboratori esterni e i fornitori deve essere contenuta apposita dichiarazione dei medesimi
 con cui si affermi di essere a conoscenza della normativa di cui al Decreto oltre che delle sue implicazioni per
 il Gruppo American Express e di non essere mai stati indagati negli ultimi 10 anni in procedimenti giudiziari
 relativi ai reati nello stesso contemplati o se lo sono stati, devono comunque dichiararlo in caso si addivenga
 all'instaurazione del rapporto di consulenza o fornitura.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente di Payback o il referente interno, in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - I

I REATI CONNESSI CON LA VIOLAZIONE DELLE NORME IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO



INDICE

<u>- P</u>	ARTE SPECIALE - I	99
PR]	EMESSA	99
<u>1.</u>	LE TIPOLOGIE DI REATO	99
2.	LE ATTIVITÀ SENSIBILI <i>[OMISSIS]</i>	101
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	101
4.	PRINCIPI GENERALI DI COMPORTAMENTO	101



- PARTE SPECIALE - I -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "I", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 septies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25-septies ex D.lgs. n. 231/2001. Omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Il reato di omicidio colposo (art. 589 c.p.) e lesioni personali colpose gravi e gravissime (art. 590 c.p.) si configura nel caso in cui la condotta del soggetto abbia cagionato, per colpa, la morte di un uomo oppure una lesione personale dalla quale è derivata una malattia grave o gravissima.

Il reato costituisce presupposto della responsabilità amministrativa degli enti soltanto se commesso in violazione delle norme sulla sicurezza e prevenzione degli infortuni sul lavoro.

Si rileva che, generalmente, i reati considerati dal Decreto sono di natura dolosa, ossia posti in essere volontariamente dal soggetto con lo scopo specifico di commettere il reato, e il Modello organizzativo ha una funzione esimente della responsabilità della Società solo ove il soggetto agente abbia agito eludendo fraudolentemente le previsioni del Modello. I reati considerati nell'ambito della presente Parte Speciale sono, al contrario, di natura colposa, ossia conseguenza di negligenza, imprudenza, imperizia o inosservanza di leggi e regolamenti da parte dell'autore del reato, e pertanto la funzione di esimente del Modello organizzativo, è rappresentata dall'introduzione di previsioni volte a far sì che i Destinatari pongano in essere una condotta



rispettosa delle procedure previste dal sistema di prevenzione e protezione ai sensi del D.lgs. n. 81/2008 (Testo Unico in materia di Salute e Sicurezza sul lavoro), congiuntamente agli adempimenti e agli obblighi di vigilanza previsti dal Modello organizzativo.

Si tratta, pertanto, di uno dei pochi casi - unitamente a quanto previsto in materia di illeciti ambientali - in cui il presupposto per la responsabilità dell'ente è ancorato ad un fatto colposo e non doloso; ciò comporta la necessità di valutare i rischi secondo parametri differenti rispetto a quelli utilizzati per la responsabilità dolosa.

Omicidio colposo (art. 589 c.p.)

"Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni.

Se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni.

Se il fatto è commesso nell'esercizio abusivo di una professione per la quale è richiesta una speciale abilitazione dello Stato o di un'arte sanitaria, la pena è della reclusione da tre a dieci anni.

Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici."

Il reato si configura nel caso in cui, violando le norme sulla tutela della salute e della sicurezza sul lavoro, si cagioni per colpa la morte di una persona.

Lesioni personali colpose (art. 590 c.p.)

"Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309.

Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239.

Se i fatti di cui al secondo comma sono commessi con violazione delle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

Se i fatti di cui al secondo comma sono commessi nell'esercizio abusivo di una professione per la quale è richiesta una speciale abilitazione dello Stato o di un'arte sanitaria, la pena per lesioni gravi è della reclusione da sei mesi a due anni e la pena per lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni.

Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo; ma la pena della reclusione non può superare gli anni cinque.

Il delitto è punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale".



Il reato si configura nel caso in cui si cagionino per colpa lesioni gravi o gravissime ad una persona, a seguito della violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Le lesioni si considerano gravi nel caso in cui: a) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; b) il fatto produce l'indebolimento permanente di un senso o di un organo (art. 583, comma 1, c.p.).

Le lesioni si considerano gravissime se dal fatto deriva: a) una malattia certamente o probabilmente insanabile; b) la perdita di un senso; c) la perdita di un arto o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; d) la deformazione, ovvero lo sfregio permanente del viso (art. 583, comma 2, c.p.).

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza nei luoghi di lavoro

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

L'applicazione dei principi di comportamento oggetto del presente paragrafo segue un doppio binario; in particolare, unitamente ai precetti che tutti i dipendenti/collaboratori sono obbligati a rispettare, sono di seguito elencati i comportamenti di natura "preventiva" che l'Ente è tenuto ad adottare al fine di garantire l'incolumità dei suoi dipendenti/collaboratori e, di conseguenza, evitare il verificarsi di qualsivoglia evento che possa comportare l'insorgenza della responsabilità dell'Ente ai sensi del D.Lgs. n. 231/2001.

