



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

DI

HBG ON LINE GAMING S.R.L.

AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

“Responsabilità amministrativa della Società”

DOCUMENTO APPROVATO IN DATA 24 FEBBRAIO 2017

INDICE

| | |
|----------------------------------------------------------------------------------------|----|
| SEZIONE PRIMA | 5 |
| 1 Il Decreto Legislativo 231/2001 | 5 |
| 1.1 <i>La Responsabilità Amministrativa degli Enti</i> | 5 |
| 1.2 <i>I reati previsti dal Decreto</i> | 5 |
| 1.3 <i>Le sanzioni previste dal Decreto</i> | 5 |
| 1.4 <i>Condizione esimente della Responsabilità amministrativa</i> | 6 |
| 1.5 <i>Le “Linee Guida” di Confindustria</i> | 7 |
| 1.6 <i>Delitti tentati e delitti commessi all’estero</i> | 8 |
| SEZIONE SECONDA | 9 |
| 2 Il Modello di Organizzazione, Gestione e Controllo di HBG On Line Gaming S.r.l. | 9 |
| 2.1 <i>Obiettivi e mission aziendale</i> | 9 |
| 2.2 <i>Modello di Governance</i> | 9 |
| 2.3 <i>Finalità del Modello</i> | 10 |
| 2.4 <i>Destinatari</i> | 11 |
| 2.5 <i>Struttura del Modello</i> | 11 |
| 2.6 <i>Elementi fondamentali del Modello</i> | 11 |
| 2.7 <i>Codice Etico e Modello</i> | 12 |
| 2.8 <i>Presupposti del Modello</i> | 12 |
| 2.9 <i>Individuazione delle attività “a rischio”</i> | 13 |
| 2.10 <i>Procedure rilevanti in ambito 231</i> | 17 |
| 2.11 <i>Principi di controllo interno generali</i> | 17 |
| SEZIONE TERZA | 29 |
| 3 Organismo di Vigilanza..... | 29 |
| 3.1 <i>Identificazione dell’Organismo di Vigilanza</i> | 29 |
| 3.2 <i>Poteri e funzioni dell’Organismo di Vigilanza</i> | 30 |
| 3.3 <i>Reporting dell’Organismo di Vigilanza</i> | 30 |
| 3.4 <i>Flussi informativi nei confronti dell’Organismo di Vigilanza</i> | 31 |
| SEZIONE QUARTA | 33 |
| 4 Sistema sanzionatorio | 33 |
| 4.1 <i>Destinatari e apparato sanzionatorio e/o risolutivo</i> | 33 |
| 5 Aggiornamento del Modello | 34 |
| 6 Informazione e formazione del personale | 34 |
| ALLEGATO A – FATTISPECIE DEI REATI | 35 |

ALLEGATO B – ARTICOLI DEL CODICE PENALE RICHIAMATI DALL’ART 4 DEL D.LGS.
231/2001.....41

DEFINIZIONI

| | |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ADM | Si intende l’Agenzia delle Dogane e dei Monopoli. |
| DECRETO | Il Decreto Legislativo 8 giugno 2001, n. 231 ¹ |
| DESTINATARI | I soggetti ai quali si applicano le regole di comportamento contenute nel Modello, meglio individuati al par. 2.4 del Modello medesimo |
| DIPENDENTI | Persone sottoposte alla direzione od alla vigilanza di uno dei soggetti apicali; quindi, ma non solo, tutti i soggetti – compresi i dirigenti - che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società nonché i lavoratori in distacco o in forza con contratti di lavoro parasubordinato |
| DOCUMENTO INFORMATICO | Qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati a rielaborarli |
| GRUPPO HBG (O SEMPLICEMENTE GRUPPO) | L’insieme delle società composto da HBG Gaming S.r.l. e dalle società direttamente e/o indirettamente controllate dalla medesima HBG Gaming S.r.l. (ivi compresa la HBG On Line Gaming S.r.l.) |
| LINEE GUIDA DI CONFINDUSTRIA | Le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 approvate da Confindustria nel mese di marzo 2014 e successive modifiche ed integrazioni |
| MODELLO DI ORGANIZZAZIONE E DI GESTIONE O MODELLO | Il presente Modello di organizzazione, gestione e controllo così come previsto ex D.Lgs. 231/2001 |
| ORGANISMO DI VIGILANZA O ODV | L’Organismo di vigilanza previsto dal D.Lgs. 231/2001 |
| PA | Pubblica Amministrazione |
| REATI | I reati di cui al Decreto legislativo 8 giugno 2001, n. 231 |
| SOCIETÀ | HBG On Line Gaming S.r.l. |
| SOGGETTI APICALI | Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione od il controllo della Società |
| HBG GAMING S.R.L. | Società Capogruppo |

¹ E successive integrazioni e modificazioni: tale precisazione vale per qualsivoglia legge, regolamento o complesso normativo, che siano richiamati nel Modello.

SEZIONE PRIMA

1 Il Decreto Legislativo 231/2001

1.1 La Responsabilità Amministrativa degli 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 il “Decreto”), 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 ha 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 nella quale sono coinvolti 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.

Con tale Decreto, dal titolo “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”, è stato introdotto nell’ordinamento italiano un regime di responsabilità amministrativa a carico di enti (società, associazioni, ecc. di seguito denominati “Enti”) per alcuni reati commessi, nell’interesse o vantaggio degli stessi da:

- persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa, dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità amministrativa degli Enti si aggiunge a 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.

1.2 I reati previsti dal Decreto

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell’ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche ed integrazioni.

Nell’“Allegato A – Fattispecie dei Reati”, sono elencati tutti i reati attualmente ricompresi nell’ambito di applicazione del Decreto.

1.3 Le sanzioni previste dal Decreto

Il sistema sanzionatorio, a fronte del compimento dei reati sopra elencati, prevede l’applicazione delle seguenti sanzioni amministrative:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca;
- pubblicazione della sentenza.

La sanzione pecuniaria è ridotta nel caso in cui: a) l’autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l’Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità, o se, prima della dichiarazione di apertura del dibattimento in primo grado: c) l’Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso e d) un Modello è stato adottato e reso operativo.

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, quando ricorre almeno una delle seguenti condizioni: a) l’Ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da

soggetti che ricoprono una posizione di rappresentanza, amministrativa o gestoria nell'Ente ovvero da soggetti sottoposti alla direzione al controllo dei primi e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; o b) in caso di reiterazione degli illeciti.

Il Decreto prevede le seguenti sanzioni interdittive, che possono avere una durata non inferiore a tre mesi e non superiore a due anni:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Ai sensi della vigente normativa, le sanzioni interdittive non si applicano in caso di commissione dei reati societari e di market abuse. Si precisa infatti che, per tali reati, sono previste le sole sanzioni pecuniarie, raddoppiate nel loro ammontare dall'art. 39, comma 5, della L. 262/2005 ("Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari").

Il Decreto prevede, inoltre, che, qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione interdittiva, possa disporre la prosecuzione dell'attività da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- la società svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

1.4 Condizione esimente della Responsabilità amministrativa

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nell'interesse o a vantaggio dell'Ente sia da soggetti apicali sia da dipendenti.

In particolare, nel caso di reati commessi da soggetti in posizione apicale, l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

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

Per quanto concerne i dipendenti, l'art. 7 prevede l'esonero nel caso in cui l'Ente abbia adottato ed efficacemente attuato prima della commissione del reato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede, inoltre, che il Modello, debba rispondere alle seguenti esigenze:

- 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.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sull' idoneità del Modello a prevenire i reati. Con riferimento ai reati ed illeciti amministrativi in materia di market abuse, tale valutazione di idoneità viene compiuta dal Ministero della Giustizia, sentita la Consob.

È infine previsto che, negli Enti di piccole dimensioni, il compito di vigilanza possa essere svolto direttamente dall'organo dirigente.

Con riferimento all'effettiva applicazione del Modello, il Decreto richiede:

- una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del Modello (cfr. par. 5 – “Aggiornamento del Modello”);
- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello.

1.5 Le “Linee Guida” di Confindustria

L'art. 6 del Decreto dispone espressamente che il Modello possa essere adottato sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Le Linee Guida di Confindustria sono state approvate dal Ministero della Giustizia con il D.M. 4 dicembre 2003. Il successivo aggiornamento, pubblicato da Confindustria in data 24 maggio 2004, è stato approvato dal Ministero della Giustizia, che ha giudicato tali Linee Guida idonee al raggiungimento delle finalità previste dal Decreto. Dette Linee Guida sono state aggiornate da Confindustria al mese di marzo 2014.

Nella definizione del Modello, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare i reati previsti dal Decreto;
- la predisposizione di un sistema di controllo² (i c.d. protocolli) idoneo a prevenire i rischi di reato identificati nella fase precedente, attraverso la valutazione del sistema di controllo esistente all'interno dell'ente ed il suo grado di adeguamento alle esigenze espresse dal Decreto.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del modello di organizzazione, gestione e controllo, sono le seguenti:

- la previsione di principi etici e di regole comportamentali in un codice etico;
- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e descrizione dei compiti con specifica previsione di principi di controllo;
- procedure, manuali e/o informatiche, che regolino lo svolgimento delle attività, prevedendo opportuni controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, laddove richiesto, l'indicazione di limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

Il sistema di controllo, inoltre, deve conformarsi ai seguenti principi:

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione;
- segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli effettuati.

² Il sistema di controllo esistente all'interno dell'ente, o sistema di controllo interno, “è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati” (v. Codice di Autodisciplina, Comitato per la Corporate Governance, Borsa Italiana S.p.A., 2006, pag. 35).

1.6 Delitti tentati e delitti commessi all'estero

L'Ente risponde anche degli illeciti dipendenti da delitti tentati e da reati commessi all'estero.

Nelle ipotesi di commissione nella forma del tentativo dei delitti previsti dal Decreto, le sanzioni pecuniarie e le sanzioni interdittive sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento. L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra Ente e soggetti che assumono di agire in suo nome e per suo conto.

In base al disposto dell'art. 4 del Decreto, l'Ente che abbia sede in Italia può essere chiamato a rispondere, in relazione a reati – contemplati dallo stesso Decreto – commessi all'estero, al fine di non lasciare sfornita di sanzione una condotta criminosa di frequente verificaione, nonché al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti su cui si fonda la responsabilità dell'Ente per reati commessi all'estero sono:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente, ai sensi dell'art. 5, comma 1, del Decreto;
- l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- le condizioni previste dagli artt. 7, 8, 9, 10 codice penale, con riferimento alla punibilità dei reati commessi all'estero, si devono essere verificate (nell'Allegato B – “Articoli del Codice Penale richiamati dall'art. 4 del D.Lgs. 231/2001”, sono descritte le fattispecie dei reati);
- non si procede nei confronti dell'Ente nello Stato in cui è stato commesso il fatto.

SEZIONE SECONDA

2 Il Modello di Organizzazione, Gestione e Controllo di HBG On Line Gaming S.r.l.

2.1 *Obiettivi e mission aziendale*

HBG On Line Gaming S.r.l. (di seguito “HBG On Line Gaming” o la “Società”) è una società concessionaria di ADM (già AAMS - Amministrazione Autonoma dei Monopoli di Stato) per la gestione del gioco a distanza e delle scommesse su rete fisica³.

In tale contesto, la Società persegue l'obiettivo di proporre e offrire le migliori opportunità di gioco disponibili sul mercato, con elevati standard di qualità, liceità, efficacia ed efficienza nello svolgimento della propria attività, anche attraverso il miglioramento continuo dell'organizzazione, delle risorse umane e tecniche ed improntando la gestione del rapporto con il cliente alla massima cortesia, rispetto, correttezza, chiarezza e professionalità.

La Società conduce, altresì, la propria attività nel rispetto delle normative comunitarie, nazionali e regolamentari vigenti ed applicabili, collaborando con l'ADM e con le Autorità pubbliche al fine di garantire un divertimento responsabile, sicuro, lecito e regolare per tutti i giocatori e respingendo la corruzione e ogni pratica illegale.

La Società è quindi sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri soci e del lavoro dei propri dipendenti ed è consapevole dell'importanza di dotarsi di un sistema di controllo interno aggiornato ed idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, rappresentanti e partner d'affari.

A tal fine, HBG On Line Gaming ha avviato un Progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto e ad implementare il Modello di Organizzazione Gestione e Controllo ex D.Lgs. 231/01 (di seguito il “Modello”).

