

**MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 8 GIUGNO 2001 N. 231
di The Data Appeal Company S.p.A.**

PARTE GENERALE	7
1. INTRODUZIONE	7
2. MODELLO DI ORGANIZZAZIONE E DI GESTIONE	11
3. ORGANISMO DI VIGILANZA	18
4. FLUSSI INFORMATIVI INTERNI	22
5. SISTEMA DISCIPLINARE	25
6. DIFFUSIONE E CONOSCENZA DEL MODELLO	28
PARTE SPECIALE “A”	30
Rapporti con la Pubblica Amministrazione	30
1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)	30
2. VALUTAZIONE DELLE AREE DI RISCHIO	40
3. INDIVIDUAZIONE DELLE ATTIVITÀ A RISCHIO	41
4. PRINCIPI DI COMPORTAMENTO NELLA GESTIONE DELLE ATTIVITÀ DI RISCHIO DIRETTO	42
5. PRINCIPI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO INDIRETTO	46
PARTE SPECIALE “B”	49
1. LA TIPOLOGIA DEI REATI SOCIETARI DI CUI AGLI ARTT. 2621 E SS. C.C. (ART. 25 TER DEL DECRETO)	49
2. AREE A RISCHIO	53
3. REGOLE DI COMPORTAMENTO GENERALI	53
4. REGOLE DI COMPORTAMENTO PARTICOLARI, RELATIVE ALLE SPECIFICHE AREE DI RISCHIO	54
PARTE SPECIALE “C”	58
1. I DELITTI DI CUI AGLI ARTT. 184 E 185 TUF (ART. 25 SEXIES DEL DECRETO)	58
2. GLI ILLECITI AMMINISTRATIVI DI CUI AGLI ARTT. 187-BIS E 187-TER DEL TUF	59
3. DEFINIZIONE DI STRUMENTI FINANZIARI RILEVANTE PER GLI ILLECITI EX ARTT. 184, 185, 187 BIS E 187 TER DEL TUF	60
4. AREE A RISCHIO	60
5. REGOLE GENERALI DI COMPORTAMENTO	60
PARTE SPECIALE “D”	62
1. OMICIDIO COLPOSO E LESIONI PERSONALI GRAVI E GRAVISSIME IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (ART. 25 SEPTIES DEL DECRETO)	62
2. DESTINATARI DELLA PRESENTE PARTE SPECIALE	64
3. FINALITÀ DELLA PRESENTE PARTE SPECIALE	64
4. SOGGETTI DEDICATI A COMPITI IN MATERIA DI SICUREZZA	66
5. POLITICA AZIENDALE DELLA SICUREZZA	66
6. PIANIFICAZIONE E ORGANIZZAZIONE DEL SISTEMA	68
7. PRINCIPI E REGOLE DI CONDOTTA GENERALI	68
8. REGOLE DI COMPORTAMENTO SPECIFICHE	70
9. VALUTAZIONE DEI RISCHI ESISTENTI	70
10. CASI PARTICOLARI E/O STRAORDINARI RISPETTO ALL’ATTIVITÀ AZIENDALE ORDINARIA	71
11. DOCUMENTAZIONE E VERBALIZZAZIONE DELLE ATTIVITÀ	72
12. DIVULGAZIONE, INFORMAZIONE E FORMAZIONE	72
13. CONTROLLO E RIVALUTAZIONE DEL SISTEMA DI SICUREZZA INTERNO	73

PARTE SPECIALE “E”	74
1. LA TIPOLOGIA DEI REATI DI RICETTAZIONE, RICICLAGGIO, REIMPIEGO DI DENARO, BENI O ALTRE UTILITÀ, AUTO – RICICLAGGIO (ART. 25 <i>OCTIES</i> DEL DECRETO)	74
2. VALUTAZIONE DELLE AREE DI RISCHIO	78
3. PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE A RISCHIO	79
4. REGOLE DI COMPORTAMENTO PARTICOLARI, RELATIVE ALLE SINGOLE AREE DI RISCHIO	81
PARTE SPECIALE “F”	82
1. LA TIPOLOGIA DEGLI ILLECITI INFORMATICI RILEVANTI (ART. 24 <i>BIS</i> DEL DECRETO).....	82
2. AREE A RISCHIO.....	86
3. REGOLE DI CONDOTTA E PROCEDURE	87
PARTE SPECIALE “G”	91
Delitti contro il diritto d'autore, l'industria ed il commercio.....	91
1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ARTT. 25 <i>BIS.1</i> , 25 <i>NOVIES</i> E 25 <i>BIS</i> COMMA 1 LETT. F <i>BIS</i> DEL DECRETO)	91
2. AREE A RISCHIO	101
3. REGOLE DI CONDOTTA	102
PARTE SPECIALE “H”	104
1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 25 <i>DECIES</i> DEL DECRETO) ...	104
2. AREA A RISCHIO	104
3. REGOLE GENERALI DI CONDOTTA	104
PARTE SPECIALE “I”	106
1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 25 <i>UNDECIES</i>)	106
2. VALUTAZIONE DELLE AREE DI RISCHIO	118
3. PRINCIPI GENERALI DI COMPORTAMENTO	119
PARTE SPECIALE “L”	121
1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 25 <i>QUINQUIES</i> DEL DECRETO)	121
2. AREE A RISCHIO	127
3. REGOLE GENERALI DI CONDOTTA	127
PARTE SPECIALE “M”	129
1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 <i>DUODECIES</i>).....	129
2. VALUTAZIONE DELLE AREE DI RISCHIO	132
3. PRINCIPI GENERALI DI COMPORTAMENTO	133
PARTE SPECIALE “N”	135
1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 24 <i>QUATER</i> DEL DECRETO) ..	135
2. AREA A RISCHIO	140
3. REGOLE GENERALI DI CONDOTTA	140
PARTE SPECIALE “O”	142
1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 <i>TER</i> , COMMA 1, LETT. S-BIS)	142
2. AREE A RISCHIO	143
3. I DESTINATARI DELLA PRESENTE PARTE SPECIALE.....	144
4. REGOLE DI COMPORTAMENTO.....	144
5. SEGNALAZIONI	146

PARTE SPECIALE “P”	147
6. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 TERDECIES)	147
7. LA VALUTAZIONE DELLE AREE DI RISCHIO	148
8. PRINCIPI GENERALI DI COMPORTAMENTO.....	148

DEFINIZIONI

Attività	indica le attività di raccolta ed elaborazione dati, le attività di fornitura di servizi svolte attraverso il Sito, così come infra definito, e i servizi accessori erogati dalla Società;
Codice della Privacy	indica il d.lgs. 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali;
Decreto	indica il D. lgs. 8 giugno 2001 n. 231;
Destinatari	indica tutti i soggetti tenuti al rispetto delle prescrizioni contenute nel Modello, in particolare: tutti coloro che operano in nome e per conto di The Data Appeal Company S.p.A., inclusi gli amministratori, i sindaci, i membri degli altri eventuali organi sociali, i dipendenti, i collaboratori anche occasionali, i procacciatori d'affari e gli agenti, i <i>partner</i> commerciali, i fornitori, i componenti dell'Organismo di Vigilanza;
Enti o Ente	ai sensi dell'art. 1 del Decreto, indica gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica cui si applicano le disposizioni del Decreto ed in particolare la responsabilità amministrativa dallo stesso introdotta;
GDPR	indica il Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali;
l.a.	indica la l. 22 aprile 1941 n. 633 in materia di Protezione del diritto d'autore e altri diritti connessi al suo esercizio;
Linee Guida	indica le Linee Guida per la costruzione dei Modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001 nell'ultima versione aggiornata al marzo 2014;
Modello	indica il Modello di organizzazione, gestione e controllo previsto dal Decreto;
Nana Bianca	indica la società Nana Bianca S.r.l., presso i cui uffici la Società svolge le proprie Attività in virtù di un apposito contratto di coworking, e proprietaria della Rete e delle infrastrutture di cui si avvale la Società per lo svolgimento delle Attività;

Pubblica Amministrazione	indica la Pubblica Amministrazione latamente intesa, avente operatività nazionale (ad es. lo Stato) o territoriale (ad es. Regione, Comune, Provincia), inclusi gli enti pubblici c.d. economici, in regime di diritto privato, così come esponenti di enti privati o soggetti privati che tuttavia esercitano attività regolate;
Reati Presupposto	indica i reati per i quali il Decreto ha introdotto la responsabilità amministrativa dell'Ente. Si tratta, in particolare, delle fattispecie di reato individuate dagli artt. 24 e 25 del Decreto;
Rete	indica la rete <i>internet</i> di Nana Bianca di cui la Società e i propri dipendenti si avvalgono per lo svolgimento delle Attività;
Sede	indica la sede legale della Società, sita a Firenze, Via Ippolito Pindemonte 63, ove la Società svolge la propria Attività presso gli spazi di Nana Bianca s.r.l., le unità locali site a Roncade, Via Sile 41 (TV) e Milano, Via Giosuè Borsi 9;
Sito	indica il sito <i>web</i> www.Dataappeal.com di The Data Appeal Company S.p.A. attraverso cui la Società eroga i propri servizi in modalità <i>web SaaS (Software as a Service)</i> ;
Testo Unico	indica il D. lgs. 9 aprile 2008 n. 81. c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
Data Appeal o la Società TUF	indica The Data Appeal Company S.p.A.; indica il D. lgs. 24 febbraio 1998 n. 58, Testo Unico in materia di intermediazione finanziaria.

PARTE GENERALE

1. INTRODUZIONE

1.1 Il regime di responsabilità amministrativa degli Enti

L'adeguamento della legislazione italiana ad alcune Convenzioni Internazionali ha portato, in esecuzione della legge delega del 29 settembre 2000 n. 300, alla promulgazione del D. lgs. 8 giugno 2001 n. 231, entrato in vigore il 4 luglio 2001, *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”*.

Il Decreto ha introdotto nell'ordinamento italiano il regime della responsabilità amministrativa degli Enti per alcuni reati (indicati dagli artt. 24 e ss. del Decreto, i c.d. Reati Presupposto) commessi, o semplicemente tentati, nell'interesse o a vantaggio degli Enti medesimi, o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, da parte di:

- (i) soggetti che abbiano la rappresentanza, l'amministrazione o la direzione o, anche di fatto, esercitino la gestione o il controllo dell'Ente o di una sua unità organizzata (i soggetti apicali ai sensi dell'art. 5 del Decreto, comma 1, lett. a); o
- (ii) soggetti sottoposti alla direzione o vigilanza dei soggetti di cui alla lettera (i) che precede (i soggetti sottoposti all'altrui direzione ai sensi dell'art. 5 del Decreto, comma 1, lett. b).

La responsabilità amministrativa dell'Ente è diretta e distinta dalla responsabilità dell'autore materiale del reato ed è tesa a sanzionare gli Enti per i reati commessi a loro vantaggio o nel loro interesse.

In virtù della responsabilità introdotta dal Decreto, l'Ente subisce pertanto un autonomo procedimento ed è passibile di sanzioni che possono giungere al punto di bloccare l'ordinaria attività d'impresa.

Infatti, oltre alle sanzioni pecuniarie, l'eventuale confisca e la pubblicazione della sentenza di condanna, il Decreto prevede che l'Ente possa essere sottoposto anche a sanzioni di carattere interdittivo (art. 9, comma 2), quali:

- l'interdizione dall'esercizio dell'attività¹;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni e servizi.