In via generale, a tutti i Destinatari del presente Modello è richiesto di:

- osservare rigorosamente tutte le norme poste dalla legge e dalle procedure e linee di condotta aziendali interne in materia di salute, sicurezza e igiene sul lavoro;
- garantire che siano comunicati tempestivamente al Responsabile del Sistema, ai Dirigenti delegati, al Responsabile del Servizio Protezione e Prevenzione designato dall'azienda, nonché all'Organismo di Vigilanza, qualsivoglia informazione relativa a infortuni avvenuti a collaboratori/dipendenti nell'esercizio della propria attività professionale che possano avere impatti sui regimi di responsabilità ex D.Lgs. n. 231/2001, anche qualora il verificarsi dei suddetti avvenimenti non abbia comportato la violazione del Modello;



- garantire che siano prontamente segnalate al Responsabile del Sistema e all'Organismo di Vigilanza possibili aree di miglioramento e/o eventuali gap procedurali riscontrati sul luogo di lavoro sia da parte di soggetti con responsabilità codificate in termini di sicurezza (RSPP, Addetti al servizio di SPP, RSL, Medico Competente) sia da parte dei soggetti in posizione apicale che abbiano ricevuto apposite segnalazioni in tal senso da parte dei propri collaboratori/sottoposti;
- non realizzare condotte volte a esercitare nei confronti dei soggetti coinvolti pressioni (anche basate sul grado
 o sulla funzione ricoperta all'interno dell'azienda) per ottenere comportamenti elusivi dei protocolli di seguito
 riportati. I soggetti coinvolti devono segnalare all'Organismo di Vigilanza l'eventuale esistenza di tali
 condotte o l'instaurarsi di prassi di questo genere.

Inoltre, il Datore di lavoro:

- provvede affinché i luoghi di lavoro siano conformi alle prescrizioni della normativa vigente in materia di salute e sicurezza sul lavoro;
- designa il Responsabile e gli Addetti al Servizio di Prevenzione e Protezione, in base ai requisiti richiesti dall'articolo 32 del D.Lgs. n. 81/2008;
- nomina, ovvero delega formalmente altro soggetto qualificato, il Medico competente per l'effettuazione della sorveglianza sanitaria, in base ai requisiti di cui all'articolo 38 del D.Lgs. n. 81/2008.
- effettua la valutazione dei rischi presenti in azienda, in collaborazione con il RSPP e il Medico competente, previa consultazione del Rappresentante dei lavoratori per la sicurezza (RLS);
- redige una relazione sulla valutazione dei rischi per la sicurezza e la salute (DVR) che abbia data certa, specificando i criteri adottati per la valutazione stessa, le misure di prevenzione e di protezione e dei dispositivi di protezione individuale adottati, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
- fornisce, tramite soggetto a ciò delegato, ai lavoratori i necessari e idonei dispositivi di protezione individuale (ove necessari);
- garantisce, direttamente ovvero tramite soggetto a ciò delegato, l'implementazione e l'aggiornamento delle misure di prevenzione;
- assicura, tramite soggetto a ciò delegato, che sia fornita formazione ai dipendenti, adeguata agli eventuali
 rischi specifici della mansione, in materia di sicurezza sia in occasione dell'assunzione che del trasferimento
 ad altre mansioni;
- adotta, direttamente ovvero tramite soggetto a ciò delegato, provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o l'altrui sicurezza.



Il Servizio di prevenzione e protezione, attraverso il proprio Responsabile (RSPP):

- collabora con il Datore di lavoro all'individuazione e valutazione dei fattori di rischio al fine di individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente;
- elabora, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del menzionato Decreto e dei sistemi di controllo di tali misure;
- elabora le procedure di sicurezza per le attività aziendali;
- propone programmi di informazione e formazione dei lavoratori;
- assicura che sia fornita adeguata informazione ai dipendenti sui rischi generali e specifici connessi all'attività di impresa, sulle procedure di primo soccorso e antincendio, sulle misure di prevenzione e protezione adottate.

Il Medico competente:

- collabora con il Datore di Lavoro, con il Dirigente delegato e con il Servizio di Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori;
- svolge l'attività di sorveglianza sanitaria attraverso l'effettuazione di visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti;
- esprime il giudizio di idoneità/inidoneità specifica alla mansione;
- collabora all'attività di informazione e formazione dei lavoratori e alla predisposizione del servizio di pronto soccorso.