Attraverso l'adozione ed attuazione del Modello, HBG On Line Gaming intende perseguire i seguenti obiettivi:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie (di natura pecuniaria e interdittiva) anche a carico della Società;
- consentire alla Società, grazie ad un sistema strutturato di procedure e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

2.2 *Modello di Governance*

La corporate governance⁴ di HBG On Line Gaming, basata sul modello tradizionale, è così articolata:

Assemblea dei soci, competente a deliberare in sede ordinaria e straordinaria sulle materie alla stessa riservate dalla legge o dallo statuto.

Organo Amministrativo, investito dei più ampi poteri per l'amministrazione della Società, con facoltà di compiere tutti gli atti opportuni per il raggiungimento degli scopi sociali, ad esclusione degli atti riservati – dalla legge e dallo statuto – all'Assemblea. L'Organo Amministrativo è rappresentato dall'Amministratore Unico⁵.

³ giochi pubblici di cui all'articolo 10, comma 9-octies, del decreto legge 2 marzo 2012, n. 16 convertito con modificazioni dalla legge 26 aprile 2012 n. 44.

⁴ Attualmente non è presente un Collegio Sindacale né un Sindaco Unico, non ricorrendone i presupposti di legge. I riferimenti contenuti nel presente documento al Collegio Sindacale devono quindi intendersi validi solo in caso di nomina di tale organo di controllo. Allo stesso modo, in caso di nomina di un Sindaco Unico, i riferimenti al Collegio Sindacale si devono intendere riferiti al Sindaco Unico.

⁵ Ove dovesse essere nominato quale Organo Amministrativo ed in alternativa all'Amministratore Unico un Consiglio di Amministrazione, ogni riferimento nel presente documento all'Amministratore Unico deve intendersi riferito all'Amministratore Delegato ed ogni riferimento all'Organo Amministrativo deve intendersi riferito al Consiglio di Amministrazione.

Società di revisione, l'attività di revisione contabile viene svolta, come previsto dalla vigente normativa, da una società di revisione, iscritta nell'albo speciale della Consob, incaricata dall'Assemblea dei Soci.

2.3 Finalità del Modello

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure ed attività di controllo (preventivo ed ex post) che abbia come obiettivo la riduzione del rischio di commissione dei reati mediante l'individuazione delle "Aree di attività a rischio" e dei "Processi strumentali/funzionali" alla commissione dei reati e la loro conseguente proceduralizzazione.

I principi contenuti nel presente Modello devono condurre, da un lato, a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di HBG On Line Gaming che quando apparentemente essa potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a HBG On Line Gaming di reagire tempestivamente nel prevenire od impedire la commissione del reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei Destinatari che operino per conto o nell'interesse della Società nell'ambito delle "Aree di attività a rischio" e dei "Processi strumentali/funzionali", di poter incorrere - in caso di comportamenti non conformi alle prescrizioni del Codice Etico e alle altre norme e procedure aziendali - in illeciti passibili di conseguenze penalmente rilevanti non solo per sé stessi, ma anche per la società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività dell'Organismo di Vigilanza sull'operato delle persone rispetto alle "Aree di attività a rischio" e ai "Processi strumentali/funzionali" e la comminazione di sanzioni disciplinari o contrattuali.

Gli elementi che caratterizzano il presente Modello sono: l'efficacia, la specificità e l'attualità.

L'efficacia

L'efficacia di un Modello dipende dalla sua idoneità in concreto ad elaborare meccanismi di decisione e di controllo tali da eliminare - o quantomeno ridurre significativamente - l'area di rischio da responsabilità. Tale idoneità è garantita dall'esistenza di meccanismi di controllo preventivo e successivo idonei ad identificare le operazioni che possiedono caratteristiche anomale, tali da segnalare condotte rientranti nelle aree di rischio e strumenti di tempestivo intervento nel caso di individuazione di siffatte anomalie. L'efficacia di un Modello, infatti, è anche funzione dell'efficienza degli strumenti idonei ad identificare "sintomatologie da illecito".

La specificità

La specificità di un Modello è uno degli elementi che ne connota l'efficacia.

- È necessaria una specificità connessa alle aree a rischio, così come richiamata dall'art. 6, comma 2 lett.a) del Decreto, che impone un censimento delle attività della Società nel cui ambito possono essere commessi i reati;
- Ai sensi dell'art. 6, comma 2 lett.b) del Decreto, è altrettanto necessario che il Modello preveda dei processi specifici di formazione delle decisioni dell'ente e dei processi di attuazione nell'ambito dei settori "sensibili".

Analogamente, l'individuazione delle modalità di gestione delle risorse finanziarie, l'elaborazione di un sistema di doveri d'informativa, l'introduzione di un adeguato sistema disciplinare sono obblighi che richiedono la specificità delle singole componenti del Modello.

Il Modello, ancora, deve tener conto delle caratteristiche proprie, delle dimensioni della Società e del tipo di attività svolte, nonché della storia della Società.

L'attualità

Un Modello è idoneo a ridurre i rischi da reato qualora sia costantemente adattato ai caratteri della struttura e dell'attività d'impresa.

In tal senso l'art. 6 del Decreto prevede che l'Organismo di Vigilanza, titolare di autonomi poteri d'iniziativa e controllo, abbia la funzione di supervisionare all'aggiornamento del Modello.

L'art. 7 del Decreto stabilisce che l'efficace attuazione del Modello contempa una verifica periodica, nonché l'eventuale modifica dello stesso allorquando siano scoperte eventuali violazioni oppure intervengano modifiche nell'attività o nella struttura organizzativa della Società.

2.4 *Destinatari*

Le regole contenute nel Modello si applicano:

- a coloro i quali siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, direttore generale, membro del collegio sindacale (ove nominato);
- a coloro i quali svolgano funzioni di direzione in veste di responsabili di specifiche Unità Organizzative;
- a coloro i quali, seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società. La previsione, di portata residuale, è finalizzata a conferire rilevanza al dato fattuale, in modo da ricomprendere, tra gli autori dei reati da cui può derivare la responsabilità della società, non soltanto l'amministratore di fatto (ovvero colui che esercita in concreto, senza averne la qualifica, poteri corrispondenti a quelli dell'amministratore), ma anche, ad esempio, il socio di maggioranza, che sia in grado di imporre la propria strategia aziendale e il compimento di determinate operazioni, anche nell'ambito di una società controllata, comunque agendo, attraverso qualsiasi forma idonea di controllo, sulla gestione concreta della società;
- ai lavoratori subordinati della Società, di qualsiasi grado e in forza di qualsivoglia tipo di rapporto contrattuale, ancorché distaccati all'estero per lo svolgimento dell'attività;
- a chi, pur non appartenendo alla Società, opera su mandato o nell'interesse della medesima. Resta quindi inteso ad esempio che eventuali terzi (ad es. in relazione ai controlli effettuati sul territorio presso gli esercizi e le sale da parte della società appaltatrice di tali attività e dai dipendenti di quest'ultima) o eventuali risorse appartenenti ad altre società del Gruppo HBG, qualora operino, anche in territorio estero, per conto o nell'interesse della Società, devono intendersi come Destinatari del Modello e dovranno, pertanto, osservare le regole comportamentali ed i principi sanciti nel Modello di HBG On Line Gaming.

Il Modello costituisce inoltre un riferimento indispensabile per tutti coloro che contribuiscono allo sviluppo delle varie attività, in qualità di fornitori di materiali, servizi e lavori, consulenti, società di service, soggetti della filiera del gioco e partners con cui HBG On Line Gaming opera.

2.5 *Struttura del Modello*

Il presente Modello è costituito da una "Parte Generale" e da singole "Parti Speciali" predisposte per le diverse tipologie di reato contemplate nel Decreto.

Si evidenzia che nelle Parti Speciali sono state riportate le tipologie di reato presupposto, identificate nell'ambito di un'attività di mappatura delle "Aree a rischio reato" e per le quali è stato ritenuto che HBG On Line Gaming sia, in via potenziale ed eventuale, esposta al rischio di commissione degli illeciti in considerazione delle attività svolte.

È demandato all'Organo Amministrativo di HBG On Line Gaming di integrare il presente Modello in una successiva fase, mediante apposite delibere, con ulteriori Parti Speciali relative ad altre tipologie di reato che, per effetto di altre normative, risultino inserite o comunque collegate all'ambito di applicazione del Decreto.

2.6 *Elementi fondamentali del Modello*

Con riferimento alle esigenze individuate nel Decreto, gli elementi fondamentali sviluppati da HBG On Line Gaming nella definizione del Modello, possono essere così riassunti:

- mappatura delle attività sensibili⁶, con esempi di possibili modalità di realizzazione dei reati e dei processi strumentali/funzionali potenzialmente associabili alla commissione dei reati richiamati dal Decreto, da sottoporre, pertanto, ad analisi e monitoraggio periodico;
- previsione di specifici protocolli relativi ai processi strumentali/funzionali ritenuti a maggior rischio potenziale di commissione di reato, diretti a regolamentare espressamente la formazione e l'attuazione delle decisioni della Società, al fine di fornire indicazioni specifiche sul sistema di controlli preventivi in relazione alle singole

⁶ Tramite l'analisi documentale e le interviste svolte, con i soggetti aziendali informati dell'organizzazione e delle attività svolte dalle Funzioni/Direzioni, nonché dei processi aziendali nei quali le attività sono articolate, sono identificate:

- le aree di attività "sensibili" alla commissione dei reati, o aree di attività a potenziale rischio-reato ai sensi del Decreto;
- i processi "strumentali/funzionali" alla realizzazione dei reati di cui al Decreto, o processi nel cui ambito potrebbero crearsi le condizioni e/o gli strumenti per la commissione del reato.

fattispecie di illecito da prevenire. Nei protocolli sono inoltre contenute le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati stessi;

- identificazione dei principi etici e delle regole comportamentali volte alla prevenzione di condotte che possano integrare le fattispecie di reato previste dal Decreto, sancite nel Codice Etico adottato dalla Società e, più in dettaglio, nel presente Modello;
- nomina di un Organismo di Vigilanza al quale sono attribuiti specifici compiti di vigilanza sull'efficace attuazione ed effettiva applicazione del Modello ai sensi dell'art. 6 punto b) del Decreto;
- approvazione di un sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello, contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- svolgimento di un'attività di informazione, sensibilizzazione e divulgazione ai Destinatari del presente Modello;
- modalità per l'adozione e l'effettiva applicazione del Modello nonché per le necessarie modifiche o integrazioni dello stesso (cfr. par. 5 "Aggiornamento del Modello").

2.7 Codice Etico e Modello

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice stesso. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte delle società del Gruppo HBG allo scopo di esprimere dei principi di "deontologia aziendale" che il Gruppo HBG riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti nonché degli amministratori, dei componenti degli organi sociali, consulenti, fornitori, partner e di tutti coloro che, stabilmente o temporaneamente, agiscono per conto delle Società del Gruppo HBG o sono legati con esse da un rapporto di collaborazione cooperando allo svolgimento delle rispettive attività ed al perseguimento dei relativi fini;
- il Modello risponde invece a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi apparentemente a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo).

2.8 Presupposti del Modello

Nella predisposizione del Modello, HBG On Line Gaming ha tenuto conto della propria organizzazione aziendale, al fine di verificare le aree di attività più esposte al rischio di potenziale commissione di reati.

La Società ha tenuto altresì conto del proprio sistema di controllo interno al fine di verificarne la capacità a prevenire le fattispecie di reato previste dal Decreto nelle aree di attività identificate a rischio.

Più in generale, il sistema di controllo interno di HBG On Line Gaming deve garantire, con ragionevole certezza, il raggiungimento di obiettivi operativi, di informazione e di conformità:

- l'obiettivo operativo del sistema di controllo interno riguarda l'efficacia e l'efficienza della Società nell'impiegare le risorse, nel proteggersi dalle perdite, nel salvaguardare il patrimonio aziendale; tale sistema è volto, inoltre, ad assicurare che il personale operi per il perseguimento degli obiettivi aziendali, senza anteporre altri interessi a quelli di HBG On Line Gaming;
- l'obiettivo di informazione si traduce nella predisposizione di rapporti tempestivi ed affidabili per il processo decisionale all'interno e all'esterno dell'organizzazione aziendale;
- l'obiettivo di conformità garantisce, invece, che tutte le operazioni ed azioni siano condotte nel rispetto delle leggi e dei regolamenti, dei requisiti prudenziali e delle procedure aziendali interne.