Per espressa previsione normativa (art. 13 comma 2 del Decreto), in generale le sanzioni interdittive hanno una durata non inferiore a 3 mesi e non superiore a 2 anni.

In base a quanto stabilito dall'art. 4, gli Enti con sede principale in Italia possono essere perseguiti anche per reati commessi all'estero, qualora la legislazione del paese straniero non preveda una forma analoga di responsabilità.

La responsabilità amministrativa dell'Ente si fonda su una "*colpa di organizzazione*": l'Ente è ritenuto, cioè, responsabile in via amministrativa del reato commesso dal suo esponente, se ha omesso di darsi un'organizzazione in grado di impedirne efficacemente la realizzazione e, in particolare, se ha omesso di dotarsi di un sistema di controllo interno e di adeguate procedure per lo svolgimento delle attività a maggior rischio di commissione dei reati previsti dal Decreto.

Al contrario, ai sensi dell'art. 5 comma 2 del Decreto, l'Ente non risponde se le persone suindicate hanno agito nell'interesse esclusivo proprio o di terzi.

Alcune delle modalità attraverso cui dotarsi di un simile sistema di organizzazione e controllo interno sono indicate agli artt. 6 e 7 del Decreto, e cioè:

- l'approvazione, adozione, ed efficace attuazione, anteriormente alla commissione di un reato, di un Modello idoneo a prevenire la commissione dei Reati Presupposto previsti dal Decreto. In linea generale, ed in estrema sintesi, il Modello è ritenuto "idoneo" quando i soggetti che hanno posto in essere il reato abbiano agito in modo deliberato e fraudolento al fine di eludere i relativi presidi posti in essere dal Modello stesso;
- la nomina di un Organismo di Vigilanza interno, con poteri autonomi di iniziativa e controllo, deputato (i) al controllo dell'effettivo funzionamento del Modello e del rispetto delle previsioni in esso contenute da parte di tutti i destinatari; (ii) alla costante verifica della reale efficacia preventiva del Modello; e (iii) alla verifica sulla necessità di un suo aggiornamento.

Il Modello, in base alle previsioni del Decreto, con riferimento ai poteri delegati ed al possibile rischio di commissione dei reati deve peraltro:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici controlli 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 dei reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- prevedere canali di comunicazione che consentano la segnalazione di condotte illecite rilevanti ai fini del Modello e che garantiscano la riservatezza dell'identità del segnalante, nonché prevedere il divieto di atti di ritorsione o discriminatori nei confronti di chi effettua tali segnalazioni;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

L'adozione del Modello, pur se non obbligatoria, ma meramente facoltativa, ha efficacia esimente ai fini della responsabilità amministrativa solo se accompagnata dall'efficace e concreta attuazione del Modello stesso e dal suo costante aggiornamento e adeguamento.

Il Tribunale in sede penale, infatti, è chiamato a valutare, nell'ambito del procedimento volto a verificare la responsabilità amministrativa dell'Ente, l'idoneità del Modello a prevenire la commissione di reati, e la sua concreta applicazione ed efficacia.

1.2 Attività di Data Appeal

The Data Appeal Company S.p.A. è una società iscritta nell'apposita sezione sociale del Registro delle Imprese di Treviso e Belluno con la qualifica di pmi innovativa.

La Società ha la propria sede nel Comune di Firenze, in via del Tiratoio 1, dove svolge la propria Attività all'interno delle infrastrutture di Nana Bianca. Con apposito contratto di *coworking* la Società ha infatti ottenuto in uso esclusivo alcuni spazi adibiti ad ufficio di proprietà di Nana Bianca e che la Società destina ai propri dipendenti. Si tratta in particolare di uno spazio costituito da una piccola sala *meeting*, un locale principale *openspace* dove sono situate le postazioni di lavoro e un piccolo ripostiglio. Tali infrastrutture saranno oggetto di trasferimento entro la fine dell'anno in corso presso un nuovo centro, sempre di proprietà di Nana Bianca, sito nel comune di Firenze.

La Società ha altresì istituito due unità locali, una a Roncade, in via Sile 41 (TV) e una a Milano in Via Borsi 9.

La Società ha per oggetto sociale attività prevalentemente orientate allo sviluppo ed alla produzione ed alla commercializzazione di prodotti o servizi ad alto valore tecnologico, consistenti in particolare nell'ideazione, creazione e sviluppo di applicazioni *software* e piattaforme informatiche, di *marketing* e servizi a valore aggiunto per favorire visibilità ed interazione tra strutture e clientela nel settore turistico-ricettivo.

In particolare, la Società raccoglie e rielabora i dati e le informazioni che definiscono il posizionamento digitale e la percezione online di un territorio e delle sue strutture di servizio al pubblico, avendo sviluppato un software di proprietà della Società che rende possibile analizzare un'enorme massa di dati (cd. *big data*) presenti sulla rete *internet* attraverso una serie di algoritmi di Intelligenza Artificiale, elaborati e sviluppati direttamente da Data Appeal, in grado di ricostruire comportamenti, preferenze, soddisfazione degli utenti, trasformandoli in un'analisi che consente di monitorare, in tempo reale, l'*appeal* di una data azienda o di una struttura sugli utenti finali, valutando anche l'impatto di fattori esterni come eventi, condizioni meteorologiche e andamento dei prezzi su immobili, *brand* e destinazioni, consentendo loro di parametrare prezzi ed offerte nei confronti, a loro volta, dei loro consumatori ed utenti finali

Tali dati analizzati attraverso l'algoritmo sono reperibili su *internet*, sia sui siti *web* delle stesse strutture turistiche, sia su quelli, terzi, che si occupano di raccogliere le recensioni e le esperienze dei consumatori e degli utenti finali. Nell'ambito di quest'ultima area, tra i servizi offerti da Data Appeal vi è anche quello di gestire per conto delle strutture le relazioni con i clienti e in particolare le recensioni *online*.

La Società opera quindi come fornitore di servizi, e presta le proprie Attività tanto in favore di enti privati, quanto di enti pubblici (Università, Enti Territoriali, Agenzie, etc.), avvalendosi per lo sviluppo della propria attività anche di consulenti esterni in specifici settori.

Le soluzioni di *business intelligence* sviluppate da Data Appeal si rivolgono comunque prevalentemente a soggetti privati che operano in vari settori, a partire da quelli *hospitality*, *vacation rental*, ad agenzie e consulenti del settore immobiliare, a consulenti di comunicazione e *marketing*, ad operatori della ristorazione e del turismo culturale, a portali di viaggi, *Online Data Agencies*, *tour operator*, destinazioni, così come a *brand* e catene di negozi, a compagnie di trasporti, ad enti e istituti finanziari.

La Società promuove i propri servizi attraverso diversi canali. Anzitutto, Data Appeal promuove la propria attività attraverso il proprio Sito ed eroga il servizio in modalità *web SaaS*, permettendo all'utente di accedere al servizio solo attraverso le credenziali che gli vengono fornite in sede di sottoscrizione di uno specifico abbonamento tra quelli disponibili sul Sito o offerto dal personale commerciale. L'accesso al servizio può inoltre avvenire tramite API o *machine to machine*, per mezzo di credenziali fornite attraverso un dispositivo, cd. token.

La società opera anche come fornitrice di servizi personalizzati, quali report e statistiche, aventi ad oggetto destinazioni, strutture, trend di mercato basati sui dati raccolti tramite la propria piattaforma di ascolto della Rete.

I servizi offerti dal Data Appeal, di cui si può usufruire, sempre attraverso l'accesso all'area riservata del Sito, possono essere acquistati dagli utenti non solo tramite vendita diretta dalla Società, ma anche attraverso *partner* commerciali di Data Appeal. Nell'ambito del servizio sopra descritto Data Appeal fornisce altresì agli utenti un servizio di assistenza e supporto mediante operatore, gestito dagli stessi dipendenti della Società.

Per quanto riguarda invece i rapporti con gli enti pubblici, che rientrano comunque nella clientela della Società, Data Appeal fornisce i servizi sopra descritti su richiesta o su propria candidatura, tramite aggiudicazione a bandi di gara, affidamento diretto e/o affidamento tramite MePA, il nuovo portale online della Pubblica Amministrazione (per la descrizione più analitica dei rapporti con la Pubblica Amministrazione si rinvia alla Parte Speciale ad essi dedicata)

2. MODELLO DI ORGANIZZAZIONE E DI GESTIONE

2.1 Funzione del Modello

Il Modello ha lo scopo di realizzare un sistema strutturato di protocolli e di procedure, unitamente ad una serie di attività di controllo e verifica, idoneo a prevenire, o quanto meno a ridurre, il rischio di commissione dei Reati Presupposto da parte dei Destinatari del Modello.

Il Modello ha, tra l'altro, il fine di:

- ribadire che tutte le forme di comportamento illecito, non solo quelle tali da integrare Reati Presupposto, sono fortemente condannate da Data Appeal in quanto contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui Data Appeal ispira lo svolgimento della propria attività d'impresa;
- permettere a Data Appeal, grazie ad un'azione di individuazione delle aree di attività nel cui ambito possono essere commessi i reati, e all'attuazione delle procedure, di intervenire tempestivamente per prevenire o comunque contrastare la commissione di reati.

Ne consegue che aspetti qualificanti del Modello sono, oltre a quanto sopra evidenziato:

- la sensibilizzazione e la formazione di tutti i Destinatari delle previsioni di comportamento e delle procedure volte a garantire il rispetto del Modello;
- la mappatura delle aree di attività di Data Appeal in relazione alle quali possono essere commessi i Reati Presupposto;
- la dotazione ed attribuzione all'Organismo di Vigilanza di Data Appeal di specifici poteri autonomi di iniziativa e di vigilanza sull'efficacia e sul buon funzionamento del Modello;
- il controllo e la documentazione delle operazioni a rischio;
- il rispetto del principio di separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali dei Destinatari, nonché del funzionamento e dell'aggiornamento del Modello.

2.2 Struttura del Modello

Il Modello è composto da una "Parte Generale" e da più "Parti Speciali", redatte in relazione alle tipologie dei Reati Presupposto per i quali Data Appeal ha ritenuto sussistere un rischio di commissione da parte dei Destinatari in virtù dell'Attività dalla stessa svolta.

Data Appeal è consapevole della circostanza che l'implementazione del Modello si accompagna nella prassi all'adozione anche di un Codice Etico, in cui l'Ente normalmente formalizza i principi cui ispira l'esercizio della propria attività aziendale.

Data Appeal adotterà pertanto, in occasione dell'adozione del Modello, e in linea con la prassi sopra illustrata, anche un proprio Codice Etico, ove sono stati indicati i principi generali cui la Società uniforma la propria azione nei confronti di tutti i soggetti cui entra a vario titolo in contatto nell'esercizio delle proprie Attività.

Il Codice Etico adottato da Data Appeal sarà pubblicato nella parte del Sito della Società accessibile a tutti, in modo che tutti i Destinatari del Modello possano accedervi e prenderne visione. Una copia del Codice Etico e del Modello verrà consegnata a ognuno dei dipendenti, ai quali verrà richiesto di controfirmare apposita dichiarazione di ricevuta. Il Modello è inoltre pubblicato nel Sito della Società, per garantirne l'accesso e la visione a tutti, inclusi gli utenti e i *partner* commerciali.