I Rappresentanti dei Lavoratori per la Sicurezza:

- accedono ai luoghi di lavoro;
- sono consultati preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- sono consultati sulla designazione del RSPP, degli ASPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso;
- sono consultati in merito all'organizzazione delle attività formative;
- avvertono il Datore di Lavoro dei rischi individuati nel corso della loro attività e promuovono l'elaborazione,
 l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;



• possono far ricorso alle autorità competenti qualora ritengano che le misure di prevenzione e protezione dai rischi adottate dal Datore di lavoro o dai Dirigenti e i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

L'Ente programma e svolge attività di audit con riferimento al rispetto delle procedure e delle istruzioni di lavoro impartite ai lavoratori, elaborando un sistema che preveda chiaramente ruoli e responsabilità. Al termine dell'attività di monitoraggio è elaborato un verbale che attesti eventuali carenze e indichi le azioni correttive da intraprendere.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di Dipendente) o referente interno (in caso di soggetti terzi) ed inoltrare formale segnalazione all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano per conto o nell'interesse dell'Ente, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di falsità
 in strumenti o segni di riconoscimento, industria e commercio nonché in materia di diritto d'autore e dei diritti
 connessi);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento) e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui
 al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa
 internazionale e locale relativa ai delitti in materia di falsità in strumenti o segni di riconoscimento es.
 clausole risolutive espresse, penali).



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - J

REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO



INDICE

<u>- P</u>	PARTE SPECIALE - J	107
PR	REMESSA	107
<u>1.</u>	LE TIPOLOGIE DI REATO	
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	110
<u>3.</u>	IL SISTEMA DI CONTROLLO [OMISSIS]	110
4.	PRINCIPI GENERALI DI COMPORTAMENTO	111



- PARTE SPECIALE - J-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "J", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 octies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Il reato di ricettazione tutela il patrimonio e l'amministrazione della giustizia contro comportamenti in grado di recare danno ad entrambi tali beni giuridici. Fermo restando quanto di seguito dettagliato in riferimento alle singole attività sensibili, i rapporti che potrebbero dare luogo alla commissione del reato *de quo* sono stati identificati in tutti quelli che concernono l'utilizzo di danaro ovvero la gestione degli acquisti e la gestione degli incassi e dei pagamenti.

Art. 25-octies ex D.lgs. n. 231/2001. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio.

Ricettazione (art. 648 c.p.)

"Fuori dei casi di concorso nel reato, chi, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare, è punito con la reclusione da due ad otto anni e con la multa da cinquecentosedici euro a diecimilatrecentoventinove euro. La pena è aumentata quando il fatto riguarda denaro o cose provenienti da delitti di rapina aggravata ai sensi dell'articolo 628, terzo comma, di estorsione aggravata ai sensi dell'articolo 629, secondo comma, ovvero di furto aggravato ai sensi dell'articolo 625, primo comma, n. 7-bis).



La pena è della reclusione sino a sei anni e della multa sino a cinquecentosedici euro, se il fatto è di particolare tenuità.

Le disposizioni di questo articolo si applicano anche quando l'autore del delitto, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale delitto."

Il delitto di ricettazione può essere integrato da chiunque, fuori dai casi di concorso nel reato, acquista, riceve od occulta denaro o cose provenienti da delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.

La ricettazione presuppone, per la sua integrazione, che venga commesso un altro reato, il cosiddetto "reato presupposto".

L'acquisto viene inteso in senso lato comprensivo di ogni negozio, a titolo gratuito od oneroso, idoneo al trasferimento della cosa nella sfera patrimoniale dell'acquirente. La ricezione fa riferimento a qualsiasi forma di conseguimento del possesso del bene proveniente dal delitto - anche diversa dunque dalla compravendita - che si realizzi anche solo in via temporanea o per mera compiacenza.

La ricettazione può realizzarsi anche mediante l'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa, per la cui integrazione è sufficiente che il mediatore metta in contatto, anche in modo indiretto, le parti.

Perché l'autore dei fatti sia punibile per il delitto di ricettazione è necessario che agisca con dolo - anche nella forma eventuale - ossia che sia a conoscenza o nel ragionevole dubbio della provenienza illecita del denaro o delle cose e le voglia acquistare, ricevere, occultare o, dolosamente, voglia intromettersi nel favorire queste condotte con la consapevolezza di raggiungere - o di far raggiungere a terzi - un profitto dal reato. L'assenza del dolo tipico della ricettazione potrebbe portare, in ogni caso, ad una incriminazione per incauto acquisto (art. 712 c.p.), reato tuttavia non rilevante ai fini del D.lgs. n. 231/2001.

Riciclaggio (art. 648 bis c.p.)

"Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da milletrentadue euro a quindicimilaquattrocentonovantatre euro.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

Si applica l'ultimo comma dell'articolo 648."

La norma in esame codifica un reato plurioffensivo, dato che, oltre al patrimonio, vengono tutelati altri beni giuridici come l'amministrazione della giustizia, l'ordine pubblico, l'ordine economico-finanziario.



Il denaro, la cosa o l'utilità oggetto della condotta devono essere di provenienza delittuosa, ma con esclusivo riferimento al delitto colposo. Solamente i delitti colposi e le contravvenzioni non possono fungere da presupposto del riciclaggio.

Le condotte incriminate sono le seguenti:

- la sostituzione, ovvero l'attività diretta alla ripulire l'oggetto del delitto presupposto, in modo da elidere un collegamento con l'attività criminosa precedente;
- il trasferimento, configurabile come una specificazione della sostituzione, in quanto si sostanzia nello spostamento dei valori di provenienza illecita da un soggetto ad un altro, in modo da far perdere le tracce della provenienza, della titolarità e della effettiva destinazione;
- le altre operazioni per ostacolare l'identificazione, formulazione intesa a rendere il riciclaggio un reato a forma libera.