In particolare, il sistema di controllo interno si basa sui seguenti elementi:

- sistema organizzativo formalizzato e chiaro nell'attribuzione delle responsabilità;
- sistema procedurale;
- sistemi informatici orientati alla segregazione delle funzioni;
- sistema di controllo di gestione e reporting;

- poteri autorizzativi e di firma assegnati in coerenza con le responsabilità;
- sistema di comunicazione interna e formazione del personale.

Alla base del sistema di controllo interno di HBG On Line Gaming vi sono i seguenti principi:

- ogni operazione, transazione e azione deve essere veritiera, verificabile, coerente e documentata;
- nessuno deve poter gestire un intero processo in autonomia (c.d. segregazione dei compiti);
- il sistema di controllo interno deve poter documentare l'effettuazione dei controlli, anche di supervisione.

Tutto il personale, nell'ambito delle funzioni svolte, è responsabile della definizione e del corretto funzionamento del sistema di controllo attraverso i controlli di linea, costituiti dall'insieme delle attività di controllo che le singole unità operative svolgono sui loro processi.

2.9 Individuazione delle attività "a rischio"

La Società ha condotto un'attenta analisi dei propri strumenti di organizzazione, gestione e controllo, diretta a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto e, ove si sia reso necessario, ad adeguarli.

Il Decreto prevede espressamente, al relativo art. 6, comma 2, lett. a), che il Modello dell'ente individui, infatti, le attività aziendali, nel cui ambito possano essere potenzialmente commessi i reati di cui al medesimo Decreto.

È stata, dunque, condotta l'analisi delle attività aziendali di HBG On Line Gaming e delle relative strutture organizzative, allo specifico scopo di identificare le aree di attività aziendale a rischio in cui possono essere commessi i reati previsti dal Decreto (nonché pratici esempi di attività "sensibili"), gli esempi di possibili modalità di realizzazione degli stessi, nonché i processi nel cui svolgimento, sempre in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (cosiddetti processi "strumentali/funzionali").

In considerazione delle attività caratteristiche di HBG On Line Gaming le aree a rischio rilevate riguardano, in particolar modo, i reati previsti dagli artt. 24 e 25, 24 bis, 24 ter, 25 ter, 25 septies, 25 octies, 25 decies, 25 undecies e 25 duodecies.

Nell'ambito di tali attività a rischio ed in considerazione del fatto che HBG On Line Gaming S.r.l. è concessionaria di ADM nel settore dei giochi a distanza e delle scommesse su rete fisica, si è in particolare tenuto conto della possibilità che, nello svolgimento delle attività e funzioni pubbliche oggetto della concessione, il personale della società possa essere qualificato, come peraltro confermato dal provvedimento del Ministero dell'Economia e delle Finanze del 15 giugno 2005, come "incaricato di pubblico servizio"⁷⁸, con le conseguenze da ciò derivanti in termini di potenziale estensione dei rischi di commissione di illeciti contro la Pubblica Amministrazione anche ai reati propri di corruzione passiva (e non solo attiva) e di concussione per induzione.

L'identificazione delle aree di attività a rischio di commissione dei reati previsti dal Decreto (cd. mappatura), come già sopra ricordato, è stata realizzata anche attraverso le interviste ai soggetti aziendali di ciascuna direzione/dipartimento competente, come tali provvisti della più ampia e profonda conoscenza dell'operatività di ciascun singolo settore dell'attività aziendale.

⁷ Per la definizione di "incaricato di pubblico servizio" si veda la Parte Speciale A del presente Modello.

⁸ Secondo la Suprema Corte di Cassazione, infatti: (i) "le attività dispiagate da un privato concessionario in funzione e in dipendenza della concessione nonché in adempimento degli obblighi con essa impostigli al fine di assicurare il perseguimento dell'interesse pubblico, non possono definirsi attività di diritto privato per il solo fatto che sono espletate da un soggetto estraneo alla Pubblica Amministrazione, ma conservano la natura di attività amministrativa in senso oggettivo, il cui esercizio da parte del concessionario secondo le previsioni contenute nell'atto concessorio, attribuisce a costui il ruolo di organo indiretto dell'amministrazione" (cfr. Cass. pen., Sez. VI, 17/10/1996, n. 10735); (ii) "nell'ambito dei soggetti che svolgono pubbliche funzioni, la qualifica di pubblico ufficiale è riservata a coloro che formano o concorrono a formare la volontà della Pubblica Amministrazione o che svolgono tale attività per mezzo di poteri autorizzativi o certificativi, mentre quella di incaricato di pubblico servizio è assegnata dalla legge in via residuale a coloro che, pur agendo nell'ambito di una attività disciplinata nelle forme della pubblica funzione, mancano dei poteri tipici di questa, a patto che non svolgano semplici mansioni d'ordine nè prestino opera meramente materiale" cfr. Cass. pen., Sez. VI, 21/02/2003, n. 11417).

I risultati dell'attività di mappatura sopra descritta, previamente condivisi con i referenti aziendali intervistati, sono stati raccolti in una scheda descrittiva (c.d. Matrice delle attività a rischio – reato), che illustra nel dettaglio i concreti profili di rischio di commissione dei reati richiamati dal Decreto, nell'ambito delle attività della Società.

La Matrice delle attività a rischio-reato è custodita presso la sede della Società, dalla Direzione Compliance di HBG On Line Gaming.

Nello specifico, è riscontrabile il rischio di possibile commissione dei reati previsti dal Decreto nelle seguenti aree di attività aziendale⁹:

- Gestione dei rapporti con gli enti pubblici competenti e con soggetti incaricati della raccolta in occasione dell'espletamento degli adempimenti amministrativi connessi all'attività caratteristica, a titolo esemplificativo:
 - Rapporti con la PA per richieste/rilascio di autorizzazioni, certificazioni etc. per l'esercizio delle attività;
 - Rapporti con *service provider* per le scommesse e con soggetti incaricati della raccolta per l'affidamento della attività di raccolta del gioco;
 - Spostamento dei diritti, previa autorizzazione di ADM, ad altri Negozi Scommesse;
 - Certificazione dei nuovi giochi a distanza;
 - Trasmissione dei livelli di servizio ad ADM;
 - Rapporti con gli enti certificatori per l'omologazione della piattaforma del gioco a distanza;
 - Gestione delle promozioni e concorsi nell'ambito del gioco a distanza.
- Gestione degli adempimenti, delle comunicazioni e delle richieste non connesse all'attività caratteristica, anche in occasione di verifiche, ispezioni ed accertamenti da parte degli enti pubblici competenti o delle autorità amministrative indipendenti
 - Rapporti con la PA in caso di verifiche ispettive, a titolo esemplificativo:
 - ✓ ADM per controlli sull'esercizio del gioco, il rispetto di titoli autorizzativi;
 - ✓ Agenzia delle Entrate e degli Enti competenti per verifiche in materia fiscale e tributaria;
 - ✓ Guardia di Finanza e altre Autorità di pubblica sicurezza.
 - Rapporti con le Autorità Amministrative Indipendenti (es. Autorità Garante per la Protezione dei Dati Personali) e gestione delle comunicazioni e delle informazioni a esse dirette, anche in occasione di verifiche ispettive.
 - Gestione dei flussi telematici con Enti Pubblici che implicano l'accesso ai siti istituzionali (ad esempio, ADM, Agenzia delle Entrate, Camera di Commercio, Direzione del Lavoro, SOGEI).
- Gestione del personale e gestione degli adempimenti in materia di assunzioni, cessazione del rapporto di lavoro, retribuzioni, ritenute fiscali e contributi previdenziali e assistenziali, relativi a dipendenti e collaboratori (ove presenti)
 - Gestione dei rapporti con i candidati alla assunzione e con i Funzionari Pubblici in occasione di verifiche circa il rispetto dei presupposti e delle condizioni richieste dalla normativa vigente per le assunzioni agevolate.
 - Gestione dei rapporti, anche tramite consulenti esterni, con funzionari competenti (INPS, INAIL, ASL, Direzione Provinciale del Lavoro ecc.) per l'osservanza degli obblighi previsti dalla normativa di riferimento, anche in occasione di verifiche ispettive:
 - ✓ predisposizione delle denunce relative a costituzione, modifica ed estinzione del rapporto di lavoro;
 - ✓ autorizzazione per l'assunzione di personale appartenente a categorie protette;
 - ✓ ottenimento della Certificazione di Ottemperanza in materia di collocamento obbligatorio;

⁹ Nelle aree di attività aziendali sono comprese sia attività direttamente svolte dalle funzioni interne della Società sia attività svolte sempre dalla Società ma attraverso funzioni formalmente dipendenti da altre società del Gruppo HBG o fornitori di servizi terzi rispetto alla Società (*service provider* e società di sviluppo informatico), nell'interesse e per conto della medesima Società.

- ✓ elenchi del personale attivo, assunto e cessato presso l'INAIL;
 - ✓ controlli e verifiche circa il rispetto dei presupposti e delle condizioni previste dalla normativa vigente.
- Gestione dei contenziosi (es.: civili, tributari, giuslavoristici, amministrativi, penali), in tutti i gradi di giudizio
 - Gestione dei rapporti con i giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi (civile, penale, amministrativo, giuslavoristico e tributario) con particolare riferimento alla nomina dei legali esterni.
 - Gestione dei rapporti con soggetti che possono avvalersi della facoltà di non rispondere nel processo penale.
- Gestione della contabilità generale e formazione del bilancio
 - Gestione della contabilità generale, con particolare riferimento alle attività di:
 - ✓ Rilevazione, classificazione e controllo di tutti i fatti gestionali aventi riflessi amministrativi, finanziari ed economici (es. gestione e registrazione contabile della fatturazione attiva);
 - ✓ Verifica dati provenienti dai sistemi alimentanti;
 - ✓ Raccolta e aggregazione dei dati contabili necessari per la predisposizione della bozza di Bilancio civilistico.
- Gestione degli adempimenti in materia societaria e gestione degli adempimenti fiscali
 - Rapporti con il Collegio Sindacale (ove nominato) relativamente alle verifiche sulla gestione amministrativa/contabile e sul Bilancio d'Esercizio, e con il Socio nelle attività di verifica della gestione aziendale.
 - Tenuta delle scritture contabili e dei libri contabili e sociali.
 - Gestione degli adempimenti fiscali, calcolo e versamento di imposte e tributi e presentazione delle dichiarazioni fiscali.
 - Gestione dei rapporti e dell'espletamento degli adempimenti con i Funzionari degli Enti competenti in materia di adempimenti societari e/o tributari (es. Registro delle imprese presso le Camere di Commercio competenti, Agenzia delle Entrate).
- Gestione del sistema di sicurezza del lavoro ai sensi del D.lgs 81/08 (Testo Unico Sicurezza)
 - Espletamento e gestione degli adempimenti in materia di tutela della salute e della sicurezza sul lavoro ai sensi del D.lgs. 81/2008 – Testo Unico sulla Sicurezza nei luoghi di lavoro e successive integrazioni.
 - Gestione dei rapporti con le autorità di controllo in materia di tutela della sicurezza e salute sul lavoro, anche in occasione di verifiche ed ispezioni, in occasione di, a titolo esemplificativo:
 - ✓ adempimenti previsti dal D.Lgs. 81/2008 - Testo Unico sulla Sicurezza nei Luoghi di Lavoro
 - ✓ relative ispezioni in materia di sicurezza, salute, igiene sul lavoro;
 - ✓ autorizzazione sanitaria.
- Approvvigionamento di beni e servizi e, in generale, negoziazione e sottoscrizione di contratti con soggetti terzi
 - Gestione degli acquisti di beni e servizi con particolare riferimento alle seguenti attività:
 - ✓ predisposizione e conservazione delle richieste di acquisto e, in generale, della relativa documentazione;
 - ✓ emissione degli ordini;
 - ✓ autorizzazioni interne;
 - ✓ gestione dei rapporti e della relazioni con i terzi in sede di verifica e controllo del rispetto degli impegni assunti;
 - ✓ gestione di eventuali contestazioni.