Data Appeal si impegna inoltre ad organizzare appositi corsi di formazione destinati a tutti i dipendenti in occasione dell'entrata in vigore del Codice Etico e del Modello; analoghi corsi di formazione verranno periodicamente ripetuti con la finalità di ricordare a tutti le regole di condotta e le procedure da rispettare per garantire l'efficace attuazione del Modello; una specifica formazione anche in merito alle prescrizioni del Codice Etico e del Modello verrà indirizzata ai neoassunti in occasione di ogni nuova assunzione.

La Società si impegna inoltre a rendere edotti anche i collaboratori esterni (inclusi quindi i collaboratori anche occasionali, i procuratori d'affari, gli agenti e i fornitori) in relazione ai contenuti del Codice Etico e del Modello, facendosi rilasciare apposita dichiarazione di presa visione.

Il testo originario del Decreto si limitava a individuare, come Reati Presupposto, alcuni delitti contro la Pubblica Amministrazione ed altri contro il patrimonio mediante frode (artt. 24 e 25).

Successivi interventi legislativi hanno ampliato notevolmente il numero dei Reati Presupposto per i quali è configurabile la responsabilità amministrativa dell'Ente, che ricomprende oggi numerose e disparate fattispecie di reato, ed in particolare:

- delitti informatici e trattamento illecito di dati (art. 24 – *bis*);
- delitti di criminalità organizzata (art. 24 – *ter*);
- falsità in monete, in carte di pubblico credito e in valori di bollo (art. 25 - *bis*);
- delitti contro l'industria e il commercio (art. 25 *bis1*);
- reati societari (art. 25 - *ter*);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25 – *quater*);
- pratiche di mutilazione degli organi genitali femminili (art. 25 – *quater1*);
- delitti contro la personalità individuale (art. 25 - *quinquies*);
- abusi di mercato (art. 25 - *sexies*);
- omicidio colposo e lesioni personali gravi e gravissime commessi in violazione delle norme tutela della salute o sicurezza sul lavoro (art. 25 - *septies*);

- ricettazione, riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25 – *octies*);
- delitti in materia di violazione del diritto d'autore (art. 25 - *novies*);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 - *decies*);
- reati ambientali (art. 25 - *undecies*);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 - *duodecies*);
- razzismo e xenofobia (art. 25 – *terdecies*);
- frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 – *quaterdecies*);

Nel corso degli anni infatti, si sono succeduti diversi interventi normativi che hanno progressivamente – anche se non sempre in maniera organica e razionale – ampliato la categoria dei Reati Presupposto.

È noto infatti che attraverso l'inserimento di nuovi articoli (sotto forma di sottonumeri) agli artt. 24 e 25 del Decreto, il legislatore ha progressivamente e costantemente ampliato il novero dei reati per i quali è prevista la responsabilità amministrativa degli Enti, dando spesso attuazione ad esigenze ed indicazioni sorte a livello della normativa comunitaria. Si tratta quindi di una tendenza che non è destinata a scomparire, a meno di un generale intervento di revisione, a livello normativo, del sistema della responsabilità degli Enti di cui si discute da parecchio tempo. È lecito quindi ipotizzare che il numero dei Reati Presupposto sia destinato a conoscere, anche nel breve periodo, ulteriori ampliamenti.

Tra questi, la legge 18 novembre 2019 n.133 di conversione del d.l. 21 settembre 2019 n. 105 ha istituito il perimetro di sicurezza nazionale cibernetica², la cui disciplina è destinata alle amministrazioni pubbliche, agli enti e agli operatori pubblici e privati che abbiano sede nel territorio nazionale e da cui dipenda l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio alla sicurezza nazionale. La determinazione dei soggetti che sono sottoposti alla disciplina così introdotta è demandata ad una serie di decreti attuativi che dovranno essere adottati dal Governo; a loro carico sono inoltre poste tutta una serie di prescrizioni ed obblighi, oltre all'introduzione di un nuovo reato presupposto (art. 24 *bis* del Decreto) che andrà a colpire le condotte (tanto attive quanto omissive) dei soggetti sottoposti alla disciplina qui in esame. Alla data di approvazione del presente Modello, non risulta che la Società rientri tra gli operatori privati soggetti alla nuova disciplina, con la conseguenza che il rischio di commissione del nuovo reato presupposto è inesistente.

² Il perimetro è finalizzato ad assicurare un livello adeguato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio alla sicurezza nazionale.

La Società si impegna comunque a monitorare la situazione e a effettuare nuovamente l'analisi dei rischi in relazione alla commissione del reato in questione.

Si segnala inoltre che la legge 19 dicembre 2019 n.157, di conversione del d.l. 26 ottobre 2019 n. 124 (cd. "Decreto fiscale"), ha introdotto nel Decreto l'art. 25- *quinquiesdecies*, prevedendo una serie di reati presupposto di natura tributaria, consistenti nella dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. 74/2000), la dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. 74/2000), nell'emissione di fatture per operazioni inesistenti (art. 8 D.lgs. 74/2000), nell'occultamento o distruzione di documenti contabili (art. 10 D.lgs. 74/2000) e nella sottrazione fraudolenta al pagamento di imposte (art. 11 D.lgs. 74/2000). Tali disposizioni sono entrate in vigore in data 25 dicembre 2019 (data di pubblicazione nella Gazzetta Ufficiale della legge) e pertanto la Società si impegna ad effettuare l'analisi delle condotte rilevanti ai fini della nuova normativa al fine di individuare eventuali fattori di rischio relativi a tale reato presupposto e adottare, conseguentemente, misure idonee alla prevenzione di commissione di tali reati, adeguando il Modello nei mesi successivi all'adozione dello stesso, permettendo nel frattempo di dare attuazione in via prioritaria al lavoro (già) svolto sinora e alle misure, anche di carattere generale, già previste nel presente documento.

Si rammenta, infine, che la Legge n. 117/2019 pubblicata in G.U. il 18 ottobre 2019 si prefigge di recepire la direttiva UE 2017/1371 (c.d. direttiva PIF), sanzionando le frodi che ledono gli interessi finanziari dell'Unione Europea (cd. frodi IVA) e prevedendo la responsabilità delle persone giuridiche al configurarsi della fattispecie richiamata. Al momento non è ancora stato disciplinato il Reato Presupposto relativo a tale norma, che dovrà essere integrato nel Decreto con misure di prossima adozione.

Pertanto, anche per tali norme, occorre considerare l'eventualità che trovino futura attuazione nei confronti di Data Appeal. Consapevole della necessità di procedere agli adeguamenti del Modello ogni qual volta ciò si renda necessario, e quindi anche (ma non solo) in occasione di nuovi interventi legislativi, Data Appeal provvederà a dare seguito ai necessari interventi di adeguamento, anche su richiesta dell'Organismo di Vigilanza.

2.3 Parte Generale

Secondo quanto stabilito dall'art. 6 comma 3, del Decreto, la Parte Generale del Modello deve mirare a tre fondamentali finalità:

1) Individuazione delle attività aziendali nel cui ambito possano essere commessi i Reati Presupposto: mappatura dei rischi

L'art. 6 comma 2, lett. a) del Decreto richiede anzitutto che il Modello provveda alla cosiddetta mappatura dei rischi: è necessaria, pertanto, l'analisi della complessiva attività svolta da Data Appeal e l'individuazione delle fasi operative o decisionali che comportino il rischio di commissione dei Reati Presupposto.

Dati gli interventi legislativi che hanno portato ad una progressiva estensione dei Reati Presupposto, e dati anche i mutamenti che possono intervenire tanto sulla struttura societaria di Data Appeal, quanto sulle attività dalla stessa svolte, la mappatura dei rischi non potrà mai dirsi definitiva e immodificabile, ma, al contrario, deve essere sottoposta ad una continua attività di controllo e revisione e deve essere allo stesso modo costantemente aggiornata.

Data Appeal e l'Organismo di Vigilanza provvederanno pertanto ad integrare, ove occorra, la mappatura dei rischi ogni qual volta ciò si renda necessario in ragione di ulteriori interventi legislativi, di modifiche dell'assetto societario di Data Appeal, o anche solo in considerazione di modifiche delle circostanze e/o delle modalità con cui Data Appeal svolge la propria attività d'impresa.

II) Articolazione di un sistema di controllo preventivo

Ai sensi dell'art. 6 comma 2 lett. b) del Decreto, una volta compiuta la mappatura dei rischi, occorre prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente nelle individuate aree di rischio.

A tal fine, nelle singole Parti Speciali del presente Modello sono indicate dettagliatamente le specifiche misure e procedure in grado di prevenire o comunque ridurre fortemente il rischio di commissione dei Reati Presupposto.

In aggiunta a tali procedure, che hanno finalità preventiva, è espressamente riconosciuto all'Organismo di Vigilanza il potere/dovere di effettuare verifiche a posteriori su singole operazioni o singoli comportamenti aziendali.

Come la mappatura dei rischi, anche le procedure e i rimedi adottati non potranno mai dirsi definitivi: la loro efficacia e completezza devono, al contrario, essere oggetto di continua rivalutazione da parte dell'Organismo di Vigilanza, che ha anche il compito precipuo di proporre al Consiglio di Amministrazione i miglioramenti, le integrazioni e le modifiche che riterrà di volta in volta necessari.

III) Designazione dell'Organismo di Vigilanza.

Terza finalità della Parte Generale è l'individuazione di un Organismo di Vigilanza che provveda, in base al Decreto:

- al controllo costante del rispetto delle prescrizioni del Modello, nonché delle specifiche disposizioni e delle procedure predisposte in attuazione dello stesso, da parte di tutti i Destinatari;
- all'attività di valutazione costante e continuativa dell'adeguatezza della mappatura dei rischi e delle procedure descritte ai punti I) e II);
- alla proposta al Consiglio di Amministrazione di tutte le modifiche necessarie.

L'Organismo di Vigilanza sarà collegiale, composto da soggetti interni ed esterni a Data Appeal, dotati di specifici requisiti, in modo da garantire autonomia e indipendenza.

La Parte Generale è quindi dedicata all'esame delle modalità con cui Data Appeal ha dato attuazione ai tre passaggi sopra descritti (I, II e III).

2.4 Parti Speciali

Il presente Modello si articola, oltre che della Parte Generale come sopra descritta, anche di una serie Parti Speciali dedicate ciascuna ad una specifica categoria di Reati Presupposto, per i quali, sulla base della mappatura dei rischi effettuata ai sensi del Decreto, Data Appeal ha ritenuto sussistere un rischio di commissione.

Ogni Parte Speciale, oltre alla descrizione delle fattispecie delittuose esaminate, contiene l'individuazione delle aree aziendali ritenute particolarmente a rischio, nonché

l'indicazione precisa delle procedure adottate per evitare o quanto meno ridurre la commissione degli illeciti.