Ai fini della consumazione del suddetto reato, occorre che l'agente abbia realizzato la sostituzione e il trasferimento e che tali condotte siano idonee ad ostacolare l'identificazione della provenienza delittuosa del bene.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.)

"Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da cinquemila euro a venticinquemila euro.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

La pena è diminuita nell'ipotesi di cui al secondo comma dell'art. 648.

Si applica l'ultimo comma dell'articolo 648."

Tale reato comporta la punibilità dell'attività finale della commissione di illeciti di natura patrimoniale, concretantesi nell'investimento produttivo dei proventi illeciti.

Dal momento che l'impiego va riferito ad attività economiche o finanziarie, con queste si fa riferimento a qualsiasi settore idoneo a far conseguire i profitti, come le attività collegate alla circolazione di denaro o titoli, attività di intermediazione, attività relative alla produzione e circolazione di beni e servizi.

Il delitto si consuma nel momento dell'impiego dei proventi illeciti, il quale lo rende un'ipotesi di reato a consumazione prolungata.

Autoriciclaggio (art. 648 ter 1 c.p.)

"Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla



commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni.

Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

Si applica l'ultimo comma dell'articolo 648."

La norma, al fine di evitare la violazione del principio di offensività, richiede che la condotta sia "concretamente" idonea ad ostacolare l'identificazione dell'origine delittuosa dei beni. Con la precisazione apportata dall'avverbio "concretamente", si è voluto incriminare solamente quelle condotte che consistano in attività effettivamente idonee ad ostacolare l'identificazione e l'accertamento della provenienza delittuosa.

Per quanto concerne l'attività economica rispetto alla quale il bene può essere impiegato, sostituito o trasferito questa si qualifica come la produzione e lo scambio di beni e servizi, tale da ricomprendere il concetto di attività imprenditoriale.

Con riferimento alle attività finanziarie, si intendono tutte le attività economiche aventi ad oggetto gli strumenti finanziari. L'attività speculativa è configurabile come l'idea di perseguire il massimo guadagno con rischio elevato, purché in attività commerciali e finanziarie.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione dei flussi monetari e finanziari



[OMISSIS]

B) Gestione degli acquisti di beni e servizi

[OMISSIS]

C) Gestione dei rapporti infragruppo

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

Ai Destinatari del presente Modello è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato di ricettazione, riciclaggio, impiego di denaro, beni o altre utilità di provenienza illecita previste dall'articolo 25 *octies* del D.Lgs. n. 231/2001.

In particolare, a tali soggetti è richiesto di:

- ottemperare a quanto stabilito da norme di legge e dalle procedure e linee di condotta aziendali interne, in tutte le attività finalizzate alla gestione dei rapporti commerciali con fornitori/clienti/partner anche stranieri e alle conseguenti attività contabili e amministrative;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
- effettuare un costante monitoraggio dei flussi finanziari aziendali.

Pertanto, nella gestione delle attività in esame, l'Ente:

- gestisce un'anagrafica di clienti e fornitori e di corretta gestione contabile dei rapporti con gli stessi;
- verifica i flussi di entrata ed uscita merci e, in generale, la corrispondenza tra quanto fatturato e quanto pagato;
- nei casi in cui si renda necessario verificare l'affidabilità commerciale e professionale di fornitori, clienti e
 partner procede attraverso la richiesta di informazioni (ad es. certificati camerali) o l'interrogazione di banche
 dati specializzate;
- effettua controlli sia formali che sostanziali dei flussi finanziari (anche infragruppo) in entrata ed uscita;
- rifiuta di effettuare/ricevere pagamenti in denaro contante e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori alle soglie stabilite dal D.Lgs. 231/2007 e s.m.i., se non tramite intermediari a ciò abilitati da tale Decreto (banche e Poste Italiane S.p.A.);



- implementa un sistema interno di gestione dei pagamenti che preveda un *iter* standardizzato di autorizzazioni a livelli successivi nel caso in cui il personale addetto riscontri casi di possibile anomalia ai sensi di quanto ai punti precedenti;
- comunica all'Agenzia delle Entrate tutte le cessioni di beni e le prestazioni di servizi effettuate e ricevute, registrate o soggette a registrazione, nei confronti di operatori economici aventi sede, residenza o domicilio in Paesi cosiddetti "black list".

Ferme tutte le altre prescrizioni e regole aziendali, in caso di dubbi circa la corretta attuazione dei principi eticocomportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente dell'ente) o referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse dell'ente, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a
 comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti
 dal Decreto);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di
 cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della
 normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti
 ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti
 conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. n. 231/2001 e del Modello (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es.: clausole risolutive espresse, penali).

Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - K

DELITTI IN MATERIA DI VIOLAZIONI DEL DIRITTO DELLA PROPRIETÀ INTELLETTUALE



INDICE

<u>- P</u>	PARTE SPECIALE - K	115
<u>PR</u>	REMESSA	115
<u>1.</u>	LE TIPOLOGIE DI REATO	115
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	119
<u>3.</u>	IL SISTEMA DI CONTROLLO [OMISSIS]	119
4.	PRINCIPI GENERALI DI COMPORTAMENTO	119



- PARTE SPECIALE - K -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "K", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 novies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società. del reato de quo sono stati identificati in tutti quelli che concernono la gestione degli acquisti.

Art. 25-novies ex D.lgs. n. 231/2001. Delitti in materia di violazioni del diritto della proprietà intellettuale

Divulgazione di opere dell'ingegno attraverso rete telematica (art. 171 L. 633/1941)

"Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;



c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) (soppresso)

f) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da due a dieci milioni di lire."

Reati in materia di software e banche dati (art. 171 bis L. 633/1941)

"Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità."



Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche (art. 171 ter L. 633/1941)

"È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da cinque a trenta milioni di lire chiunque a fini di lucro (1):

- a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
- b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;
- c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
- d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato (2);
- e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
- f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;
- f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale (3).



h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (4).

È punito con la reclusione da uno a quattro anni e con la multa da cinque a trenta milioni di lire chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi:

a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante concessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (5);

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma l;

c) promuove o organizza le attività illecite di cui al comma 1.

La pena è diminuita se il fatto è di particolare tenuità.

La condanna per uno dei reati previsti nel comma 1 comporta:

- a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale
- b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale (6);
- e) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici."

Violazioni nei confronti della SIAE (art. 171 septies L. 633/1941)

"La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge."



2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione della riproduzione, trasmissione o diffusione al pubblico di opere dell'ingegno protette dal diritto d'autore o da altri diritti connessi

[OMISSIS]

B) Gestione dei sistemi informativi

[OMISSIS]

4. Principi generali di comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto alla commissione dei delitti in materia di violazione del diritto d'autore, per conto o nell'interesse dell'Ente.

In via generale, a tali soggetti è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 25 *novies* (relativamente alla violazione della normativa posta a tutela del diritto d'autore) del D.Lgs. n. 231/2001.

In particolare, è fatto divieto di:

- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione al fine di trarne profitto beni/opere realizzati usurpando il diritto d'autore o brevetti di terzi;
- diffondere tramite reti telematiche un'opera dell'ingegno o parte di essa tutelata dal diritto d'autore;
- procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale
 o comunque per trarne profitto programmi per elaboratori ovvero qualsiasi opera protetta dal diritto
 d'autore e da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico,
 artistico;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui.



In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente dell'Ente) e referente interno (in caso di soggetti terzi) e inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano per conto o nell'interesse dell'Ente, i relativi contratti devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero
 o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di diritto
 d'autore e dei diritti connessi);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di diritto d'autore e dei diritti connessi) e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. n. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa ai delitti in materia di diritto d'autore e dei diritti connessi) (es. clausole risolutive espresse, penali).





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - L

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA



INDICE

<u>- P</u>	PARTE SPECIALE - L		
<u>PR</u>	EMESSA	123	
<u>1.</u>	LE TIPOLOGIE DI REATO	123	
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]		
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	124	
4.	PRINCIPI GENERALI DI COMPORTAMENTO	124	



- PARTE SPECIALE - L -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha

esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and

Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania,

American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal

D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di

verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "L", si provvede qui di seguito a fornire una breve descrizione dei

reati in essa contemplati, indicati all'art. 25 decies del Decreto Legislativo 231/2001 e ritenuti potenzialmente

realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs.

231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle

Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state

effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali

provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della

Società.

Art. 25-decies ex D.lgs. n. 231/2001

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria (Art. 377-

bis c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di

denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona

chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando

questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni."

L'art. 377 bis c.p. punisce chi induce (mediante violenza o minaccia o con l'offerta o la promessa di danaro o altra

utilità) a non rendere dichiarazioni o a rendere dichiarazioni mendaci, la persona chiamata a rendere dichiarazioni

utilizzabili in un procedimento penale, quando tale soggetto ha la facoltà di non rispondere.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

123



3. IL SISTEMA DI CONTROLLO

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, sono coinvolti in un procedimento penale.

In particolare è fatto obbligo di:

- tenere un comportamento corretto, trasparente e collaborativo conformemente ai principi stabiliti dalle norme di legge, dalle procedure e policy aziendali.
- garantire che l'iniziativa economica non si svolga in contrasto con l'utilità sociale e, quindi, l'ordine pubblico.
- assicurare il regolare funzionamento dell'Ente, dei suoi organismi e delle sue funzioni, garantendo ed agevolando ogni forma di controllo interno sulle attività aziendali, che possano essere strumentali all'attuazione di comportamenti o condotte non conformi ai principi normativi sopra richiamati.
- non ostacolare in alcun modo lo svolgimento di eventuali indagini e iniziative da parte degli organi a ciò
 deputati, o più in generale da qualsiasi organo/ente ispettivo, finalizzate a rilevare e combattere condotte
 illecite in relazione all'ipotesi di reato considerata.