- Gestione dei flussi monetari e finanziari e gestione di attività finanziarie
 - Gestione dei flussi finanziari (ciclo attivo e ciclo passivo), tesoreria e provvista finanziaria.
 - Gestione dei rapporti con banche ed istituti finanziari e gestione dei conti correnti bancari (ad es. apertura conti correnti, riconciliazioni bancarie);
 - Impiego del capitale e gestione di operazioni di acquisto/vendita di asset/partecipazioni aziendali, investimenti, operazioni straordinarie e transazioni finanziarie con conseguenti movimentazioni di capitali (specie se realizzate a livello infragruppo o con soggetti terzi operanti all'estero in paesi black list).
- Gestione della sicurezza informatica:
 - Gestione della sicurezza logica;
 - Gestione della sicurezza e tracciabilità degli accessi alla rete da parte del personale che opera all'interno delle strutture aziendali;
 - Gestione della sicurezza dei dati sui pc e sui server.
- Gestione degli adempimenti in materia ambientale
 - Gestione degli adempimenti in materia ambientale secondo quanto previsto dalla normativa applicabile;
 - Gestione dei rifiuti;
 - Gestione dei rapporti con i soggetti pubblici (es. Regione, Ministero dell'Ambiente e della Tutela del Territorio) nell'ambito delle attività legate all'ottenimento o al rinnovo di provvedimenti amministrativi quali autorizzazioni, licenze e permessi per la gestione dei rifiuti;
 - Gestione delle attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti, ivi compresi eventuali depositi temporanei;
 - Gestione delle attività di conferimento a terzi dei rifiuti per finalità di trasporto, smaltimento e/o recupero;
 - Gestione delle comunicazioni e degli adempimenti, anche telematici, verso la Pubblica Amministrazione nell'ambito delle attività legate alla gestione del trasporto rifiuti.
- Coinvolgimento in un'organizzazione per la quale potrebbero verificarsi i presupposti del vincolo associativo ex art. 416 c.p. (associazione per delinquere)
 - Coinvolgimento in un'organizzazione per la quale potrebbero verificarsi i presupposti del vincolo associativo ex art. 416 c.p. (Associazione per delinquere).

Sono stati anche individuati e regolamentati i processi nel cui ambito, in linea di principio, potrebbero crearsi le condizioni e/o potrebbero essere forniti gli strumenti per la commissione delle fattispecie di reato (processi c.d. strumentali) e i processi che sovrintendono direttamente le attività sensibili (processi c.d. funzionali):

- 1) Consulenze e incarichi professionali a terzi
- 2) Acquisto di beni e servizi
- 3) Rimborsi spese, anticipi e spese di rappresentanza
- 4) Flussi Monetari e Finanziari e gestione di attività finanziarie
- 5) Gestione del contenzioso
- 6) Gestione di donazioni, sponsorizzazioni, omaggi e di altre liberalità
- 7) Rapporti con la Pubblica Amministrazione, con le Autorità di Vigilanza e le Autorità di Pubblica Sicurezza
- 8) Gestione della Sicurezza sul lavoro
- 9) Gestione degli adempimenti societari e fiscali
- 10) Formazione del Bilancio civilistico (Financial Closing) e gestione dei rapporti con il Collegio Sindacale (ove nominato) e Soci

- 11) Gestione, amministrazione e manutenzione degli apparati telematici, dei sistemi, dei database e delle applicazioni
- 12) Gestione delle attività antiriciclaggio
- 13) Selezione, assunzione, gestione del personale dipendente
- 14) Gestione degli adempimenti in materia ambientale

2.10 Procedure rilevanti in ambito 231

All'esito dell'avvenuta identificazione dei processi strumentali e funzionali, la Società, attenta ad assicurare condizioni di correttezza e trasparenza nella conduzione delle attività sociali e, in particolare, di prevenire la commissione di comportamenti illeciti rilevanti ai sensi del Decreto, ha provveduto ad una rilettura del corpo procedurale esistente con più specifico riferimento a quelle procedure che regolano le aree aziendali connesse al core business risultate di fatto più esposte a rischi 231.

Di conseguenza, HBG On Line Gaming ha provveduto ad apportare alcune integrazioni a talune procedure già esistenti, ritenute indispensabili per una più ampia prevenzione dei possibili rischi di realizzazione dei reati ricompresi nel D.Lgs. 231/2001, nonché a predisporre di nuove laddove il rischio sia risultato meno presidiato nel sistema di controllo in essere.

Le menzionate procedure contengono, in sostanza, un insieme di regole atte a consentire il controllo ex ante e la ricostruzione ex post di ciascun processo decisionale e delle relative fasi, idonee a governare anche profili di rischio in chiave 231.

L'elenco completo di tutte le procedure aziendali esistenti, è custodito dalla Società presso la Funzione Qualità, disponibile per consultazione.

Le procedure contengono regole di condotta aziendale e formano parte essenziale del presente Modello.

2.11 Principi di controllo interno generali

Il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di: esplicita formalizzazione delle norme comportamentali; chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna direzione e alle diverse qualifiche e ruoli professionali; precisa descrizione delle attività di controllo e loro tracciabilità; adeguata segregazione di ruoli operativi e ruoli di controllo.

In particolare devono essere perseguiti i seguenti principi generali di controllo interno:

Norme comportamentali

- Esistenza di un Codice Etico che descriva regole comportamentali di carattere generale a presidio delle attività svolte.

Definizioni di ruoli e responsabilità

- La regolamentazione interna deve declinare ruoli e responsabilità delle unità 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.

Procedure 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 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;
- sono previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni;
- il sistema di deleghe deve identificare, tra l'altro:
 - i requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
 - l'accettazione espressa da parte del delegato o del subdelegato delle funzioni delegate e conseguente assunzione degli obblighi conferiti;
 - le modalità operativa di gestione degli impegni di spesa;
- le deleghe sono attribuite secondo i principi di:
 - autonomia decisionale e finanziaria del delegato;
 - idoneità tecnico-professionale del delegato;
 - disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- Nell'ambito delle procedure o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- 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 direzione 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 (ove nominato) od organo equivalente o ad altri organi di controllo interno, alla società di revisione eventualmente nominata e all'Organismo di Vigilanza.

Principi specifici di controllo interno

Di seguito vengono enunciati, per i processi funzionali e/o strumentali individuati precedentemente, a titolo non esaustivo, i principi di controllo minimali a cui si deve ispirare l'operatività degli stessi.

In ogni caso, anche nell'ipotesi di esternalizzazione di processi e attività, presso la Società devono essere previsti poteri delegati e specifiche procure per coloro che operano in nome e per conto della Società, anche se in via temporanea e per particolari operazioni.

Per i processi "strumentali" identificati, anche nell'ipotesi di esternalizzazione, devono essere applicati dalla Società i principi nel seguito riportati.

Consulenze e Incarichi Professionali a terzi

- Deve essere prevista l'esistenza di attori diversi operanti nelle differenti fasi del processo di gestione delle consulenze (ad es. in linea di principio non vi deve essere coincidenza di identità tra chi richiede la consulenza, chi la autorizza e chi esegue il pagamento della prestazione);
- deve essere effettuata un'adeguata attività selettiva fra i diversi operatori di settore;
- devono essere utilizzati idonei dispositivi contrattuali adeguatamente formalizzati;
- nei casi di controparti commerciali residenti in paesi a regime fiscale privilegiato (c.d. black list) e/o aventi banche residenti in tali paesi, o in caso di società offshore, l'inserimento in anagrafica fornitori dovrà essere valutato e preceduto dall'autorizzazione scritta del responsabile della Direzione che usufruisce/richiede il servizio/fornitura, con esplicita motivazione del fornitore scelto e del conto corrente bancario in uso;
- devono esistere adeguati livelli autorizzativi (in coerenza con il sistema di procure aziendali e con le procedure aziendali vigenti, ivi compresa per quanto applicabile la procedura acquisti) per la stipulazione dei contratti;
- sono presenti i livelli di approvazione per la formulazione delle richieste di consulenza e per la certificazione/validazione del servizio reso;
- devono esistere i requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti e di meccanismi di valutazione complessiva del servizio reso;
- nell'impiego di consulenti esterni, nell'ambito della gestione dei rapporti con la PA, devono essere previsti dei meccanismi di verifica preventiva dell'assenza di contemporanea collaborazione sulla medesima materia con le stesse amministrazioni pubbliche (per esempio mediante auto-certificazione del consulente esterno);
- nei contratti di fornitura, patti fra soci o partners commerciali, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- devono esistere documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati.

Acquisto di Beni e Servizi

- Devono esistere norme aziendali relative all'approvvigionamento di beni e servizi e in particolare per l'approvvigionamento di particolari tipologie di beni e servizi (consulenze, prestazioni professionali) ovvero per approvvigionamenti con particolari modalità attuative (es. con riferimento al fornitore unico, o in caso di urgenza), che assicurino, per quanto possibile, una distinzione e separazione soggettiva tra chi autorizza l'attività, chi la gestisce/esegue, chi predispone/conserva/archivia la relativa documentazione e chi sulla stessa attività esercita il controllo (o comunque una condivisione, tra più soggetti, di ognuna di tali fasi). Gli acquisti della Società devono essere pertanto eseguiti e autorizzati secondo quanto previsto dalle predette norme aziendali, previa verifica da un lato della corrispondenza dei beni e/o servizi da acquistare rispetto alle esigenze aziendali e dall'altro della perfetta rispondenza tra beni e/o servizi acquistati e le relative uscite di cassa;
- le norme aziendali devono essere ispirate, in ciascuna fase del processo di approvvigionamento ed indipendentemente dalla funzione responsabile del medesimo processo (a seconda dei casi, il responsabile del

centro di costo richiedente e/o il responsabile della funzione Amministrazione Fornitori e Acquisti Generali – AFAG), a criteri di trasparenza (precisa individuazione dei soggetti responsabili, valutazione delle richieste di approvvigionamento o delle richieste di servizi, verifica che le richieste arrivino da soggetti autorizzati, determinazione dei criteri che saranno utilizzati nelle varie fasi del processo e tracciabilità delle valutazioni sulle offerte tecniche ed economiche) e di tracciabilità delle operazioni effettuate;

- la scelta e la valutazione della controparte deve avvenire, per quanto possibile, sulla base di requisiti predeterminati dalla Società (soprattutto per quanto riguarda la verifica, sia preliminare sia nel corso del rapporto, del possesso dei necessari requisiti di professionalità ed onorabilità dei *service provider* e delle società di sviluppo informatico), assicurando che ogni operazione e/o transazione, compresi i relativi flussi finanziari, sia sempre legittima, autorizzata, coerente, congrua, documentata, registrata ed in ogni tempo verificabile, al fine di consentire l'effettuazione di controlli sulle caratteristiche dell'operazione e/o della transazione, sulle motivazioni che ne hanno consentito l'esecuzione, sulle autorizzazioni allo svolgimento e sulla relativa esecuzione;
- i contratti di acquisto di valore significativo o che coinvolgono il budget di più responsabili/direzioni aziendali devono essere sempre preventivamente valutati e autorizzati dal Responsabile della funzione che richiede il bene o il servizio, sentiti i responsabili/direttori delle eventuali funzioni coinvolte e dal Direttore Generale e/o dall'Amministratore Unico della Società;
- la scelta della modalità di approvvigionamento da adottare (es. pubblicazione del bando, fornitore unico, utilizzo di vendor list qualificate) deve essere formalizzata e autorizzata a un adeguato livello gerarchico;
- la definizione delle short vendor list deve essere effettuata mediante procedure trasparenti e deve essere autorizzata a un adeguato livello gerarchico;
- nei casi di controparti commerciali residenti in paesi a regime fiscale privilegiato (c.d. black list) e/o aventi banche residenti in tali paesi, o in caso di società offshore, l'inserimento in anagrafica fornitori dovrà essere valutato e preceduto dall'autorizzazione scritta del responsabile della Direzione che usufruisce/richiede il servizio/fornitura, con esplicita motivazione del fornitore scelto e del conto corrente bancario in uso;
- il ricorso alla procedura "fornitore unico" deve essere ristretto ad una casistica limitata e chiaramente individuata, deve essere adeguatamente motivato e documentato, sottoposto a idonei sistemi di controllo e sistemi autorizzativi a un adeguato livello gerarchico;
- nei contratti di fornitura, patti fra soci o partners commerciali, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- devono essere definiti criteri di rotazione, per quanto possibile, delle persone coinvolte nel processo di approvvigionamento;
- devono essere formalmente definiti idonei sistemi di monitoraggio al fine di garantire, per quanto possibile, una corretta e fisiologica rotazione dei fornitori inclusi nelle vendor list;
- devono esistere idonei sistemi di monitoraggio e formalizzazione di report da sottoporre ad adeguato livello gerarchico per il monitoraggio sia del processo di scelta del fornitore (ad esempio numero di gare, fornitore vincitore, commissione aggiudicatrice, importo ed ente richiedente il fornitore unico, ecc.) sia dell'attività svolta dal fornitore (in particolare con i riferimenti ai fornitori – *service provider* e sviluppatori informatici – che supportano la Società nella gestione delle attività connesse al gioco *on line* e delle scommesse su rete fisica);
- devono essere chiaramente definite le condizioni di urgenza in relazione alle quali si può commissionare direttamente la fornitura e devono essere definiti adeguati strumenti autorizzativi e di monitoraggio (report sottoposti ad adeguato livello gerarchico);
- in caso di eventuali controversie relative a contestazioni aventi ad oggetto i beni e/o i servizi acquistati ed ai relativi pagamenti effettuati, deve essere garantita, in accordo con le procedure interne, la tracciabilità dei processi di monitoraggio del rapporto, ivi incluse eventuali transazioni extragiudiziarie, ai fini della validazione interna (controllo) e sottoscrizione di eventuali accordi transattivi.