Nelle Parti Speciali che seguono verranno pertanto esaminate le seguenti fattispecie:

- i) reati contro la Pubblica Amministrazione (Parte Speciale "A");
- ii) reati c.d. societari (Parte Speciale "B");
- iii) abusi di mercato (Parte Speciale "C");
- iv) omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche, sulla tutela dell'igiene e della salute sul lavoro (Parte Speciale "D");
- v) riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio (Parte Speciale "E");
- vi) reati informatici (Parte Speciale "F");
- vii) delitti contro il diritto d'autore, l'industria e il commercio (Parte Speciale "G");
- viii) delitti contro l'attività giudiziaria (Parte Speciale "H");
- ix) reati ambientali (Parte Speciale "I");
- x) delitti contro la personalità individuale (Parte Speciale "L");
- xi) reato di impiego di personale irregolare (Parte Speciale "M");
- xii) reati di criminalità organizzata (Parte Speciale "N");
- xiii) reato di corruzione tra privati (Parte Speciale "O");
- xiv) razzismo e xenofobia (Parte Speciale "P");

All'esito della mappatura dei rischi effettuata, Data Appeal ha ritenuto di non ricomprendere nel presente Modello i reati con finalità di terrorismo o di eversione dell'ordine democratico (previsti dall'art. 25 *quater*), nonché quelli relativi alle pratiche di mutilazione degli organi genitali femminili (previsti dall'art. 25 *quater I*), trattandosi di condotte che esulano assolutamente dall'attività aziendale svolta da Data Appeal, e per le quali non è stato ravvisato un rischio, nemmeno ipotetico, di commissione all'interno della Società.

Allo stesso modo e per analoghi motivi, si è deciso di escludere dall'esame del presente Modello i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e di giochi d'azzardo esercitati a mezzo di apparecchi vietati, recentemente introdotti tra i Reati Presupposto, con decorrenza dal 17 maggio 2019, dalla l. 3 maggio 2019 n. 39, che ha introdotto nel Decreto l'art. 25 *quaterdecies*. Trattandosi di fattispecie finalizzate a punire condotte poste in ambito esclusivamente sportivo, l'analisi dei rischi effettuata ha consentito di escludere un rischio di commissione di tali reati all'interno della Società, e nel suo interesse o vantaggio.

Parimenti, non si ritiene applicabile alla Società, per i motivi sopra illustrati ed allo stato attuale, la fattispecie di nuova introduzione di cui al d.l. 105/2019 in materia di sicurezza cibernetica.

2.5 L'attuazione del Decreto da parte di Data Appeal

Alla luce della volontà di operare in modo trasparente e corretto, anche a presidio della propria reputazione aziendale, così come dei propri soci, amministratori, e dipendenti, Data Appeal ha ritenuto opportuno, ed in linea con la propria filosofia aziendale, procedere all'adozione e all'attuazione del presente Modello, ed al suo successivo costante aggiornamento.

Il Modello ha anche il fine di sensibilizzare tutti i Destinatari, in modo da orientare a principi di correttezza e trasparenza il loro operare e, allo stesso tempo, evitare e prevenire ogni rischio di commissione di reati nell'ambito delle attività aziendali.

Il Modello è stato predisposto da Data Appeal avendo come riferimento la propria specifica organizzazione, dimensione e struttura, le prescrizioni e le norme del Decreto, le pronunce giurisprudenziali in materia, le Linee Guida elaborate dalle associazioni di categoria e, in particolare, quelle elaborate da Confindustria (nella versione più recente, pubblicata sul sito di Confindustria nel marzo 2014), nonché i migliori contributi elaborati in materia (tra cui anche le *Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione* elaborate da ANAC, che risultano comunque fonte di spunti utili, seppure elaborate in materia di società e enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e di enti pubblici economici, nonché il documento denominato *Principi consolidati per la redazione dei Modelli organizzativi e l'attività dell'Organismo di Vigilanza e prospettive di revisione del d.lgs. 231/2001*, redatto dal Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili in collaborazione con il Consiglio Nazionale Forense, ABI e Confindustria, pubblicato il 19 febbraio 2019).

Il Modello è stato adottato dal Consiglio di Amministrazione di Data Appeal con delibera del 6 luglio 2020. Con la medesima delibera ha altresì nominato l'Organismo di Vigilanza, composto da tre membri e dotato di autonomi poteri, con compiti di vigilanza, controllo ed iniziativa in relazione al Modello stesso ed in particolare alla sua concreta applicazione, rispetto ed aggiornamento.

2.6 Mappatura dei rischi

Sulla base delle disposizioni del Decreto e delle indicazioni fornite dalle Linee Guida, Data Appeal ha provveduto alla mappatura dei rischi, individuando, all'interno della propria realtà aziendale, le aree che risultano particolarmente a rischio di commissione di alcuno dei Reati Presupposto.

In questa sede, verrà brevemente illustrata la metodologia utilizzata per la mappatura dei rischi.

Data Appeal ha anzitutto proceduto all'analisi degli elementi costitutivi dei Reati Presupposto, allo scopo di individuare e definire le condotte concrete che, all'interno delle attività aziendali, potrebbero realizzare le varie fattispecie delittuose.

In secondo luogo, Data Appeal ha proceduto all'analisi della realtà aziendale, al fine di individuare le aree ed i settori maggiormente a rischio. L'individuazione di tali aree a rischio è stata compiuta sulla base della documentazione e delle procedure già esistenti per ogni attività aziendale.

Infine, Data Appeal ha proceduto alla verifica, all'interno delle aree a rischio così individuate, delle procedure e dei protocolli già esistenti, al fine di verificarne l'adequatezza e l'efficienza in relazione alle disposizioni del Decreto.

Gli esiti delle predette attività di mappatura dei rischi verranno dettagliatamente descritti nelle singole Parti Speciali, dove verranno anche illustrate le procedure e le cautele predisposte da Data Appeal al fine di evitare o comunque di ridurre al minimo il rischio di commissione dei Reati Presupposto.

2.7 Destinatari del Modello

Destinatari delle norme e delle prescrizioni contenute nel presente Modello, e tenuti, quindi, alla sua integrale osservanza, sono, in generale, tutti coloro che operano in nome e per conto di Data Appeal, ivi inclusi gli amministratori, i sindaci, i membri degli altri eventuali organi sociali, i dipendenti, i collaboratori anche occasionali, i partner commerciali, i fornitori, i componenti dell'Organismo di Vigilanza (i Destinatari).

3. ORGANISMO DI VIGILANZA

3.1 Identificazione dell'Organismo di Vigilanza

L'Organismo di Vigilanza di Data Appeal è un organo interno dotato di autonomi poteri di iniziativa e di controllo con il compito di vigilare sul funzionamento e sull'osservanza del Modello e provvedere al relativo aggiornamento.

L'Organismo di Vigilanza di Data Appeal è composto da tre membri, di cui due interni all'organizzazione aziendale e uno esterno alla Società, in qualità di Presidente. I componenti dell'Organismo di Vigilanza, selezionati comunque tra soggetti dotati di comprovata competenza e professionalità, provvederanno ad adottare, nel corso della prima riunione, un apposito regolamento per il funzionamento interno dell'Organismo di Vigilanza. Le riunioni dell'Organismo di Vigilanza dovranno comunque essere oggetto di verbalizzazione, e i relativi verbali conservati in appositi spazi dedicati all'interno dei locali della Società, e accessibili solamente ai componenti dell'Organismo di Vigilanza. Il regolamento interno dell'Organismo di Vigilanza disciplinerà nel dettaglio le modalità di verbalizzazione delle riunioni e di conservazione della relativa documentazione e verbali.

Alla luce delle esperienze maturate nella prassi, e nel rispetto delle disposizioni del Decreto, la Società ha ritenuto di individuare, quali componenti dell'Organismo di Vigilanza, due dipendenti che, dotati delle necessarie competenze e professionalità, unitamente ad una significativa esperienza in materia di policy aziendale, saranno in grado di fornire all'Organismo di Vigilanza il necessario bagaglio di conoscenza della realtà aziendale e del suo funzionamento. A questi si aggiunge, in qualità di Presidente dell'Organismo di Vigilanza, un soggetto esterno alla struttura aziendale di Data Appeal dotato dei requisiti richiesti di professionalità e competenza e che, proprio nella sua qualità di soggetto esterno alla realtà aziendale della Società, tutela l'indipendenza e l'autonomia dell'Organismo di Vigilanza.

Tale soluzione è ritenuta da Data Appeal la scelta ottimale, perché tale da consentire all'Organismo di Vigilanza di operare fin da subito in maniera efficace, in considerazione proprio del fatto che è composto anche da membri che conoscono in maniera approfondita tanto la struttura societaria ed organizzativa della Società, quanto le modalità con cui la stessa svolge la propria Attività.

In particolare, la scelta dei componenti dell'Organismo di Vigilanza consente, a parere di Data Appeal, di garantire il rispetto delle prescrizioni del Decreto, oltre che delle indicazioni delle Linee Guida, in riferimento ai requisiti prescritti per i componenti di tale organismo.

In ragione infatti delle specifiche funzioni attribuite ai componenti interni dell'Organismo di Vigilanza, unitamente alle loro competenze e professionalità, la Società ritiene che la loro nomina, insieme a quella del Presidente, esterno invece alla realtà aziendale, garantisca l'autonomia ed indipendenza dell'Organismo, così come la professionalità dei suoi componenti.

Resta espressamente stabilito che, con riferimento ai componenti interni, la vigenza del loro rapporto di lavoro subordinato o, comunque, di collaborazione con Data Appeal, è presupposto della loro partecipazione quali componenti dell'Organismo di Vigilanza e che pertanto, la cessazione, per qualsivoglia ragione o titolo, di tale rapporto di lavoro o di collaborazione determinerà automaticamente una causa di decadenza dalla carica di componente dell'Organismo di Vigilanza. In tal caso, il Presidente dell'Organismo di Vigilanza dovrà dare atto dell'avvenuta decadenza dalla carica del componente interessato e rivolgersi al Consiglio di Amministrazione, affinché quest'ultimo provveda alla nomina di un nuovo membro.

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione di Data Appeal e resta in carica per la durata indicata all'atto della nomina, o in mancanza di tale termine per tre anni. I suoi membri possono ricoprire la carica per più mandati.

Costituiscono cause di ineleggibilità o di revoca quali componenti dell'Organismo di Vigilanza:

- i) la condanna, anche con sentenza non definitiva o applicazione della pena su richiesta delle parti, per i delitti puniti a titolo di dolo, con l'esclusione quindi dei delitti colposi, eccettuati quelli previsti e puniti dagli articoli 589 e 590 comma 3 c.p., commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sui luoghi di lavoro, nonché le contravvenzioni che comportino l'applicazione di una pena accessoria di cui all'art. 19 c.p., o previste da specifiche disposizioni di legge;
- ii) in ogni caso, qualsiasi condanna, anche non definitiva, che comporti l'applicazione di una pena accessoria di cui all'art. 19 c.p. o previste da specifiche disposizioni di legge;
- iii) l'applicazione di una misura di sicurezza, personale o patrimoniale, l'applicazione di una misura di prevenzione personale o patrimoniale o l'applicazione di una misura di prevenzione antimafia personale o patrimoniale;
- iv) la dichiarazione di interdizione o di inabilità ai sensi del codice civile, come pure il conflitto di interessi con Data Appeal.