In relazione alla gestione dei rapporti con soggetti coinvolti in procedimenti giudiziari, ad amministratori e dipendenti della Società:

- è fatto obbligo di segnalare al General Counsel Officer la richiesta di rendere o produrre davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni;
- si vieta di indurre o favorire i soggetti coinvolti in procedimenti giudiziari a non rendere/produrre le suddette dichiarazioni, ovvero a renderle mendaci;
- si vieta di favorire i soggetti coinvolti in procedimenti giudiziari a eludere le investigazioni dell'Autorità o a sottrarsi alle ricerche di questa.

È inoltre fatto espresso obbligo ad ogni Destinatario di non porre in essere atti di violenza, minaccia (o altre forme analoghe di coartazione) ovvero di non dare o di non promettere elargizioni in danaro o altre forme di utilità affinché il soggetto indagato/imputato:

- non presti una fattiva collaborazione al fine di rendere dichiarazioni veritiere, trasparenti e correttamente rappresentative dei fatti;
- non esprima liberamente le proprie rappresentazioni dei fatti, esercitando la propria facoltà di non rispondere attribuita dalla legge, in virtù delle suddette forme di condizionamento.



Inoltre, all'Ente e ai propri dipendenti è fatto divieto di:

- predisporre i mezzi attraverso i quali supportare l'operatività della condotta illecita.
- promuovere o comunque proporre, la realizzazione di obiettivi delittuosi di volta in volta individuati come utili o necessari nell'ottica del conseguimento di un vantaggio per l'Ente.

Gli obblighi sopra rappresentati si intendono riferiti non solo ai rapporti instaurati con soggetti privati, ma anche ad interlocutori appartenenti alla Pubblica Amministrazione.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente di Payback o il referente interno, in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - M REATI AMBIENTALI



INDICE

<u>- P.</u>	PARTE SPECIALE - M	128
PR	REMESSA	128
<u>1.</u>	LE TIPOLOGIE DI REATO	128
<u>2.</u>	LE ATTIVITÀ SENSIBILI [OMISSIS]	129
<u>3.</u>	IL SISTEMA DI CONTROLLO [OMISSIS]	129
4	PRINCIPI GENERALI DI COMPORTAMENTO	129



- PARTE SPECIALE - M -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "M", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 undecies del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Societàin ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25-undecies ex D.lgs. n. 231/2001. Reati ambientali

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 D. Lgs. 152/2006)

"(comma IV): Le imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all'articolo 212, comma 8, che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all'articolo 188-bis, comma 2, lettera a), ed effettuano il trasporto di rifiuti senza il formulario di cui all'articolo 193 ovvero indicano nel formulario stesso dati incompleti o inesatti sono puniti con la sanzione amministrativa pecuniaria da milleseicento euro a novemilatrecento euro. Si applica la pena di cui all'articolo 483 del codice penale a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto."

Il reato previsto ai sensi dell'art. 258, comma quattro del D.lgs. 152/2006 si realizza qualora le imprese trasportino rifiuti non pericolosi, in assenza del formulario previsto ai sensi dell'art. 193 ovvero nel caso in cui, all'interno del suddetto formulario, siano stati riportati dati incompleti o inesatti.



La specifica relativa ai rifiuti non pericolosi risulta essenziale, dal momento che nel caso di trasporto di rifiuti pericolosi e di false certificazioni di analisi si applica la sanzione penale.

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione degli adempimenti in materia ambientale

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto alla commissione dei reati ambientali, per conto o nell'interesse dell'Ente.

È inoltre previsto l'espresso divieto di:

- assegnare a terzi le attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione ovvero in violazione di alcuni dei requisiti normativamente previsti per lo svolgimento di dette attività;
- costituire e/o gestire una discarica non autorizzata di rifiuti anche pericolosi;
- omettere i doverosi interventi di bonifica ovvero violare le disposizioni inerenti il progetto di bonifica
 approvato dall'autorità competente nel caso di eventi inquinanti del suolo, del sottosuolo, delle acque
 superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio, in violazione
 di quanto previsto dall'articolo 242 del D. Lgs. 152/2006 e s.m.i.;
- omettere la comunicazione dell'evento inquinante alle Autorità competenti, ai sensi della norma di cui al punto precedente;
- cedere, ricevere, trasportare, esportare, importare, o comunque gestire abusivamente ingenti quantitativi di rifiuti, anche radioattivi, effettuando più operazioni ovvero ricorrendo a mezzi e attività continuative organizzate, al fine di per conseguire un ingiusto profitto;
- predisporre un certificato di analisi dei rifiuti fornendo false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti ovvero inserire un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti;



 utilizzare durante il trasporto un certificato di analisi contenente false indicazioni su natura, composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati ovvero di una copia cartacea della scheda SISTRI fraudolentemente alterata.