Rimborsi spese, anticipi e spese di rappresentanza

- Non devono essere ammessi anticipi o rimborsi delle spese sostenute direttamente dai soggetti esterni, in particolare da rappresentanti della Pubblica Amministrazione che beneficiano di ospitalità;

- la gestione dei rimborsi spese deve avvenire in accordo con la normativa, anche fiscale, applicabile;
- i processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti;
- nello svolgimento di attività di servizio devono essere sempre ricercate le soluzioni più convenienti, sia in termini di economicità che di efficienza operativa;
- il sostenimento di spese di rappresentanza deve soddisfare il concetto di “opportunità” della spesa, in linea pertanto con gli obiettivi aziendali;
- le spese per forme di accoglienza e di ospitalità devono attenersi ad un criterio di contenimento dei costi entro limiti di normalità.

Flussi Monetari e Finanziari e Gestione di attività finanziarie

- Deve essere assicurata la ricostruzione delle operazioni attraverso l’identificazione della clientela e dei terzi e la registrazione dei dati in appositi archivi;
- l’Organo Amministrativo, o il soggetto da esso delegato deve stabilire e modificare, se necessario, la procedura di firma congiunta per determinate tipologie di operazioni o per operazioni che superino una determinata soglia quantitativa. Di tale modifica è data informazione all’Organismo di Vigilanza;
- non deve esservi identità soggettiva tra chi impegna HBG On Line Gaming nei confronti di terzi e chi autorizza o dispone il pagamento di somme dovute in base agli impegni assunti; laddove ciò non sia possibile in merito a singole operazioni, ne deve essere data comunicazione all’Organismo di Vigilanza;
- deve essere sempre prevista la rilevazione e l’analisi di pagamenti/incassi ritenuti anomali per controparte, importo, tipologia, oggetto, frequenza o entità sospette;
- devono essere immediatamente interrotte o, comunque, non deve essere data esecuzione ad operazioni di incasso o pagamento che vedano coinvolti soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell’antiriciclaggio e nella lotta al terrorismo;
- devono essere stabiliti limiti all’autonomo impiego delle risorse finanziarie, mediante la fissazione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone;
- le operazioni che comportano utilizzo o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono essere autorizzate ed avere sempre una causale espressa e essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile. Il processo operativo e decisionale deve essere tracciabile e verificabile nelle singole operazioni;
- devono essere definite regole che impongano la garanzia della assoluta trasparenza, correttezza ed effettività delle operazioni e dei flussi finanziari posti in essere; in particolare, deve essere prevista una apposita verifica dei presupposti di carattere strategico, economico e finanziario nonché dell’attuabilità delle operazioni poste in essere;
- devono essere definite apposite verifiche circa la legittima e lecita provenienza dei capitali e delle risorse utilizzate per acquisti, approvvigionamenti ed operazioni/investimenti nonché specifiche modalità di archiviazione della documentazione rilevante prodotta e del processo decisionale, con evidenza delle relative motivazioni;
- deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione anche con riferimento alle operazioni infragruppo; in particolare dovrà essere precisamente verificato che vi sia coincidenza tra il soggetto a cui è intestato l’ordine e il soggetto che incassa le relative somme;
- deve essere previsto il divieto di utilizzo del contante, ad eccezione dell’uso per importi non significativi della cassa interna, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie nonché il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili;
- per la gestione dei flussi in entrata e in uscita, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell’Unione europea o enti creditizi/finanziari

situati in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;

- devono essere vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa espressamente autorizzate dalla funzione amministrazione, ed in particolare per le operazioni di piccola cassa.
- devono essere previste specifiche regole di condotta e procedurali per la gestione di conti correnti e per la gestione del capitale e del risparmio.

Gestione del contenzioso

- Nell'ambito dell'organizzazione interna devono essere definiti:
 - i limiti delle deleghe di spesa dei soggetti coinvolti nella gestione del contenzioso;
 - i criteri di individuazione di legali esterni per la gestione dei contenziosi;
- l'articolazione del processo deve garantire la segregazione funzionale tra:
 - coloro che hanno la responsabilità di gestire il contenzioso, anche mediante l'ausilio di legali esterni;
 - coloro che hanno la responsabilità di imputare a budget le spese legali da sostenere;
 - coloro che hanno la responsabilità di verificare il rispetto delle deleghe di spesa e di poteri conferiti ed il rispetto dei criteri definiti per la scelta dei legali e la natura e la pertinenza degli oneri legali sostenuti;
- deve essere sempre identificato un Responsabile, coerentemente con l'oggetto della materia, dotato dei poteri necessari per rappresentare la Società o per coordinare l'azione di eventuali professionisti esterni;
- deve essere prevista la predisposizione di uno scadenziario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti;
- deve essere garantita la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate.

Gestione di Donazioni, Sponsorizzazioni, Omaggi e Liberalità

- Deve esistere una autorizzazione formalizzata (del Direttore Generale o di un Dirigente da questi incaricato) a conferire utilità;
- gli omaggi devono essere selezionati nell'ambito di un elenco apposito - gestito dalla direzione competente e da un soggetto diverso da quello che intrattiene rapporti con la Pubblica Amministrazione;
- devono esistere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, validati dal superiore gerarchico e archiviati;
- gli eventuali fornitori delle utilità devono essere scelti all'interno di una lista gestita dalla direzione competente. L'inserimento / eliminazione dei fornitori dalla lista deve essere basato su criteri oggettivi. L'individuazione, all'interno della lista, del fornitore della singola utilità deve essere motivata e documentata;
- nei casi di fornitori di utilità residenti in paesi a regime fiscale privilegiato (c.d. black list) e/o aventi banche residenti in tali paesi, o in caso di società offshore, l'inserimento in anagrafica fornitori dovrà essere valutato e preceduto dall'autorizzazione scritta del responsabile della Direzione che usufruisce/richiede il servizio/fornitura, effettua l'inserimento a sistema dell'anagrafica, con esplicita motivazione del fornitore scelto e del conto corrente bancario in uso;
- è prevista la rilevazione di operazioni (donazioni, sponsorizzazioni, omaggi e liberalità) ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- nei contratti di fornitura, patti fra soci o partner commerciali, deve essere inserita esplicitamente l'accettazione delle regole e dei comportamenti previsti nel presente Modello, ovvero l'indicazione da parte del contraente della adozione di un proprio Modello ex Decreto;
- deve essere verificata la regolarità dei pagamenti per donazioni, sponsorizzazioni o liberalità con riferimento alla piena coincidenza dei destinatari dei pagamenti e le controparti effettivamente coinvolte;
- sono immediatamente interrotte o, comunque, non è data esecuzione ad operazioni relative a donazioni, sponsorizzazioni, omaggi e liberalità, che vedano coinvolti come beneficiari, soggetti operanti, anche in parte,

in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;

- devono esistere report periodici sulle spese per la concessione di utilità, con motivazioni e nominativi / beneficiari, inviati al livello gerarchico superiore e archiviati;
- nel budget e nei consuntivi devono essere separate le spese per ciascuna tipologia di utilità.

Rapporti con la Pubblica Amministrazione, con le Autorità di Vigilanza e le Autorità di Pubblica Sicurezza

- Gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle normative vigenti, nazionali o comunitarie;
- gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere (e tale diligenza e professionalità deve essere richiesta anche ai fornitori che supportano la Società nella gestione delle attività connesse al gioco *on line* e delle scommesse su rete fisica;
- tutta la documentazione deve essere verificata e sottoscritta da parte del responsabile della direzione interessata o da altro soggetto delegato o, se necessario, da parte di un procuratore della società;
- le funzioni interessate dovranno dotarsi di un calendario/scadenziario per quanto riguarda gli adempimenti ricorrenti;
- ciascuna direzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta nell'ambito della propria attività, ivi inclusa quella trasmessa alla Pubblica Amministrazione anche eventualmente in via telematica;
- deve essere prestata completa ed immediata collaborazione alle Autorità o Organi di Vigilanza e Controllo, fornendo puntualmente ed in modo esaustivo la documentazione e le informazioni richieste;
- la gestione dei rapporti con i pubblici funzionari in caso di visite ispettive è totalmente nella responsabilità del responsabile di direzione competente, che gestisce i sopralluoghi dalla fase di accoglimento alla firma del verbale di accertamento;
- qualora i pubblici funzionari redigano un verbale in occasione degli accertamenti condotti presso la Società, il responsabile di direzione coinvolto ha l'obbligo di firmare questi verbali e di mantenerne copia nei propri uffici.

Gestione della Sicurezza sui luoghi di lavoro

- Sono predisposti un budget, piani annuali e pluriennali di investimento e programmi specifici al fine di identificare e allocare le risorse necessarie per il raggiungimento di obiettivi in materia di salute e sicurezza;
- sono definite procedure, ruoli e responsabilità in merito alle fasi dell'attività di predisposizione e attuazione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori;
- sono definiti, in coerenza con le disposizioni di legge vigenti in materia, i meccanismi relativi a:
 - valutazione e controllo periodico dei requisiti di idoneità e professionalità del responsabile del servizio di prevenzione e protezione (c.d. "RSPP") e degli addetti al servizio di prevenzione e protezione (c.d. "SPP");
 - definizione delle competenze minime, del numero, dei compiti e delle responsabilità dei lavoratori addetti ad attuare le misure di emergenza, di prevenzione incendi e di primo soccorso;
 - processo di nomina e relativa accettazione da parte del Medico Competente, con evidenza delle modalità e della tempistica in caso di avvicendamento nel ruolo;
- sono definiti i meccanismi di predisposizione dei Documenti di Valutazione dei Rischi ("DVR", "DUVRI") per la Salute e la Sicurezza sul Lavoro;
- è predisposto un modello di monitoraggio sistemico e continuo dei dati/indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il sistema di prevenzione e protezione;
- sono individuati i requisiti e le competenze specifiche per la conduzione delle attività di audit sul modello di Salute e Sicurezza dei lavoratori nonché le modalità e le tempistiche delle verifiche sullo stato di attuazione

delle misure adottate;

- sono previste riunioni periodiche con la dirigenza, con i lavoratori e i loro rappresentanti;
- è prevista la consultazione preventiva dei rappresentanti dei lavoratori in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive;
- devono essere previsti meccanismi di controllo che garantiscano l'inclusione nei contratti di appalto, subappalto e somministrazione, dei costi relativi alla sicurezza del lavoro.