Costituisce inoltre causa di sospensione dalla carica, per tutta la durata della misura, l'applicazione di una misura cautelare personale (custodia cautelare in carcere o in luogo di cura, arresti domiciliari, divieto e obbligo di dimora, obbligo di presentarsi alla Polizia Giudiziaria, divieto di espatrio) e l'applicazione di una misura interdittiva (sospensione

dall'esercizio di un pubblico ufficio o servizio, divieto temporaneo di esercitare determinate attività professionali e imprenditoriali).

All'Organismo di Vigilanza ed ai suoi membri si applicheranno le norme del Codice civile in tema di mandato.

3.2 Prerogative e risorse dell'Organismo di Vigilanza

L'Organismo di Vigilanza potrà avvalersi della collaborazione di soggetti appartenenti alle diverse attività aziendali, qualora si rendano necessarie le loro conoscenze e competenze specifiche per particolari analisi, e per la valutazione di specifici passaggi operativi e decisionali dell'attività di Data Appeal.

In ogni caso, l'Organismo di Vigilanza avrà la facoltà, laddove si manifesti la necessità di avvalersi di professionalità non presenti al proprio interno, o comunque nell'organigramma di Data Appeal, di utilizzare la consulenza di professionisti esterni.

L'Organismo di Vigilanza, all'inizio del proprio mandato, e successivamente con cadenza annuale, presenterà al Consiglio di Amministrazione di Data Appeal una richiesta di budget di spesa annuale da erogarsi da parte della stessa Data Appeal ed in particolare:

- l'Organismo di Vigilanza presenterà al Consiglio di Amministrazione la richiesta di erogazione dell'importo corrispondente al budget annuale per il corretto adempimento del mandato;
- Il Consiglio di Amministrazione non potrà ragionevolmente rifiutarsi di provvedere all'erogazione di tale importo, fermo restando che l'Organismo di Vigilanza lo potrà utilizzare, in via autonoma e senza obbligo di preventiva autorizzazione, esclusivamente per gli scopi previsti dal presente Modello;
- tale importo dovrà coprire le spese che, secondo le stime, l'Organismo di Vigilanza dovrà sostenere nell'esercizio delle proprie funzioni (fermo restando che gli eventuali costi relativi alle risorse umane o materiali messi a disposizione da Data Appeal non fanno parte del budget);
- tale importo sarà messo a disposizione dell'Organismo di Vigilanza su un conto corrente bancario intestato a Data Appeal, con firma singola del presidente dell'Organismo di Vigilanza, che ne potrà disporre in via autonoma e senza alcun obbligo di autorizzazione preventiva;
- tale importo sarà erogato in rate trimestrali anticipate con obbligo di rendiconto da parte dell'Organismo di Vigilanza entro i sessanta giorni successivi la scadenza del trimestre, fermo restando comunque l'obbligo di rendiconto annuale alla scadenza di ciascun anno di durata del mandato.

Qualora, in ragione di eventi o circostanze straordinarie (cioè al di fuori dell'ordinario svolgimento dell'attività dell'Organismo di Vigilanza) si rendesse necessaria per l'Organismo di Vigilanza l'erogazione di somme ulteriori rispetto all'importo sopra indicato, il Presidente dell'Organismo di Vigilanza dovrà formulare richiesta motivata al Consiglio di Amministrazione di Data Appeal indicando con ragionevole dettaglio le ragioni ed i fatti posti a base di tale richiesta. La richiesta degli ulteriori fondi non potrà essere respinta dal Consiglio di Amministrazione senza fondato motivo.

3.3 Funzioni e poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza di Data Appeal è affidato il compito di:

- vigilare sull'osservanza delle prescrizioni del Modello e dei documenti ad esso ricollegabili da parte dei Destinatari, assumendo ogni iniziativa necessaria;
- vigilare sulla reale efficacia, efficienza ed effettiva capacità delle prescrizioni del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei Reati Presupposto;
- verificare l'opportunità di aggiornamento ed adeguamento delle procedure disciplinate dal Modello, formulando al Consiglio di Amministrazione le opportune relative proposte;
- segnalare al Consiglio di Amministrazione le violazioni accertate del Modello perché possa assumere i provvedimenti conseguenti.

Fermo restando l'obbligo di vigilanza sul rispetto del Modello e delle procedure ivi indicate attribuito all'Organismo di Vigilanza, il suo operato non è sindacabile da parte del Consiglio di Amministrazione, se non per motivi attinenti ad inadempimenti del mandato conferito.

In particolare, l'Organismo di Vigilanza di Data Appeal realizzerà le predette finalità attraverso:

- le ricognizioni delle attività aziendali, ai fini della mappatura aggiornata delle aree di rischio nell'ambito del contesto aziendale;
- la verifica dell'adeguatezza delle norme in essere in relazione ad eventuali trasformazioni, modifiche ed allargamenti dell'attività aziendale;
- la proposizione al Consiglio di Amministrazione delle opportune modifiche ed integrazioni delle singole Parti Speciali;
- l'aggiornamento conseguentemente delle norme di condotta delle singole Parti Speciali;
- il coordinamento con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree individuate a rischio di commissione dei reati presupposto;
- il controllo dell'effettiva presenza e della regolare tenuta della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di reati;
- la segnalazione al Consiglio di Amministrazione di eventuali carenze del Modello e le relative proposte di modifica o miglioramento. In tal ambito l'Organismo di Vigilanza deve ricevere costantemente informazioni sull'evoluzione delle aree di rischio, e ha libero accesso a tutta la relativa documentazione aziendale. A tal fine dovrà ricevere costantemente, da parte del Consiglio di Amministrazione di Data Appeal, le segnalazioni sulle eventuali situazioni che possano comportare rischi di illeciti;

- il coordinamento con i responsabili delle altre funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello;
- ogni altro controllo, sia periodico che mirato, sul concreto svolgimento di singole operazioni, procedure o attività all'interno di Data Appeal che si renda opportuno;
- la redazione e la verifica della validità delle clausole standard finalizzate all'attuazione di meccanismi sanzionatori (ad es. quelle di risoluzione dei contratti nei riguardi di partner commerciali, collaboratori o fornitori), se si accertino violazioni delle prescrizioni di cui al Decreto;
- per quanto riguarda le comunicazioni sociali e in particolare il bilancio, che nel caso di Data Appeal è certificato da una società di revisione (si veda in proposito la Parte Speciale "B"), la vigilanza costante sulla effettiva indipendenza della società di revisione, nonché le verifiche periodiche sui rapporti con le Autorità di Vigilanza;
- l'Organismo di Vigilanza dovrà predisporre una relazione informativa destinata al Consiglio di Amministrazione, con cadenza annuale.

Infine, e conformemente alle disposizioni di cui all'art. all'art. 6 comma 1 lett. b) del Decreto, i compiti di monitoraggio e di aggiornamento del Modello assegnati all'Organismo di Vigilanza si articolano su tre differenti tipi di verifiche:

- verifiche sugli atti: annualmente l'Organismo di Vigilanza procederà a una verifica dei principali atti societari e dei contratti di maggior rilevanza conclusi da Data Appeal (o dalla relativa società) nell'ambito delle aree di rischio;
- verifiche sulle procedure: periodicamente l'Organismo di Vigilanza verificherà l'effettivo funzionamento del presente Modello;
- verifiche sulle segnalazioni e le misure: annualmente l'Organismo di Vigilanza esaminerà tutte le segnalazioni ricevute nel corso dell'anno, le azioni intraprese in proposito, gli eventi e gli episodi considerati maggiormente rischiosi, nonché l'effettività della conoscenza tra tutti i Destinatari del contenuto del Modello e delle ipotesi di reato per le quali è prevista la responsabilità amministrativa dell'ente.

Dei risultati di questa attività di verifica l'Organismo di Vigilanza dovrà dare conto, seppure sommariamente, nella relazione predisposta con cadenza annuale dall'Organismo di Vigilanza per il Consiglio di Amministrazione.

4. FLUSSI INFORMATIVI INTERNI

4.1 Obblighi informativi nei confronti dell'Organismo di Vigilanza

Oltre alla documentazione espressamente indicata da ogni singola Parte Speciale del Modello secondo le procedure in esse contemplate, dovrà essere portata a conoscenza dell'Organismo di Vigilanza ogni altra informazione attinente all'attuazione del Modello nelle aree di rischio, nonché quella relativa ad eventuali violazioni delle prescrizioni del Modello stesso.

Dovranno sempre essere comunicate all'Organismo di Vigilanza tutte le informazioni riguardanti:

- le decisioni relative alla richiesta, erogazione e utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dipendenti (ivi inclusi i dirigenti) nei confronti dei quali la magistratura proceda per taluno dei Reati Presupposto;
- i provvedimenti e/o le notizie provenienti dalla Magistratura e dagli organi di Polizia Giudiziaria o da qualsiasi altra autorità, dai quali risulti lo svolgimento di indagini, anche nei confronti di ignoti, per fatti in cui siano potenzialmente interessate le attività aziendali di Data Appeal;
- i risultati e le conclusioni di commissioni di inchiesta o altre relazioni interne dalle quali emergano ipotesi di responsabilità per i Reati Presupposto;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello;
- procedimenti disciplinari svolti, eventuali sanzioni irrogate ovvero provvedimenti di archiviazione di tali procedimenti con relative motivazioni;
- rendicontazione mensile degli appalti a seguito di gare pubbliche ovvero di trattative private, tramite elaborazione automatica a mezzo del CRM aziendale;
- rendicontazione mensile delle commesse attribuite da enti pubblici, dalla Comunità Europea o da soggetti che svolgano funzioni di pubblica utilità tramite elaborazione automatica a mezzo del CRM aziendale.

In aggiunta, il Consiglio di Amministrazione è tenuto a dare piena informazione all'Organismo di Vigilanza sulle questioni che rientrano nella competenza dell'Organismo di Vigilanza medesimo.

Al fine di consentire all'Organismo di Vigilanza l'efficace adempimento dei compiti che gli sono demandati, Data Appeal garantisce a tutti i Destinatari del Modello, nonché ad eventuali terzi, la facoltà di segnalare a tale organo qualsiasi illecito, anomalia o attività sospetta, in relazione alla commissione o al rischio di commissione di uno dei Reati Presupposto, di cui siano venuti a conoscenza per qualsivoglia ragione.

Le disposizioni sopra illustrate si completano oggi con le specifiche previsioni della l. 179/2017 (*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*), che è intervenuta per dettare una disciplina *ad hoc* sul fenomeno del c.d. *whistleblowing*, e alle cui indicazioni la Società si è adeguata.

È quindi espressamente previsto, a carico di tutti coloro che svolgono funzioni di rappresentanza, amministrazione o direzione all'interno della Società, nonché a tutti coloro che sono sottoposti alla loro direzione o vigilanza, di segnalare immediatamente all'Organismo di Vigilanza ogni fatto preciso, concordante e circostanziato che integri

una condotta illecita rilevante ai sensi del Decreto e/o una o più violazioni del Modello, di cui siano venuti a conoscenza in ragione delle funzioni svolte all'interno della Società.

La segnalazione di tali, circostanziate, condotte illecite costituisce un obbligo a carico di chiunque ne abbia avuto notizia nello svolgimento della propria attività in Data Appeal. Oltre che un obbligo, sanzionabile con il ricorso alle misure disciplinari previste dal CCNL applicabile, la Società ritiene che la segnalazione di eventuali condotte illegittime debba anche essere intesa anche come un'opportunità di far emergere comportamenti illeciti che andrebbero a penalizzare non soltanto la Società, ma tutti i suoi dipendenti (intesi in senso lato, e quindi anche dirigenti, amministratori, sindaci, consulenti e fornitori).