In caso di dubbi circa la corretta attuazione dei principi etico - comportamentali di cui sopra nel corso dello svolgimento delle attività operative, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente della Società) o referente interno (in caso di soggetti terzi) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.

L'Ente inoltre, al fine di evitare il proprio coinvolgimento in attività suscettibili di concretizzare uno o più reati ambientali, si impegna a svolgere e a verificare che tali attività siano svolte responsabilmente e secondo le modalità idonee a garantire il rispetto dell'ambiente, ed in particolare:

- si adopera per una gestione dei rifiuti orientata al recupero, al reimpiego e al riciclaggio dei materiali, al fine di garantire un maggior grado di protezione della salute dell'uomo e dell'ambiente;
- affida le attività di raccolta, trasporto, recupero e smaltimento dei rifiuti esclusivamente ad imprese autorizzate e nel rispetto delle procedure aziendali relative alla qualificazione dei fornitori;
- in conformità a quanto previsto dalle disposizioni in materia ambientale, compila accuratamente e regolarmente il Modello Unico di Dichiarazione Ambientale;
- definisce i principali adempimenti da adottare in ambito aziendale in merito alla gestione delle diverse tipologie rifiuti - pericolosi e non pericolosi - al fine di operare in modo uniforme su tutto il territorio nazionale;
- provvede alla classificazione dei rifiuti prodotti nell'ambito delle attività aziendali in conformità a quanto stabilito dalle disposizioni legislative vigenti e dalle autorità competenti e a tal fine informa e fornisce adeguata formazione al personale delle unità produttive di rifiuti sulla base delle rispettive attribuzioni;
- garantisce che ogni unità produttiva di rifiuti tenga regolarmente il registro di carico e scarico e che lo stesso, unitamente ai formulari identificativi del rifiuto, sia compilato in modo corretto e veritiero, astenendosi dal porre in essere operazioni di falso ideologico o materiale (ad esempio in relazione alle informazioni sulle caratteristiche qualitative o quantitative dei rifiuti).
- istituisce presidi idonei a garantire il rispetto delle disposizioni normative relative al deposito dei rifiuti ed in particolare delle modalità e dei limiti quantitativi e temporali tempo per tempo vigenti;
- vigila costantemente sulla corretta gestione dei rifiuti segnalando eventuali irregolarità alle funzioni competenti.

Infine, nei confronti di terze parti contraenti (es.: Collaboratori esterni, consulenti, Partner, Fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura, coinvolte nello



svolgimento di attività a rischio rispetto ai reati ambientali e che operano per conto o nell'interesse della Società, i relativi contratti devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai reati ambientali);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di
 cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della
 normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti
 ai reati ambientali) e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai reati ambientali) (es. clausole risolutive espresse, penali).



PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - N

IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE



INDICE

<u>- P</u>	PARTE SPECIALE - N	
PR	REMESSA	134
<u>1.</u>	LE TIPOLOGIE DI REATO	134
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	135
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	135
4.	PRINCIPI GENERALI DI COMPORTAMENTO	135



- PARTE SPECIALE - N-

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "N", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, indicati all'art. 25 *duodecies* del Decreto Legislativo 231/2001 e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25-duodecies ex D.lgs. n. 231/2001. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 22, comma 12-bis, D.lgs. n. 286/1998)

"Il datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dal presente articolo, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, revocato o annullato, è punito con la reclusione da sei mesi a tre anni e con la multa di 5000 euro per ogni lavoratore impiegato.

Le pene per il fatto previsto dal comma 12 sono aumentate da un terzo alla metà:

- a) se i lavoratori occupati sono in numero superiore a tre;
- b) se i lavoratori occupati sono minori in età non lavorativa;
- c) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'articolo 603-bis del codice penale."

Il reato si configura quando il datore di lavoro occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno previsto dall' art. 22 del d.lgs. 286/98 ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge il rinnovo, revocato o annullato.



2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione degli acquisti di beni e servizi

[OMISSIS]

J) Gestione del processo di selezione e assunzione del personale

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti di tipo commerciale o comunque istituzionale con interlocutori terzi, pubblici o privati, per conto o nell'interesse della Società.

In particolare, i Destinatari sono tenuti a:

- richiedere l'impegno dei collaboratori esterni e dei fornitori al rispetto degli obblighi di legge in tema di tutela
 del lavoro minorile e delle donne, condizioni igienicosanitarie e di sicurezza, diritti sindacali o comunque di
 associazione e rappresentanza richiesti dalla normativa del paese in cui essi operano;
- svolgere con particolare attenzione la selezione delle controparti destinate a fornire particolari servizi (quali ad esempio le imprese con alta incidenza di manodopera non qualificata), siano essi partner o fornitori;
- nel processo di assunzione diretta di personale, verificare il rispetto delle norme giuslavoristiche e degli accordi sindacali per l'assunzione e il rapporto di lavoro in generale. Deve essere, altresì, verificato il rispetto delle regole di correttezza e di buon comportamento nell'ambiente di lavoro ed in ogni caso deve essere posta particolare attenzione a situazioni lavorative anormali o abnormi;
- qualora un partner, un collaboratore esterno o un fornitore abbiano la propria sede all'estero ed ivi venga svolta
 l'opera o la prestazione a favore di Payback, ad attenersi alla normativa locale o, se più severe, alle convenzioni
 ILO sull'età minima per l'accesso al lavoro e sulle forme peggiori di lavoro minorile ("C138 Convenzione
 sull'età minima 1973" e "C182 Convenzione sulle forme peggiori di lavoro minorile 1999");
- nei contratti con i collaboratori esterni e i fornitori, prevedere un'apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al Decreto oltre che delle sue implicazioni per il Gruppo American Express e di non essere mai stati indagati negli ultimi 10 anni in procedimenti giudiziari relativi ai reati nello stesso contemplati o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del rapporto di consulenza o fornitura;