Formazione del Bilancio civilistico (Financial Closing) e gestione dei rapporti con il Collegio Sindacale (ove nominato) e Soci

- Devono essere diffuse al personale coinvolto in attività di predisposizione del bilancio, norme anche di gruppo che definiscano con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio civilistico e consolidato e le modalità operative per la loro contabilizzazione. Tali norme devono essere tempestivamente integrate / aggiornate dalle indicazioni fornite dall'ufficio competente sulla base delle novità in termini di normativa civilistica e diffuse ai destinatari sopra indicati;
- devono essere previamente identificati i dati e le notizie da fornire alla Direzione Amministrazione Finanza e Controllo ed alla Funzione Contabilità e Bilancio in relazione alle chiusure annuali e infrannuali (per il bilancio civilistico), con esplicitazione di modalità e tempistiche;
- qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, deve essere previsto che la funzione preposta informi tempestivamente l'Organismo di Vigilanza;
- i documenti riguardanti la formazione delle decisioni che governano le operazioni delle attività a rischio sopra indicate, nonché quelli che danno attuazione alle decisioni devono essere archiviati e conservati a cura della funzione competente per l'operazione;
- l'accesso ai documenti già archiviati deve essere consentito solo alle persone autorizzate in base alle procedure operative aziendali, al Collegio Sindacale (ove nominato), alla Società di Revisione e all'Organismo di Vigilanza;
- la trasmissione delle informazioni deve essere consentita alle sole persone autorizzate e avvenire attraverso mezzi tecnici che garantiscano la sicurezza dei dati e la riservatezza delle informazioni;
- il sistema informatico utilizzato per la trasmissione di dati e informazioni deve garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascuna Direzione/Funzione coinvolto nel processo deve garantire la tracciabilità di tutti i dati e le informazioni finanziarie. La procedura concernente la circolazione di tali dati e informazioni finanziarie prevede che la mera trasmissione degli stessi comporti l'automatica attestazione del mittente in merito alla completezza e veridicità dei medesimi (generati in modo automatico e non automatico);
- ogni modifica ai dati contabili deve essere effettuata dalla sola Direzione/Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Direttore/Responsabile di Funzione;
- devono essere erogate, oltre che alle funzioni coinvolte nella redazione del bilancio e dei documenti connessi, attività di formazione di base (in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio) anche alle funzioni interessate alla attività di definizione delle poste valutative del bilancio;
- devono essere previste regole formalizzate che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione dell'Organo Amministrativo al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;
- devono essere previste regole di comportamento, rivolte agli Amministratori per la massima correttezza nella redazione delle comunicazioni imposte o comunque previste dalla legge e dirette al Socio o al pubblico. Tali regole devono prevedere che nelle comunicazioni vengano inserite informazioni chiare, precise, veritiere e complete;
- per ciascuna funzione deve essere individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale (ove nominato) previa verifica della loro completezza, inerenza e correttezza;

- le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale (ove nominato), devono essere documentate e conservate a cura del responsabile di funzione;
- tutti i documenti all'ordine del giorno delle riunioni dell'Assemblea o dell'Organo Amministrativo relativi a operazioni sulle quali il collegio sindacale (ove nominato) debba esprimere parere devono essere messi a disposizione di quest'ultimo con ragionevole anticipo rispetto alla data della riunione;
- devono essere previste direttive che sanciscono l'obbligo alla massima collaborazione e trasparenza nei rapporti con il collegio sindacale (ove nominato), anche con riferimento a richieste di notizie relative alle controllate, all'andamento di determinate operazioni sociali o affari, e in occasione di richieste da parte del Socio;
- deve essere sempre garantita la tracciabilità di fonti e informazioni nei rapporti con il Socio e il collegio sindacale (ove nominato).

Gestione degli adempimenti societari e fiscali

- Gli adempimenti societari e fiscali e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle normative vigenti, nazionali o comunitarie;
- gli adempimenti societari e la predisposizione della relativa documentazione devono essere effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere.
- devono essere definite regole in materia di gestione dei dati contabili e controllo della correttezza e completezza dei medesimi dati contabili, nonché verifiche preventive circa la regolarità e correttezza del bilancio;
- devono essere eseguite apposite verifiche sugli adempimenti tributari, sulle imposte dovute e sulle dichiarazioni fiscali (tax risk management), anche se possibile tramite specifiche procedure in tema di *compliance* contabile/fiscale).

Gestione, amministrazione e manutenzione degli apparati telematici, dei sistemi, dei database e delle applicazioni

Generale

- La politica sulla sicurezza delle informazioni deve esser redatta, formalmente approvata, aggiornata periodicamente e comunicata a tutto il personale aziendale; le policies e le procedure relative alla gestione della sicurezza delle informazioni devono esser allineate all'orientamento indicato nella politica, devono esser aggiornate periodicamente e diffuse a tutti gli utenti;
- la gestione del back up deve esser disciplinata da una procedura in cui siano definite le attività di back up per ogni rete di telecomunicazione, la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;
- a fronte di eventi disastrosi la Società deve prevedere un piano di Business Continuity ed un piano di Disaster Recovery, al fine di garantire la continuità dei sistemi informativi e dei processi ritenuti critici; le soluzioni individuate devono esser periodicamente aggiornate e testate;
- la generazione e la protezione dei log delle attività sui sistemi, almeno nel contesto delle attività relative a dati sensibili, devono esser disciplinate da apposite procedure formalizzate;
- la rilevazione e risoluzione degli incidenti di sicurezza logica deve esser regolamentata da procedure idonee in cui siano definiti i criteri di classificazione degli incidenti e livelli di escalation a seconda della tipologia dell'anomalia segnalata, sia prevista la comunicazione degli stessi ai soggetti interessati e siano condotte attività di reporting sui risultati ottenuti.

Gestione di accessi, account e profili

- I requisiti di autenticazione ai sistemi per l'accesso ai dati, per l'accesso alle applicazioni ed alla rete devono essere individuali ed univoci;
- la procedura che definisce le regole per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad esempio: lunghezza minima della password,

regole di complessità, scadenza, ecc.) deve essere formalizzata e comunicata a tutti gli utenti per la selezione e l'utilizzo della parola chiave;

- l'assegnazione dell'accesso remoto ai sistemi da parte di soggetti terzi quali consulenti e fornitori deve essere regolato mediante l'esecuzione delle attività definite in una procedura formalizzata;
- gli accessi effettuati sugli applicativi dagli utenti devono essere oggetto di verifiche e, per quanto concerne l'ambito dei dati sensibili, le applicazioni devono tener traccia delle modifiche ai dati compiute dagli utenti e devono essere attivati controlli che identificano variazioni di massa nei database aziendali;
- la gestione di account e di profili di accesso deve prevedere l'utilizzo di un sistema formale di autorizzazione e registrazione dell'attribuzione, modifica e cancellazione dei profili di accesso ai sistemi; devono essere formalizzate procedure per l'assegnazione e l'utilizzo di privilegi speciali (amministratore di sistema, super user, ecc.);
- devono essere condotte verifiche periodiche dei profili utente al fine di convalidare il livello di responsabilità dei singoli con i privilegi concessi; i risultati devono essere opportunamente registrati.

Gestione dei sistemi hardware

- La gestione dei sistemi hardware deve prevedere la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e regolamentare le responsabilità, le modalità operative in caso di implementazione e/o manutenzione di hardware in una procedura formalizzata.

Gestione dei sistemi software

- La gestione dei sistemi software deve includere la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione, sui principali sistemi, di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso;
- il processo di change management inteso come manutenzione al software o nuove implementazioni deve essere definito da procedure formali per il controllo ed il test del nuovo software rilasciato sia da personale interno che da fornitori in outsourcing.

Gestione degli accessi fisici ai siti ove risiedono le infrastrutture IT

- La gestione della sicurezza fisica dei siti ove risiedono le infrastrutture deve includere in una apposita procedura formalizzata le misure di sicurezza adottate, le modalità di vigilanza, la frequenza, le responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;
- l'accesso fisico ai locali riservati in cui risiedono le infrastrutture IT deve essere garantito mediante l'utilizzo di codici di accesso, token authenticator, pin, badge, valori biometrici; devono essere effettuati controlli periodici sulla corrispondenza delle abilitazioni concesse ed il ruolo ricoperto dall'utente autorizzato.

Gestione e sicurezza della documentazione in formato digitale

- L'utilizzo di specifiche tecniche di crittografia per la protezione e/o trasmissione delle informazioni deve essere regolamentato in una procedura formalizzata in cui siano definite le modalità operative e le responsabilità dei soggetti coinvolti nel processo di gestione;
- deve essere implementato un sistema di gestione delle chiavi a sostegno dell'uso delle tecniche crittografiche per la generazione, distribuzione, revoca ed archiviazione delle chiavi;
- devono essere predisposti ed opportunamente documentati i controlli per la protezione delle chiavi da possibili modifiche, distruzioni, utilizzi non autorizzati;
- devono essere formalizzate le procedure che regolamentano la gestione dell'utilizzo della firma digitale nei documenti, disciplinandone responsabilità, livelli autorizzativi, regole di adozione di sistemi di certificazione, eventuale utilizzo ed invio dei documenti, modalità di archiviazione e distruzione degli stessi;

- la procedura di archiviazione, produzione e manutenzione di un documento informatico deve essere redatta e diffusa a tutti i soggetti che sono coinvolti nel processo di gestione di un documento informatico.

Gestione delle attività antiriciclaggio

- È prevista la rilevazione di operazioni (pagamenti) ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette;
- sono immediatamente interrotte o, comunque, non è data esecuzione ad operazioni di incasso e pagamento che vedano coinvolti soggetti operanti, anche in parte, in Stati segnalati come non cooperativi secondo le indicazioni di organismi nazionali e/o sopranazionali operanti nell'antiriciclaggio e nella lotta al terrorismo;
- le operazioni che comportano utilizzo o impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie devono essere autorizzate ed avere una causale espressa ed essere documentate e registrate in conformità con i principi di professionalità e correttezza gestionale e contabile; il processo operativo e decisionale deve essere tracciabile e verificabile nelle singole operazioni;
- deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione anche con riferimento alle operazioni infragruppo;
- deve essere previsto il divieto di utilizzo del contante, ad eccezione dell'uso per importi non significativi della cassa interna, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie nonché il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili.
- devono in generale essere rispettate le prescrizioni normative di cui al D.lgs. n. 231/2007 (antiriciclaggio) e le relative disposizioni contenute nelle procedure operative all'uso adottate dalla Società, soprattutto con riferimento alle attività di gioco a distanza ed alle scommesse, rispettivamente ai sensi dell'art. 14, co. 1, lett. e ed e-bis del citato D.lgs. n. 231/2007.

Selezione, assunzione, gestione del personale dipendente

- Per la selezione del personale devono esistere procedure con criteri oggettivi di selezione dei candidati e un'autorizzazione formalizzata all'assunzione;
- la scelta dei dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile;
- devono essere definiti criteri di controllo nel caso in cui l'ente stesso faccia ricorso al lavoro interinale mediante le agenzie specializzate;
- nei contratti di assunzione il dipendente deve firmare apposita dichiarazione per l'accettazione delle regole e dei comportamenti previsti nel Modello e nel Codice Etico;
- deve essere predisposto un budget annuale per gli inserimenti di nuovo personale; eventuali richieste extra budget devono essere formalmente autorizzate da soggetto avente responsabilità in materia;
- eventuali sistemi premianti ai dipendenti e collaboratori devono rispondere ad obiettivi realistici e coerenti con le mansioni, l'attività svolta e le responsabilità affidate;
- nell'assunzione di dipendenti, consulenti e collaboratori deve essere preventivamente assicurato il controllo sia formale sia sostanziale da parte delle funzioni competenti della presenza nelle Liste di Riferimento.

Gestione degli adempimenti in materia ambientale

- assicurare l'esistenza di una normativa aziendale che definisca ruoli, responsabilità e modalità operative per:
 - la valutazione periodica e l'individuazione del rischio ambientale aziendale (ad es. in tema di gestione dei rifiuti) e l'identificazione e la gestione di tutte le attività svolte dalla Società che possano comportare l'accadimento di un evento potenzialmente contaminante o inquinante dell'aria, suolo, sottosuolo e delle acque sotterranee e superficiali (in particolare, tali da poter comportare una

compromissione o un deterioramento significativi e misurabili (i) delle acque o dell'aria, o di porzioni estese o significative del suolo o sottosuolo, o (ii) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna ovvero una alterazione irreversibile di un ecosistema), affinché sia prevenuto o comunque ridotto il rischio di accadimento di tali eventi;

- la verifica iniziale e periodica della necessità e del possesso di certificazioni, licenze ed autorizzazioni ambientali eventualmente previste dalla normativa;
 - la gestione della documentazione, delle certificazioni e delle autorizzazioni amministrative ambientali e la calendarizzazione degli adempimenti eventualmente necessari (richiesta, aggiornamento, ecc.);
 - l'individuazione e rispetto degli adempimenti previsti dalla normativa o dagli atti autorizzativi, rispettandone scrupolosamente tutte le relative prescrizioni;
 - la predisposizione e archiviazione della documentazione amministrativa relativa;
 - la tracciabilità di tutte le attività relative alla gestione dei fattori inquinanti;
- accertare, prima dell'instaurazione del rapporto, la rispettabilità e l'affidabilità dei fornitori di servizi connessi alla gestione dei rifiuti, anche attraverso l'acquisizione e la verifica delle comunicazioni, certificazioni e autorizzazioni in materia ambientale da questi effettuate o acquisite a norma di legge;
 - inserire nei contratti stipulati con i fornitori di servizi connessi alla gestione dei rifiuti specifiche clausole attraverso le quali ciascuna società possa riservarsi il diritto di verificare periodicamente le comunicazioni, certificazioni e autorizzazioni in materia ambientale, tenendo in considerazione i termini di scadenza e rinnovo delle stesse;
 - svolgere l'attività di gestione e smaltimento dei rifiuti con la massima cura ed attenzione con particolare riferimento alla caratterizzazione dei rifiuti, alla gestione dei depositi temporanei, al divieto di miscelazione dei rifiuti siano essi pericolosi o non pericolosi;
 - affidare 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;
 - a tal riguardo, in particolare assicurare che:
 - gli operatori economici inseriti nell'albo delle imprese qualificate che svolgano attività di gestione dei rifiuti, siano sottoposti a costante monitoraggio e aggiornamento, anche attraverso la consultazione dell'Albo Nazionale dei Gestori Ambientali tenuto presso il Ministero dell'Ambiente e della Tutela del Territorio e del Mare;
 - in sede di affidamento delle attività di smaltimento o recupero di rifiuti alle imprese autorizzate sia verificata: a) la data di validità dell'autorizzazione, b) la tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero; c) la localizzazione dell'impianto di smaltimento e d) il metodo di trattamento o recupero;
 - in fase di esecuzione delle attività di trasporto di rifiuti alle imprese autorizzate sia verificata: a) la data di validità dell'autorizzazione; b) la tipologia e la targa del mezzo; c) i codici CER autorizzati;
 - vigilare costantemente sulla corretta gestione dei rifiuti segnalando eventuali irregolarità alle Strutture competenti al fine di porre in essere le conseguenti azioni di tipo amministrativo e contrattuale oltre che le eventuali azioni di tipo legale dinanzi alla competente autorità.