Le segnalazioni dovranno essere inviate direttamente all'indirizzo e-mail appositamente creato per l'Organismo di Vigilanza e a cui hanno accesso solo i suoi componenti per la durata della carica, che raccoglie comunque anche tutte le ulteriori comunicazioni e flussi informativi previsti dal presente Modello organismodivigilanza@datappeal.io . La Società ha inoltre messo a disposizione dei Destinatari un ulteriore canale di segnalazione tramite la piattaforma di collaborazione aziendale cd. *slack* già in uso presso la Società, che verrà adattata in modo da consentire l'invio e la ricezione di messaggi istantanei diretti all'Organismo di Vigilanza e/o ai suoi singoli componenti, anche se esterni, la cui visione e lettura sarà circoscritta ai soli destinatari del messaggio.

Le segnalazioni possono avvenire, oltre che in forma riservata, anche in forma anonima attraverso i medesimi canali, purché siano sufficientemente circostanziate e in grado di far emergere fatti e situazioni relazionandoli a contesti determinati, al fine di consentire la verifica della segnalazione da parte degli organi e/o dei soggetti competenti.

A tutti coloro che invieranno comunicazioni o segnalazioni all'Organismo di Vigilanza, Data Appeal garantisce espressamente l'esclusione di qualsiasi forma di ritorsione, discriminazione o penalizzazione, ed in ogni caso assicura la riservatezza sull'identità del segnalante.

Tutti i dipendenti di Data Appeal hanno quindi la facoltà, oltre che il dovere, di comunicare, in forma scritta, ogni informazione relativa a possibili anomalie interne od attività illecite di cui abbiano avuto notizia nello svolgimento dei compiti loro assegnati.

L'Organismo di Vigilanza potrà anche ricevere e valutare segnalazioni e comunicazioni provenienti da estranei alla Società.

L'Organismo di Vigilanza potrà richiedere ogni genere di informazione e/o documentazione, utile agli accertamenti e ai controlli ad esso demandati, al Consiglio di Amministrazione ed a tutti i dipendenti, facendo obbligo ai soggetti indicati di ottemperare con la massima cura, completezza e sollecitudine ad ogni richiesta dell'Organismo di Vigilanza.

L'Organismo di Vigilanza di Data Appeal deve ricevere dal Consiglio di Amministrazione informazioni dettagliate circa il sistema di poteri adottato e le deleghe attribuite.

L'Organismo di Vigilanza verifica ed analizza le informazioni e le comunicazioni ricevute e i provvedimenti da attuare. Una volta attuati, i provvedimenti dovranno essere in linea e conformi alle previsioni dettate dal sistema disciplinare del presente Modello.

L'Organismo di Vigilanza può richiedere al CEO e/o alla funzione HR, a seconda di quanto di rispettiva competenza, l'emissione di sanzioni disciplinari a carico di coloro che si sottraggono agli obblighi di informazione.

L'Organismo di Vigilanza comunicherà al Consiglio d'Amministrazione per le proprie determinazioni se, all'esito degli accertamenti svolti sulle comunicazioni e segnalazioni pervenute, le stesse furono redatte con dolo o colpa grave, oppure finalizzate al nocimento della società, dei propri amministratori, dirigenti e dipendenti.

4.2 Obblighi informativi dell'Organismo di Vigilanza nei confronti degli organi societari

L'Organismo di Vigilanza è tenuto a specifici obblighi informativi nei confronti direttamente del Consiglio di Amministrazione.

L'Organismo di Vigilanza ha inoltre l'obbligo specifico di fornire tempestive informazioni su ogni modifica, integrazione o aggiornamento che possa interessare il Decreto. L'Organismo di Vigilanza ha altresì il dovere di comunicare al Consiglio di Amministrazione ogni violazione accertata nell'ambito dello svolgimento della propria attività.

L'Organismo di Vigilanza di Data Appeal potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione o potrà a sua volta richiedere di essere da questo sentito, per riferire in merito al funzionamento del Modello o a situazioni specifiche.

Con cadenza annuale, inoltre, l'Organismo di Vigilanza trasmette al Consiglio di Amministrazione una relazione scritta sull'attuazione del Modello.

4.3 Raccolta e conservazione delle informazioni

Le informazioni e i *report* predisposti o ricevuti in base al Decreto devono essere conservati a cura dell'Organismo di Vigilanza in un archivio apposito, informatico o cartaceo che, previa autorizzazione scritta dello stesso Organismo di Vigilanza, potrà essere reso accessibile a soggetti esterni in base a procedure da delineare a cura dello stesso Organismo di Vigilanza.

5. SISTEMA DISCIPLINARE

5.1 Principi generali

L'art. 6, comma 2 lettera e), del Decreto stabilisce che deve essere introdotto un sistema disciplinare idoneo a sanzionare le violazioni intervenute.

La definizione di un sistema disciplinare (da commisurarsi alla tipologia delle infrazioni) da applicarsi in caso di violazione delle previsioni del Modello, rende efficace l'azione di vigilanza e prevenzione affidata all'Organismo di Vigilanza e ha lo scopo di garantire l'efficacia del Modello stesso.

Il sistema disciplinare è stato redatto anche sulla base dei seguenti principi:

- differenziazione in base ai Destinatari del Modello;
- individuazione delle sanzioni disciplinari da adottarsi nei confronti dei destinatari nel rispetto delle disposizioni previste dai CCNL e delle prescrizioni legislative applicabili;

- individuazione di procedure di accertamento delle violazioni, infrazioni, elusioni, imperfette o parziali applicazioni, nonché di una apposita procedura di irrogazione delle sanzioni applicabili, individuando il soggetto preposto alla loro irrogazione ed in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema disciplinare.

In particolare, il sistema disciplinare è rivolto:

- a tutti coloro che rivestono, anche di fatto, funzioni di rappresentanza, di amministrazione o di direzione (inclusi anche eventuali liquidatori) di Data Appeal o di una sua unità organizzata dotata di autonomia finanziaria e gestionale;
- alle persone sottoposte alla direzione o vigilanza di uno dei soggetti di cui sopra, ed in generale a tutti i dipendenti così come a tutti coloro che, a qualsiasi titolo ed ai vari livelli di responsabilità, operano nell'ambito di Data Appeal concorrendo, con i propri atti, allo svolgimento della complessiva attività aziendale, compresi i collaboratori, i partner commerciali, i fornitori.

Il presente sistema disciplinare è suddiviso in sezioni specifiche ognuna riferita ad una categoria di destinatari, tenuto conto dello *status* giuridico dei diversi soggetti. Il sistema disciplinare è reso pubblico e diffuso mediante affissione nei locali di Data Appeal.

È affidato all'Organismo di Vigilanza il compito di vigilare sull'osservanza e sulla corretta applicazione del sistema disciplinare e sulla sua effettività, nonché di adottare gli opportuni provvedimenti affinché il Consiglio di Amministrazione di data Appeal provveda ad aggiornare, modificare e/o integrare il sistema disciplinare stesso.

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

L'Organismo di Vigilanza potrà proporre al Consiglio di Amministrazione della Società l'adozione di misure disciplinari commisurate all'entità ed alla gravità delle violazioni accertate.

5.2 Sanzioni disciplinari nei confronti dei dipendenti

Le condotte tenute dai lavoratori dipendenti in violazione delle singole regole di comportamento indicate nel presente Modello, costituiranno illeciti disciplinari.

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti rientrano tra quelle previste dal CCNL applicato in azienda, nel rispetto delle procedure previste dall'articolo 7 della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali applicabili.

In particolare, la sanzioni irrogate, a seconda della gravità della violazione, potranno essere quelle previste dal CCNL Commercio, nonché dal CCNL *[da indicare]*.

Le sanzioni saranno irrogate, nel rispetto delle procedure previste dal CCNL applicabile, dal Consiglio di Amministrazione, di propria iniziativa o su proposta dell'Organismo di Vigilanza.

5.3 Misure nei confronti degli amministratori

In caso di violazioni del Modello da parte degli amministratori di Data Appeal, l'Organismo di Vigilanza ne informerà l'intero Consiglio di Amministrazione, che provvederà ad assumere le opportune iniziative previste ai sensi della normativa vigente.

5.4 Misure nei confronti di collaboratori, partner commerciali e fornitori

Ogni comportamento posto in essere da collaboratori, da partner commerciali o da fornitori in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un Reato Presupposto potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di *partnership*, la risoluzione del rapporto contrattuale, fatta salva la richiesta di risarcimento qualora da tale comportamento derivino danni a Data Appeal, come nel caso di applicazione da parte del Giudice delle misure previste dal Decreto.

6. DIFFUSIONE E CONOSCENZA DEL MODELLO

Presupposto perché il Modello possa costituire esimente della responsabilità amministrativa dell'Ente è la sua efficacia, nonché la sua concreta ed effettiva applicazione.

Condizione indispensabile per garantire il concreto e costante rispetto del Modello e delle procedure dallo stesso descritte è la conoscenza dello stesso da parte di tutti i Destinatari.

Data Appeal ha pertanto adottato le iniziative che verranno descritte qui di seguito al fine di assicurare una corretta divulgazione del Modello non soltanto all'interno ma anche all'esterno della propria realtà aziendale.

6.1 Formazione del personale

Data Appeal promuove la conoscenza del Modello tra tutti i Destinatari, che sono pertanto tenuti a conoscerne il contenuto, ad osservarlo e a contribuire alla sua migliore attuazione.

Ai fini dell'attuazione del Modello la formazione del personale (a cui vanno aggiunti anche i consulenti esterni) sarà articolata secondo le seguenti modalità:

- Formazione iniziale attraverso riunioni specifiche nel periodo immediatamente successivo all'approvazione del Modello;
- Diffusione di una nota informativa interna esplicativa del Modello e delle sue funzioni;
- Pubblicazione sul sito internet di Data Appeal del Modello;
- Diffusione tramite circolare interna di materiale informativo dedicato all'argomento, con comunicazione costante e tempestiva di eventuali aggiornamenti e modifiche;
- Informativa in sede di assunzione.

6.2 Informazione dei collaboratori, dei partner commerciali e dei fornitori

Data Appeal promuove la conoscenza e l'osservanza del Modello anche tra i partner commerciali, i collaboratori ed i fornitori, attraverso la pubblicazione del presente Modello sul proprio sito internet. I partner commerciali, i collaboratori ed i fornitori dovranno sottoscrivere una dichiarazione di ricevuta del Modello, che verrà poi conservata dalla Società presso il proprio archivio.

L'informativa nei confronti di collaboratori, partner commerciali e fornitori riguarda anche eventuali aggiornamenti del Modello che si siano resi necessari a fronte di novità legislative – che comportino un allargamento della categoria dei Reati Presupposto – ovvero di mutamenti della struttura e/o dell'organizzazione aziendale che richiedano una revisione del Modello stesso. In ogni caso di revisione del Modello, pertanto, Data Appeal si occuperà di darne debita informazione ai soggetti terzi.