• in caso persistano dubbi sulla correttezza di comportamenti dei collaboratori esterni e fornitori, l'Organismo di Vigilanza emetterà una raccomandazione per gli esponenti aziendali.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente di Payback o il referente interno, in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.





PAYBACK ITALIA S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE - O

REATI DI RAZZISMO E XENOFOBIA



INDICE

- P	ARTE SPECIALE - O	139
PR	REMESSA	139
<u>1.</u>	LE TIPOLOGIE DI REATO	
2.	LE ATTIVITÀ SENSIBILI [OMISSIS]	140
3.	IL SISTEMA DI CONTROLLO [OMISSIS]	140
4.	PRINCIPI GENERALI DI COMPORTAMENTO	140



- PARTE SPECIALE - O -

PREMESSA

Payback S.r.l. (di seguito anche la "Società" o l'"Ente"), sulla base di contratti di servizi infragruppo, ha esternalizzato i seguenti servizi: Tax, Accounting, Treasury, Global Real Estate, Human Resources, Health and Safety, Security, Payroll, Global Supply Management (AESEL), Information Technology (Payback Germania, American TRSco).

L'esternalizzazione delle attività non esime la Società dalla responsabilità per la commissione dei reati previsti dal D.lgs. n. 231/2001, rimanendo in capo all'Ente stesso il compito di vigilare sull'attività esternalizzata e di verificare l'osservanza delle previsioni di legge.

1. LE TIPOLOGIE DI REATO

Per quanto concerne la presente Parte Speciale "O", si provvede qui di seguito a fornire una breve descrizione dei reati in essa contemplati, previsti dall'art. 25-terdecies e ritenuti potenzialmente realizzabili all'interno della Società in ragione delle attività svolte e ritenute "sensibili" ai sensi del D.Lgs. 231/2001.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti (cd. Mappatura o "Matrice delle Attività a rischio-reato") e le considerazioni svolte sulla possibile realizzabilità dei predetti reati, sono state effettuate anche attraverso le interviste ai soggetti delle funzioni aziendali/unità di business competenti, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività della Società.

Art. 25-terdecies ex D.lgs. n. 231/2001. Razzismo e xenofobia

Al fine di adeguare il nostro ordinamento a quello comunitario, la Legge n. 167 del 20 novembre 2017, "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2017", ha previsto l'inserimento tra i reati di cui al D.lgs. n. 231/2001, del reato di istigazione e incitamento al razzismo e alla xenofobia con conseguente possibile responsabilità in capo alle società.

Razzismo e xenofobia (art. 3, comma 3 bis, L. n. 654/1975)

"È vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni."

I delitti richiamati dall'articolo 3, comma 3, della Legge 654/1975 puniscono ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali,



etnici, nazionali o religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi un concreto pericolo di diffusione.

Il suddetto reato si fonda, altresì, sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale (ratificato ex Legge 232/1999).

2. LE ATTIVITÀ SENSIBILI

[OMISSIS]

3. IL SISTEMA DI CONTROLLO

[OMISSIS]

A) Gestione delle attività di marketing

[OMISSIS]

4. PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, direttamente o indirettamente, siano coinvolti nelle attività "sensibili" rispetto ai delitti di cui all'art. 24 terdecies, D.Lgs. n. 231/2001 per l'espletamento della propria attività lavorativa in favore della Società.

In relazione ai reati in esame, fermo quanto previsto dalle altre Sezioni della Parte speciale del Modello, l'Ente adotta i seguenti principi generali di comportamento:

- Verifica, con l'ausilio dell'Advertising Review Board, che tutte le comunicazioni, prima della loro pubblicazione siano: i) allineate con la normativa; ii) trasparenti e non idonee a incitare e/o istigare al razzismo e alla xenofobia;
- Controlla e valuta il contenuto delle comunicazioni pubblicitarie, in modo tale da apportare le modifiche idonee ad evitare l'insorgenza del reato *ex* art. 3, comma 3 bis, L. n. 654/1975, per cui l'Ente verrebbe sanzionato ai sensi dell'art. 24 terdecies del D.Lgs. n. 231/2001.

In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente di Payback o il referente interno, in caso di soggetto terzo) ed inoltrare formalmente richiesta di parere all'Organismo di Vigilanza.