SEZIONE TERZA

3 Organismo di Vigilanza

3.1 Identificazione 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 interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso rimessi.

Non potrà essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal Decreto.

In ossequio alle prescrizioni del Decreto, alle indicazioni espresse dalle Linee Guida di Confindustria e agli orientamenti della giurisprudenza formati in materia, HBG On Line Gaming ha ritenuto di istituire un Organismo di Vigilanza di natura collegiale, interno alla Società, dotato di autonomia ed indipendenza dagli altri organi societari e di controllo interno.

In ogni caso, i componenti dell'Organismo di Vigilanza sono - e saranno - scelti tra soggetti che non abbiano rapporti di parentela con i soci e con gli Amministratori, che ne possano compromettere l'indipendenza di giudizio.

L'Organismo di Vigilanza è composto da membri interni e/o esterni alla Società.

I componenti interni non potranno essere scelti tra dirigenti responsabili di funzioni appartenenti alle aree di business aziendale o soggetti dotati di poteri decisori ed i componenti esterni non dovranno avere rapporti commerciali con la Società che possano configurare ipotesi di conflitto di interessi.

Nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza riferisce esclusivamente all'Organo Amministrativo.

All'Organismo di Vigilanza sono attribuiti autonomi poteri di spesa che prevedono l'impiego di un budget annuo adeguato, approvato dall'Organo Amministrativo, su proposta dell'Organismo di Vigilanza. L'Organismo di Vigilanza può impegnare risorse che eccedono i propri poteri di spesa, dandone successivamente conto all'Organo Amministrativo.

L'Organismo di Vigilanza è nominato dall'Organo Amministrativo, sentito il parere del Collegio Sindacale (ove nominato). I componenti dell'Organismo di Vigilanza sono scelti tra soggetti qualificati, con competenze in ambito legale o contabile o di controllo interno, provvisti dei requisiti di:

- **Autonomia e indipendenza:** detto requisito è assicurato dalla composizione plurisoggettiva dell'Organismo di Vigilanza, dall'assenza di alcun riporto gerarchico all'interno dell'organizzazione e dalla facoltà di reporting all'Organo Amministrativo.
- **Professionalità:** requisito questo garantito dal bagaglio di conoscenze professionali, tecniche e pratiche, di cui dispongono i componenti dell'Organismo di Vigilanza.
- **Continuità d'azione:** con riferimento a tale requisito, l'Organismo di Vigilanza è tenuto a vigilare costantemente, attraverso poteri di indagine, sul rispetto del Modello, a curarne l'attuazione e l'aggiornamento, rappresentando un riferimento costante per tutto il personale della Società.

I componenti dell'Organismo di Vigilanza restano in carica per due anni e sono in ogni caso rieleggibili.

Mediante appositi documenti organizzativi/comunicazioni interne sono stabiliti i criteri di funzionamento del suddetto Organismo, nonché i flussi informativi da e verso l'Organismo stesso. Per il suo funzionamento, l'Organismo si è inoltre dotato di un proprio Regolamento, comunicato per informativa all'Organo Amministrativo.

L'Organo Amministrativo designa tra i membri dell'Organismo di Vigilanza un Presidente, al quale può essere delegato l'esercizio di specifiche funzioni, secondo quanto previsto dal Regolamento. Ove non vi provveda l'Organo Amministrativo, il Presidente è nominato dallo stesso Organismo di Vigilanza tra i propri membri. Il Regolamento dell'Organismo di Vigilanza individua i requisiti di indipendenza richiesti ai componenti dell'Organismo di Vigilanza, e definisce le cause di ineleggibilità, decadenza e revoca dall'incarico.

3.2 Poteri e funzioni dell'Organismo di Vigilanza

All'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

Tali compiti sono svolti dall'Organismo attraverso le seguenti attività:

- vigilanza sulla diffusione nel contesto aziendale della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilanza sulla validità ed adeguatezza del Modello, con particolare riferimento ai comportamenti riscontrati nel contesto aziendale;
- verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal Decreto;
- propone l'aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e/o adeguamenti dello stesso, in relazione alle mutate condizioni legislative e/o aziendali (cfr. par. 5 "Aggiornamento del Modello").

Nello svolgimento di dette attività, l'Organismo provvederà ai seguenti adempimenti:

- collaborare con la direzione aziendale competente nella programmazione di un piano periodico di formazione volto a favorire la conoscenza delle prescrizioni del Modello di HBG On Line Gaming differenziato secondo il ruolo e la responsabilità dei destinatari;
- istituire specifici canali informativi "dedicati" (indirizzo di posta elettronica dedicato), diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello.

Al fine di consentire all'Organismo la miglior conoscenza in ordine all'attuazione del Modello, alla sua efficacia e al suo effettivo funzionamento, nonché alle esigenze di aggiornamento dello stesso, è fondamentale che l'Organismo di Vigilanza operi in stretta collaborazione con le Direzioni aziendali.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo è dotato dei poteri di seguito indicati:

- accedere liberamente, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D.Lgs. 231/2001;
- disporre che i responsabili delle Direzioni aziendali, e in ogni caso tutti i Destinatari, forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- ricorrere a consulenti esterni nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello.

3.3 Reporting dell'Organismo di Vigilanza

Al fine di garantire la piena autonomia e indipendenza nello svolgimento delle relative funzioni, l'Organismo di Vigilanza comunica direttamente all'Organo Amministrativo della Società, e al Collegio Sindacale (ove nominato). Segnatamente, l'Organismo di Vigilanza riferisce, sia all'Organo Amministrativo sia al Collegio Sindacale (ove nominato), lo stato di fatto sull'attuazione del Modello, gli esiti dell'attività di vigilanza svolta e gli eventuali interventi opportuni per l'implementazione del Modello:

- in modo continuativo nei confronti dell'Organo Amministrativo e, almeno semestralmente, attraverso una relazione scritta;
- periodicamente nei confronti del Collegio Sindacale (ove nominato), su richiesta dello stesso in ordine alle attività svolte;
- occasionalmente nei confronti del Collegio Sindacale (ove nominato), nei casi di presunte violazioni poste in essere dall'Organo Amministrativo, potendo ricevere dal Collegio Sindacale richieste di informazioni o di chiarimenti.

L'OdV di HBG On Line Gaming potrà essere convocato in qualsiasi momento dai suddetti organi o potrà a sua volta presentare richiesta in tal senso, per riferire in merito al funzionamento del Modello o a situazioni specifiche. Annualmente, inoltre, l' OdV di HBG On Line Gaming trasmette all'Organo Amministrativo, un report scritto sull'attuazione del Modello presso HBG On Line Gaming.

3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza, secondo quanto previsto dai protocolli adottati e nelle singole Parti Speciali del Modello.

Per ciascuna "area a rischio reato" (come enunciate al precedente paragrafo 2.9) saranno identificati uno o più "Responsabili Interni" che dovranno, tra l'altro, fornire all'OdV almeno con cadenza semestrale, i flussi informativi così come dallo stesso definiti (fatti salvi i casi in cui su indicazione o in accordo con l'Organismo di Vigilanza i flussi informativi potranno avere una periodicità almeno annuale). Anche nel caso in cui, nel periodo selezionato, non vi siano state segnalazioni significative da comunicare all'OdV, allo stesso dovrà essere inviata una segnalazione "negativa".

Sono stati inoltre istituiti precisi obblighi gravanti sugli organi sociali e sul personale di HBG On Line Gaming in particolare:

- gli organi sociali devono riferire all'Organismo di Vigilanza ogni informazione rilevante per il rispetto e il funzionamento del Modello;
- i Destinatari devono riferire all'Organismo di Vigilanza ogni informazione relativa a comportamenti che possano integrare violazioni delle prescrizioni del Modello o fattispecie di reato.

A tali fini è istituito un canale di comunicazione per la consultazione dell'Organismo di Vigilanza, consistente in un indirizzo di posta elettronica dedicato, e precisamente OdV-HbgOnLineGaming@hbg-gaming.it, al quale potranno essere inviate le eventuali segnalazioni. Tale modalità di trasmissione delle segnalazioni è volta a garantire la riservatezza dei segnalanti anche al fine di evitare atteggiamenti ritorsivi nei loro confronti. Inoltre le segnalazioni potranno essere inviate presso il seguente indirizzo:

HBG On Line Gaming S.r.l. – Organismo di Vigilanza

Via Cesare Pascarella, 7

00153 Roma

L'Organismo di Vigilanza valuterà le segnalazioni pervenutegli, e potrà convocare, qualora lo ritenga opportuno, sia il segnalante per ottenere maggiori informazioni, assicurandogli la necessaria riservatezza, che il presunto autore della violazione, dando inoltre luogo a tutti gli accertamenti e le indagini che siano necessarie per appurare la fondatezza della segnalazione.

Oltre alle segnalazioni sopra indicate, devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, 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 assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario, in particolare per i reati ricompresi nel Decreto;
- attività di controllo svolte dai responsabili di altre direzioni 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 (ivi compresi i provvedimenti verso i dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- segnalazione di infortuni gravi (omicidio colposo o lesioni colpose gravi o gravissime, in ogni caso qualsiasi infortunio con prognosi superiore ai 40 giorni) occorsi a dipendenti, addetti alla manutenzione, 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.

SEZIONE QUARTA

4 Sistema sanzionatorio

4.1 Destinatari e apparato sanzionatorio e/o risolutivo

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al Decreto, e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

Sanzioni per i lavoratori dipendenti

Ai comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono applicabili – fatta eccezione per i richiami verbali – le procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e le norme pattizie di cui al Contratto Collettivo Nazionale di Lavoro del Terziario vigente e applicabile a cui si rimanda.

In particolare, in caso di (a) violazione delle disposizioni del Modello, delle sue procedure interne (ad esempio il mancato rispetto delle procedure, la mancata comunicazione delle informazioni richieste all'Organismo di Vigilanza, il mancato svolgimento dei controlli, etc.), del Codice Etico, del Decreto o di qualsivoglia altra disposizione penale in esso inclusa o (b) mancato rispetto delle disposizioni di cui al Modello nello svolgimento di attività in aree "a rischio" o (c) danneggiamento della Società o l'aver causato una situazione oggettiva di pericolo per i beni della stessa (gli "Illeciti Disciplinari") saranno applicabili i seguenti provvedimenti disciplinari per i Dipendenti:

- biasimo inflitto verbalmente;
- biasimo inflitto per iscritto;
- multa in misura non eccedente l'importo di quattro ore della normale retribuzione;
- sospensione dalla retribuzione e dal servizio per un massimo di giorni dieci;
- licenziamento disciplinare.

Sanzioni nei confronti dei dirigenti

Nel caso in cui i dirigenti commettano un Illecito Disciplinare, si provvederà ad applicare nei confronti dei responsabili le seguenti misure in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti di Aziende del Terziario, Distribuzione e Servizi vigente e applicabile:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione – o ripetute violazioni - di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
- laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

Sanzioni nei confronti dei membri dell'OdV

In caso di Illeciti Disciplinari commessi da membri dell'OdV, l'Organo Amministrativo dovrà essere prontamente informato e lo stesso potrà richiamare per iscritto tale membro dell'OdV o revocarlo a seconda della gravità dell'illecito commesso. Le sanzioni previste per dipendenti e dirigenti si applicheranno altresì ai membri dell'OdV che ricadono in tali categorie.