6.3 Clausole contrattuali

Al fine di assicurare il rispetto delle prescrizioni e delle procedure di cui al presente Modello anche da parte di soggetti terzi che partecipano, anche in via indiretta, all'esercizio dell'attività di impresa di Data Appeal, la Società inserirà nei contratti e nelle lettere di incarico sottoscritti con partner commerciali, fornitori e collaboratori apposite clausole contrattuali attraverso le quali i sottoscrittori si impegneranno al rispetto delle norme del Modello, accettando altresì che la loro violazione possa costituire motivo di risoluzione del relativo contratto da parte di Data Appeal.

La Società ritiene infatti che tale rimedio contrattuale costituisca l'unico strumento che consenta di tutelare il rispetto delle procedure e dei principi elaborati dal Modello anche da parte di soggetti (quali i collaboratori, i partner commerciali ed i collaboratori) che, non sono esposti al rischio delle sanzioni disciplinari previste espressamente per i dipendenti.

PARTE SPECIALE “A”

Rapporti con la Pubblica Amministrazione

1. LA TIPOLOGIA DEI REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 DEL DECRETO)

Si riporta qui di seguito una descrizione dei Reati Presupposto relativi ai rapporti con la Pubblica Amministrazione, indicati negli artt. 24 e 25 del Decreto, quest’ultimo oggetto di significative apportate nel mese di gennaio 2019.

Le due fattispecie disciplinano reati che, seppure previsti da due distinti articoli del Decreto, hanno come comune denominatore quello di presupporre l’instaurazione di rapporti con soggetti pubblici e/o esercenti una pubblica funzione o un pubblico servizio. Vengono quindi trattati congiuntamente nella presente Parte Speciale.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
316 <i>bis</i> c.p.	Malversazione a danno dello Stato	fino a 500 quote. Aumentata da 200 a 600 quote se l’ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità	sì: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
316 <i>ter</i> c.p.	Indebita percezione di erogazioni a danno dello Stato	fino a 500 quote. Aumentata da 200 a 600 quote se l’ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità	sì: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
640 comma 2 n. 1 c.p.	Truffa a danno dello Stato o di altro ente pubblico	fino a 500 quote. Aumentata da 200 a 600 quote se l’ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità	sì: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di

			pubblicizzare beni o servizi
640 <i>bis</i> c.p.	Truffa aggravata per il conseguimento di erogazioni pubbliche	fino a 500 quote. Aumentata da 200 a 600 quote se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità	si: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
640 <i>ter</i> c.p.	Frode informatica commessa in danno dello Stato o di altro ente pubblico	fino a 500 quote. Aumentata da 200 a 600 quote se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità	si: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
318 c.p.	Corruzione per l'esercizio della funzione	fino a 200 quote	No
322 commi 1 e 3 c.p.	Istigazione alla corruzione (quando la promessa sia fatta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio per l'esercizio delle loro funzioni o dei loro poteri)	fino a 200 quote	No
346 <i>bis</i> c.p.	Traffico di influenze illecite	fino a 200 quote	No
319 c.p.	Corruzione per un atto contrario ai doveri d'ufficio	da 200 a 600 quote	sì: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*
319 <i>ter</i> comma 1 c.p.	Corruzione in atti giudiziari per favorire o danneggiare una parte in un processo civile, penale o amministrativo	da 200 a 600 quote	si: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il

			reato è commesso da un sottoposto*
322 commi 2 e 4 c.p.	Istigazione alla corruzione (quando la promessa sia fatta ad un pubblico ufficiale o ad un incaricato di un pubblico servizio per indurre ad omettere o ritardare un atto dell'ufficio, ovvero a fare un atto contrario ai doveri)	da 200 a 600 quote	si: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*
317 c.p.	Concussione	da 300 a 800 quote	si: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo

			non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*
319 aggravato ai sensi dell'art. 319 <i>bis</i> c.p., quando l'ente ha conseguito un profitto di rilevante entità	Corruzione per un atto contrario ai doveri d'ufficio, quando ha ad oggetto il conferimento di pubblici impieghi o stipendi o pensioni, ovvero la stipulazione di contratti nei quali sia interessata la Pubblica Amministrazione alla quale il pubblico ufficiale appartiene, o, ancora, il pagamento o il rimborso di tributi	da 300 a 800 quote	si: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*
319 <i>ter</i> comma 2 c.p.	Corruzione in atti giudiziari, quando dal fatto deriva l'ingiusta condanna	da 300 a 800 quote	si: 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 di agevolazioni,

			finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*
319 <i>quater</i> c.p.	Induzione indebita a dare o promettere utilità	da 300 a 800 quote	sì: 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 di agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. Per un periodo non inferiore a 4 anni e non superiore a 7, se il reato è commesso da un apicale; per un periodo non inferiore a 2 anni e non superiore a 4, se il reato è commesso da un sottoposto*

* In tutti questi casi, se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi, le sanzioni interdittive hanno una durata non inferiore a 3 mesi e non superiore a 2 anni (art. 25 comma 5 *bis* del Decreto).

Per tutti i reati, inoltre, le sanzioni pecuniarie si applicano all'ente anche quando i delitti sono stati commessi da una persona incaricata di un pubblico servizio, ovvero membri delle Corti Internazionali o degli organi della Comunità Europea o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità Europee e di Stati esteri.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

Malversazione a danno dello Stato (art. 316 bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato per la realizzazione di opere o per lo svolgimento di attività di pubblico interesse, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta).

La norma punisce, quindi, l'uso distorto di finanziamenti o contributi legittimamente conseguiti.

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che successivamente non siano stati destinati alle finalità per cui erano stati erogati.

Indebita percezione di erogazioni in danno dello Stato (art. 316 ter c.p.)

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute - si ottengano per sé o per altri, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato o da altri enti pubblici.

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316 bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Inoltre, a differenza della fattispecie prevista al punto precedente – che costituisce un reato c.d. “proprio”, in quanto può essere commesso solo da un soggetto, estraneo alla P.A., legittimo percettore di fondi pubblici – il reato di indebita percezione di erogazioni in danno dello Stato o di altri enti pubblici è reato “comune” e può, pertanto, essere commesso da chiunque.

Le condotte punibili consistono:

- i. nella presentazione di dichiarazioni o documenti falsi o attestanti cose non vere;
- ii. nell'utilizzo di dette dichiarazioni o di detti documenti;
- iii. nell'omissione di informazioni dovute.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato (prevista dall'art. 640 bis c.c. e che sarà di seguito descritta), nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Truffa in danno dello Stato o di altro Ente Pubblico (art. 640, comma 2, n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico), determinandolo a fornire una specifica prestazione patrimoniale.

Tale reato può realizzarsi, ad esempio, nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta), al fine di ottenere l'aggiudicazione della gara stessa.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Ciò che caratterizza la fattispecie in esame rispetto a quella descritta al punto precedente (art. 640, comma 2, n.1 c.p.) è l'oggetto del reato: nel caso previsto dall'art. 640 bis c.p., infatti, questo è costituito esclusivamente dalle erogazioni pubbliche.

Frode informatica in danno dello Stato o di altro Ente Pubblico (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o intervenendo, senza diritto e con qualsiasi modalità, su dati, informazioni o programmi in esso contenuti, si ottenga un ingiusto profitto da parte dello Stato o di altro ente pubblico, arrecando danno a terzi.

Il concetto di "alterazione" comprende qualsiasi azione sulla componente logica del computer (il *software*) ovvero sulle parti meccaniche di questo (l'*hardware*) che incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei dati.

Il concetto di "intervento" comprende qualsiasi azione che determini modifiche ai regolari processi del computer.

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

Concussione (art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di pubblico servizio, abusando della propria posizione, costringa taluno a dare o a promettere indebitamente a sé o ad altri denaro o altre utilità non dovute.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del Decreto stesso, nell'ipotesi in cui un dipendente o un agente di una società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la società).³

³ **Note sulla nozione di pubblico ufficiale e di incaricato di pubblico servizio**

Buona parte delle fattispecie elencate negli artt. 24 e 25 D. Lgs. 231/01 sono configurabili come reati "propri", in quanto possono essere integrati solo in rapporti in cui almeno uno dei due soggetti sia dotato della qualifica di pubblico ufficiale o di incaricato di pubblico servizio.

Agli effetti della legge penale (art. 357 c.p.), è pubblico ufficiale chi esercita una pubblica funzione legislativa, amministrativa o giudiziaria, formando o concorrendo a formare la volontà sovrana dello Stato o di altro Ente pubblico presso il quale è chiamato ad esplicare mansioni autoritarie (deliberanti, consultive o esecutive). Deve invece considerarsi incaricato di pubblico servizio (art. 358 c.p.) chi, pur agendo nell'ambito di un'attività disciplinata nelle stesse forme della pubblica funzione, manca dei poteri tipici di quest'ultima, purché non svolga semplici mansioni di ordine né presti opera meramente materiale.

Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318-319 c.p.)

L'ipotesi prevista dall'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altra utilità, ovvero ne accetti la promessa, per l'esercizio delle sue funzioni o dei suoi poteri (determinando un vantaggio in favore dell'offerente).

Condotta simile è quella punita dall'art. 319 c.p.: in questo caso il pubblico ufficiale riceve, per sé o per un terzo, denaro o altra utilità, ovvero ne accetta la promessa, al fine di omettere o ritardare, oppure per avere omesso o ritardato un atto del suo ufficio, ovvero per avere compiuto un atto contrario ai doveri di ufficio.

Il reato potrà configurarsi, ai sensi del Decreto, laddove vi sia un flusso illecito di denaro (o altre utilità) tra esponenti aziendali e un soggetto pubblico, nell'esercizio delle sue funzioni o dei suoi poteri, senza la necessità che sia dimostrato un nesso causale tra la prestazione (o l'utilità erogata) e un singolo e specifico provvedimento o atto della Pubblica Amministrazione.

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

Il reato è aggravato (ai sensi dell'art. 319 *bis* c.p.) quando il fatto di corruzione abbia ad oggetto il conferimento di pubblici impieghi o stipendi o pensioni, ovvero la stipulazione di contratti nei quali sia interessata la pubblica amministrazione alla quale il pubblico ufficiale appartiene o il pagamento o il rimborso di tributi.

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

La fattispecie trova applicazione quando le condotte descritte negli articoli 318 e 319 c.p. sono realizzate per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

È opportuno precisare che la fattispecie in esame è destinata a trovare applicazione anche a prescindere dall'esercizio delle funzioni giudiziarie da parte del soggetto attivo del reato. Infatti, come precisato dalla Corte di Cassazione, costituisce "atto giudiziario" anche ogni atto funzionale ad un procedimento giudiziario, a prescindere quindi dalla qualifica soggettiva di chi lo ponga in essere.

Con i concetti di "favore" e "danno" la norma si riferisce non soltanto all'esito finale di un procedimento, ma anche a tutti gli altri provvedimenti che possono essere adottati nel corso di questo.

Inoltre, per la sussistenza del reato non occorre che il favore o il danno perseguiti siano ingiusti.

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

La norma ha un'applicazione residuale, nel senso che si applica solo ove il fatto commesso non costituisca un reato più grave, e riguarda l'ipotesi del pubblico ufficiale o dell'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altre utilità.

La norma, a differenza delle altre qui in esame, punisce anche la condotta del privato, che diventa qui soggetto attivo del reato, promettendo denaro o altra utilità, seppure con pene minori.