Misure nei confronti degli Amministratori e dei Sindaci (ove nominati)

In caso di Illeciti Disciplinari commessi da Amministratori o da Sindaci della Società, l'OdV informerà l'Organo Amministrativo e il Collegio Sindacale (ove nominato) della stessa i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa, coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, revoca per giusta causa, ecc.).

Misure nei confronti di Collaboratori, Partner, Consulenti e Fornitori

Ogni comportamento posto in essere da Collaboratori, Partners, Consulenti o Fornitori che configuri un Illecito Disciplinare potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di partnership, la risoluzione automatica del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società.

Misure nei confronti di dipendenti di Società del Gruppo HBG che operano su mandato o nell'interesse di HBG On Line Gaming

In caso Illeciti Disciplinari commessi da parte di risorse, appartenenti a società del Gruppo, che operino, anche di fatto, su mandato e nell'interesse della Società, l'OdV di HBG On Line Gaming informerà l'Organo Amministrativo. Quest'ultimo, per il tramite delle strutture competenti della Società, comunicherà l'accaduto agli organi/strutture deputate delle società del Gruppo HBG interessate, le quali valuteranno la situazione e, provvederanno ad adottare le più opportune misure sanzionatorie, in base alle normative interne e locali.

5 Aggiornamento del Modello

L'adozione e l'efficace attuazione del Modello sono - per espressa previsione legislativa - una responsabilità rimessa all'Organo Amministrativo. Ne deriva che il potere di adottare eventuali aggiornamenti del Modello compete, dunque, all'Organo Amministrativo, 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 Decreto.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti dell'Organo Amministrativo.

6 Informazione e formazione del personale

Conformemente a quanto previsto dal Decreto, HBG On Line Gaming ha definito un programma di comunicazione e formazione finalizzato a garantire una corretta divulgazione e conoscenza del Modello e delle regole di condotta in esso contenute, nei confronti delle risorse già presenti in azienda e di quelle da inserire.

Il sistema di informazione e formazione è supervisionato dall'Organismo di Vigilanza ed è gestito dalla Funzione Risorse Umane con i responsabili delle direzioni aziendali di volta in volta coinvolte nell'applicazione del Modello.

In relazione alla comunicazione del Modello, HBG On Line Gaming si impegna a:

- diffondere il Modello nel contesto aziendale attraverso qualsiasi strumento ritenuto idoneo (ad esempio, e-mail, intranet);
- organizzare uno specifico incontro formativo con tutti i dipendenti della Società nell'ambito del quale illustrare il D.Lgs. 231/2001 ed il Modello adottato.

In ogni caso, l'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 e le prescrizioni del Modello adottato sarà differenziata nei contenuti e nelle modalità in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

ALLEGATO A – FATTISPECIE DEI REATI

Sono elencati, di seguito, tutti i reati attualmente ricompresi nell'ambito di applicazione del Decreto suddivisi per macrocategorie.

Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto):

- Malversazione a danno dello Stato o di altro ente pubblico o dell'Unione Europea (art. 316 bis c.p.);
- Indebita percezione di erogazioni a danno dello Stato o di altro ente pubblico o dell'Unione europea (art. 316 ter c.p.);
- Concussione (art. 317 c.p.)
- Corruzione per l'esercizio della funzione o corruzione per un atto contrario ai doveri d'ufficio (artt. 318 - 319 c.p.)
- Circostanze aggravanti (art. 319 bis);
- Corruzione in atti giudiziari (art. 319 ter c.p.);
- Induzione indebita a dare o promettere utilità (art.319 quater c.p.)
- Pene per il corruttore (art. 321 c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.);
- Truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1, c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);
- Frode informatica a danno dello Stato o di altro ente pubblico (art. 640 ter c.p.);

Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis del Decreto):

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo, o di carta filigranata (art. 461 c.p.);
- Uso di valori bollati contraffatti o alterati (art. 464, commi 1 e 2, c.p.);
- Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 c.p.);
- Introduzione nello stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Reati societari (art. 25 ter del Decreto):

- False comunicazioni sociali (artt. 2621, 2621 bis e 2622 c.c.);
- Impedito controllo (art. 2625, comma 2, c.c.);

- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.);
- Estensione delle qualifiche soggettive (art. 2639 c.c.);
- Corruzione tra privati (art. 2635 c.c.).

Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 quater del Decreto).

Pratiche di mutilazione degli organi genitali femminili (art. 25 quater 1, del Decreto):

- Pratiche di mutilazione degli organi genitali femminili (art. 583 bis c.p.).

Reati contro la personalità individuale (art. 25 quinquies del Decreto):

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600 bis c.p.);
- Pornografia minorile (art. 600 ter c.p.);
- Detenzione di materiale pornografico (art. 600 quater c.p.);
- Pornografia virtuale (art. 600 quater.1, c.p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603 bis c.p.);
- Adescamento di minorenni (art. 609-undecies c.p.).

Reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25 sexies del Decreto):

- Abuso di informazioni privilegiate (art. 184 T.U.F.);
- Manipolazione del mercato (art. 185 T.U.F.);
- Illecito amministrativo di abuso di informazioni privilegiate (art. 187-bis TUF);
- Illecito amministrativo di manipolazione di mercato (art. 187-ter TUF).

Reati transnazionali:

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.);
- Favoreggiamento personale (art. 378 c.p.);

- Associazione per delinquere (art.416 c.p.);
- Associazione di tipo mafioso (art.416 bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (D.P.R. 43/1973, art. 291 quater);
- Disposizioni contro le immigrazioni clandestine (D.Lgs. 286/1998, art. 12, comma 3, 3 bis, 3 ter e 5);
- Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 DPR 309/90);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del DPR n. 309/90).

Reati colposi commessi in violazione della normativa antinfortunistica e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies del Decreto):

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose, gravi o gravissime (art. 590 c.p.).

Reati in materia di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 octies del Decreto):

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- Autoriciclaggio (art. 648 ter 1 c.p.).

Reati di criminalità informatica (art. 24 bis del Decreto):

- Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- Danneggiamento di sistemi informatici e telematici (art. 635 quater c.p.);
- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 quinquies c.p.);
- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.).

Reati di criminalità organizzata introdotti dalla Legge 94/2009 (art. 24 ter del Decreto):

- Associazione per delinquere (art. 416, ad eccezione sesto comma, c.p.);
- Associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d. lgs 286/1998 (art. 416, sesto comma, c.p.);
- Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.);

- Scambio elettorale politico-mafioso (art. 416 ter c.p.);
- Sequestro di persona a scopo di estorsione (Art. 630 c.p.);
- Associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 DPR 309/90);
- Delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine (art. 407 comma 2 lettera a) c.p.p).

Reati contro l'industria e il commercio introdotti dalla Legge 99/2009 (art. 25 bis 1):

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.).

Reati in materia di violazione del diritto d'autore introdotti dalla Legge 99/2009 (art. 25 novies del Decreto):

- Immissione su sistemi di reti telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette o parte di esse (art. 171, primo comma, lett. a-bis) Legge 633/41);
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, terzo comma Legge 633/41);
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di un programma per elaboratori (art. 171-bis, comma 1 Legge 633/41);
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati; estrazione o reimpiego della banca di dati; distribuzione, vendita o concessione in locazione di banca di dati (art. 171-bis, comma 2, Legge 633/41);
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico – musicali, multimediali, anche se inserite in opere collettive o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita, cessione o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette (art. 171-ter, Legge 633/41);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies, Legge 633/41);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies, Legge 633/41).

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria introdotti dalla Legge 116/2009 (art. 25 decies del Decreto):

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.).

Reati ambientali, introdotti nel Decreto dal D.Lgs. 121/2011 (art. 25-undecies):

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727--bis c.p.);
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
- Scarichi di acque reflue industriali 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. 137 commi 2, 3, 5, 11 e 13 D.Lgs. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 commi 1, 3, 5 e 6 secondo periodo D.Lgs. 152/2006);
- Omessa bonifica dei siti in conformità al progetto approvato dall'autorità competente (art. 257 commi 1 e 2 D.Lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 comma 4 secondo periodo D.Lgs. 152/2006);
- Traffico illecito di rifiuti (art. 259 comma 1 D.Lgs. 152/2006);
- Attività organizzate per il traffico illecito di rifiuti (art. 260 commi 1 e 2 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. 260-bis D.Lgs. 152/2006);
- Superamento di valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria (art. 279 comma 5 D.Lgs. 152/2006);
- Importazione, esportazione, riesportazione di esemplari appartenenti alle specie protette di cui agli Allegati A, B e C del Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii.; omessa osservanza delle prescrizioni finalizzate all'incolumità degli esemplari appartenenti alle specie protette; uso dei predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi; trasporto e transito degli esemplari in assenza del certificato o della licenza prescritti; commercio di piante riprodotte artificialmente in contrasto con le prescrizioni di cui all'art. 7 par. 1 lett. b) Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii.; detenzione, uso per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali, offerta in vendita o cessione di esemplari senza la prescritta documentazione (artt. 1 e 2 Legge n. 150/1992);
- Falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni previste dall'art. 16, par. 1, lett. a), c), d), e), ed l), del Regolamento CE n. 338/97 del Consiglio, del 9 dicembre 1996 e ss.mm.ii. (art. 3 Legge n. 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 per l'incolumità pubblica (art. 6 Legge n. 150/1992);
- Cessazione e riduzione dell'impiego di sostanze lesive (art. 3 Legge n. 549/1993);
- Inquinamento doloso di nave battente qualsiasi bandiera (art. 8 D.Lgs. n. 202/2007);
- Inquinamento colposo di nave battente qualsiasi bandiera (art. 9 D.Lgs. n. 202/2007).
- Inquinamento ambientale (art. 452 bis c.p.);
- Disastro ambientale (art. 452 quater c.p.);
- Delitti colposi contro l'ambiente (art. 452 quinquies c.p.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.);
- Circostanze aggravanti (art. 452 octies c.p.).

Reato di “Impiego di cittadini di paesi terzi il cui soggiorno nel territorio dello Stato risulti irregolare” (art. 25-duodecies del Decreto).

ALLEGATO B – ARTICOLI DEL CODICE PENALE RICHIAMATI DALL’ART 4 DEL D.LGS. 231/2001

Art. 7 “Reati commessi all’estero”

Punibilità incondizionata per il cittadino o lo straniero che commette all’estero:

- a) delitti contro la personalità dello Stato;
- b) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto;
- c) delitti di falsità in monete aventi corso legale nel territorio dello Stato o in valori di bollo o in carte di pubblico credito italiano;
- d) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alla propria funzione;
- e) ogni altro reato per il quale specifiche disposizioni di legge o convenzioni internazionali stabiliscono l’applicabilità della legge penale italiana.

Art. 8 “Delitto politico commesso all’estero”

Punibilità per il cittadino o lo straniero che commette all’estero un delitto politico (ossia un delitto che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino o ancora un delitto comune determinato in tutto o in parte da motivi politici), su richiesta del Ministro della Giustizia o a querela della persona offesa se si tratta di reato perseguibile a querela di parte.

Si fa presente che non vi sono reati ex d.lgs. 231/2001 qualificabili come “delitti politici”.

Art. 9 “Delitto comune del cittadino all’estero”

Punibilità per il cittadino che, fuori dai casi indicati in precedenza commette all’estero un reato per il quale la legge italiana stabilisce l’ergastolo o la reclusione non inferiore nel minimo a tre anni, se questi si trova nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del Ministro della Giustizia ovvero a istanza o querela della persona offesa.

In entrambi i casi, se si tratta di delitto commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del Ministro della Giustizia se non è stata concessa l’extradizione o se non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto.

Art. 10 “Delitto comune dello straniero all’estero”

Punibilità per lo straniero che, fuori dai casi indicati in precedenza commette all’estero un reato per il quale la legge italiana stabilisce l’ergastolo o la reclusione non inferiore nel minimo a un anno: a) se questi si trova nel territorio dello Stato e vi sia b) la richiesta del Ministro della Giustizia ovvero c) istanza o querela della persona offesa.

Se il delitto è commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero il colpevole è punito a richiesta del Ministro della Giustizia se: a) si trova nel territorio dello Stato, b) si tratta di delitto per il quale è stabilita la pena dell’ergastolo o della reclusione non inferiore nel minimo a tre anni, c) non è stata concessa l’extradizione o se non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto o da quello dello Stato a cui appartiene.