La fattispecie, introdotta nel 2015, si differenzia dalla concussione, in cui il pubblico ufficiale, attraverso la violenza o la minaccia di un male ingiusto, costringe il privato a dare o promettere denaro

Al riguardo, la giurisprudenza ormai consolidata ha precisato che, ai fini della individuazione della qualità di pubblico ufficiale o di incaricato di pubblico servizio, occorre verificare se la relativa attività sia disciplinata da norme di diritto pubblico e sia volta in concreto al perseguimento di interessi collettivi, restando irrilevanti la qualificazione e l'assetto formale dell'Ente per il quale il soggetto presta la propria opera.

In altri termini, la qualifica di pubblico ufficiale o di incaricato di pubblico servizio può attribuirsi non solo ad esponenti di Enti pubblici in senso stretto, ma anche a quelli di Enti regolati dal diritto privato che, in concreto, svolgono attività o prestano servizi nell'interesse della collettività.

o altre utilità per evitare il male prospettato, seppure senza che questi ne percepisca alcun vantaggio. Nell'induzione indebita, invece, la soggezione psicologica del privato è più tenue: il privato finisce per accettare la richiesta della prestazione indebita, nella prospettiva di conseguire un tornaconto personale.

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

La norma stabilisce l'applicazione delle pene previste per i reati di cui agli artt. 318 comma 1, 319, 319 *bis*, 319 *ter* e 320 c.p. anche per il soggetto corruttore.

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione del pubblico ufficiale o dell'incaricato di pubblico servizio per l'esercizio delle sue funzioni o dei suoi poteri, questo rifiuti l'offerta illecitamente avanzatagli.

Traffico di influenze illecite (art. 346 bis c.p.)

La norma ha applicazione residuale, trovando il proprio ambito operativo fuori dai casi di concorso nei reati di cui agli artt. 318, 319, 319-*ter* e nei reati di corruzione di cui all'art. 322 *bis* c.p., e riguarda l'ipotesi in cui vengano sfruttate o vantate relazioni esistenti o asserite con un pubblico ufficiale, un incaricato di un pubblico servizio ovvero uno degli altri soggetti di cui all'art. 322 c.p. per farsi dare o promettere, per sé o per altri, denaro o altra utilità come prezzo della propria mediazione illecita ovvero a titolo di remunerazione per l'esercizio di funzioni e poteri da parte del soggetto corrotto.

I reati considerati, come detto, trovano come loro presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato e tale da ricomprendere anche la Pubblica Amministrazione di Stati esteri, delle Istituzioni Europee e/o delle Corti internazionali⁴, così come esponenti di enti privati o soggetti privati che tuttavia esercitano attività regolate da norme di diritto pubblico e, in generale, di pubblico interesse, visto il rinvio, dell'art. 25 del Decreto, anche all'art. 322 *bis* c.p., intitolato "*Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati Esteri*").

⁴ Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitano funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitano funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale (2);

5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali (3);

5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali (4).

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali (6).

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitano funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi.

2. VALUTAZIONE DELLE AREE DI RISCHIO

Il rischio di commissione di delitti contro la Pubblica Amministrazione è immanente in ogni attività di impresa: qualsiasi società infatti si trova, nel corso della propria ordinaria attività, ad interfacciarsi in più di un'occasione con i più disparati enti pubblici e per le più disparate ragioni (ciò avviene anche solo per la costituzione della società, con riferimento agli adempimenti formali di iscrizione e di pubblicità richiesti).

Il rischio di illeciti nei confronti della Pubblica Amministrazione è poi sempre particolarmente alto a causa della loro specifica conformazione: essi si fondano su un rapporto intersoggettivo, tra privato e pubblico ufficiale (la corruzione ne è l'esempio per eccellenza). In questa situazione, anche comportamenti e rapporti in realtà non finalizzati alla commissione di illeciti, ma caratterizzati da semplice ambiguità (si pensi a rapporti con un amministratore locale di eccessiva vicinanza, confidenzialità ed informalità) possono ingenerare sospetti, determinare l'apertura di indagini, essere insomma travisati, sia dal pubblico ufficiale coinvolto, sia da osservatori esterni.

Altro elemento di delicatezza è costituito dal fatto che la giurisprudenza tende ad accogliere nozioni molto ampie di pubblico ufficiale e di incaricato di pubblico servizio (ossia delle qualifiche soggettive che portano alla configurazione degli illeciti in parola) con la conseguenza che anche figure appartenenti a persone giuridiche ed enti formalmente privati, in ragione dello svolgimento di attività in senso lato di pubblica rilevanza possono essere ritenuti titolari della qualifica ai fini dell'applicazione della legge penale.

Ciò detto in via generale, si deve aggiungere che, per Data Appeal, la valutazione della specificità delle Attività e l'analisi dei relativi rischi ha portato a ritenere che il rischio specifico per i reati qui in esame debba debitamente essere preso in considerazione.

Data Appeal, infatti, intrattiene numerosi rapporti con la Pubblica Amministrazione, intesa in senso lato, che rientra tra i "clienti" cui la Società vende i propri servizi.

Rientrano infatti nella clientela di Data Appeal anche soggetti di diritto pubblico, quali Enti Territoriali (Comuni, Province, Regioni), Enti museali e culturali, Camere di commercio, apparati statali (Ministeri), istituti del turismo, università pubbliche, i quali sono – al pari di quelli privati - interessati ad ottenere informazioni sui trend rilevanti associati al turismo e alla frequentazione di specifici territori per valorizzare al meglio la propria reputazione, recettività, partecipazione ad un evento, ecc.

Le specifiche forme di collaborazione tra la Società e la Pubblica Amministrazione come sopra descritta si realizzano attraverso diverse modalità: partecipazione a bandi di gara e conseguente aggiudicazione del progetto e sottoscrizione del relativo contratto, affidamenti diretti di incarico laddove consentito dalla normativa applicabile, affidamenti tramite MePA (Mercato elettronico a disposizione delle amministrazioni pubbliche italiane per effettuare acquisti di importo inferiore alla soglia comunitaria, *i.e.* 135 mila euro per le Pubbliche Amministrazioni centrali e 209 mila euro per le amministrazioni locali).

Si deve precisare che – a prescindere dalla modalità di instaurazione/conclusione del rapporto contrattuale utilizzata - le condizioni, i costi e le modalità di erogazione della prestazione da parte di Data Appeal non sono mai autonomamente determinati dalla Società, ma sono prefissati dalla Pubblica Amministrazione in via preventiva, o comunque vincolati alle condizioni economiche prefissate nei bandi. Talvolta, infatti, la Pubblica Amministrazione definisce già il corrispettivo da corrispondere all'aggiudicatario del servizio, talvolta determina una base d'asta, comprensiva di determinati servizi, a partire da cui la Società potrà partire per presentare la propria offerta economica.

Stante quindi la presenza di specifici rischi nell'ambito dell'Attività, Data Appeal sottolinea che le regole fondamentali, in ogni caso in cui un esponente della Società si interfacci con la Pubblica Amministrazione devono essere le seguenti:

- qualsiasi rapporto con la Pubblica Amministrazione, con le persone fisiche che le rappresentano e con soggetti che in senso lato svolgono funzioni ed hanno attinenza con attività di pubblico interesse, deve essere considerato come attività per definizione pericolosa;
- di tutti i passaggi e di tutte le negoziazioni con la Pubblica Amministrazione deve essere conservata evidenza, in modo che gli stessi siano sempre tracciabili e rintracciabili.

La Società, tenuto conto della frequenza e delle modalità con cui si interfaccia con la Pubblica Amministrazione, ha deciso di adottare al proprio interno una specifica procedura, con la finalità di disciplinare le modalità di gestione, a livello interno, di qualsiasi rapporto con la Pubblica Amministrazione, a partire dai primi contatti (siano essi sollecitati direttamente dalla Pubblica Amministrazione, oppure da parte della Società), attraverso la partecipazione alla gara/bando, ove previsto, la successiva sottoscrizione del contratto, la fornitura del servizio e/o della prestazione concordata, e, non ultimo, la rendicontazione.

La procedura è denominata, evidentemente, "*Rapporti con la Pubblica Amministrazione*".

Come in ogni altro ambito dell'attività di impresa, nei rapporti con la Pubblica Amministrazione il riferimento alle procedure interne ed alle norme di comportamento richiamati nella presente Parte Speciale deve essere indefettibile ed il loro rispetto deve essere quanto mai rigoroso.

3. INDIVIDUAZIONE DELLE ATTIVITÀ A RISCHIO

I reati considerati, come detto, trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione (intesa in senso lato).

Sono pertanto da considerarsi a rischio tutte quelle attività aziendali che implicano l'instaurazione di un rapporto con la Pubblica Amministrazione (attività di rischio diretto).

Sono poi da considerarsi allo stesso modo a rischio le aree aziendali che, pur non implicando direttamente l'instaurazione di rapporti con la Pubblica Amministrazione, gestiscono strumenti di tipo finanziario e di pagamento e altre attività che potrebbero consentire di attribuire vantaggi e utilità a pubblici ufficiali (o a soggetti ad essi collegati) nella commissione di reati contro la Pubblica Amministrazione (attività di rischio indiretto).

Costituiscono, in particolare, aree di rischio indiretto:

con riferimento alla possibilità che esse possano essere impiegate per la formazione di riserve occulte di danaro o da impiegare in ipotesi per illecite dazioni o per dissimulare simili illecite dazioni:

- le attività di amministrazione, finanza, contabilità e fiscale,
- le attività di pagamento,

con riferimento all'ipotesi che i soggetti selezionati possano essere ricollegabili ad amministratori e pubblici ufficiali locali che quindi l'attribuzione dell'incarico possa essere la contropartita di un patto corruttivo o comunque di un illecito vantaggio:

- la promozione della Società a eventi come fiere, convegni, attività di formazione;
- l'assegnazione di contratti di consulenza e prestazione professionale, in particolare quando il soggetto selezionato abbia sede, operi abitualmente e sia localmente radicato nell'area in cui Data Appeal stia in quel momento operando;

- la selezione del personale;
- la nomina di dirigenti e di membri degli organi sociali.

4. PRINCIPI DI COMPORTAMENTO NELLA GESTIONE DELLE ATTIVITÀ DI RISCHIO DIRETTO

La presente Parte Speciale prevede l'espresso divieto - a carico di tutti i Destinatari - di:

- porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o comunque presentarsi in modo non cristallino ed essere oggetto di fraintendimento;
- porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato.

Nell'ambito di ogni rapporto con la Pubblica Amministrazione è fatto divieto in particolare di:

- effettuare elargizioni in denaro a pubblici funzionari;
- distribuire omaggi e regali al di fuori di quanto previsto dalla prassi e dalla specifica procedura aziendale adottata dalla Società. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte), o tesi a promuovere l'Attività attraverso *gadgets* e prodotti approvati da Data Appeal. I regali offerti – salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte verifiche;
- accordare altri vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione, ovvero loro familiari e/o persone legate da rapporti di amicizia con loro o da loro segnalate, che siano finalizzate ad influire sull'esito di una transazione commerciale;
- effettuare prestazioni in favore dei *partner* commerciali che non trovino adeguata giustificazione nel contesto del rapporto associativo costituito con i *partner* stessi;
- riconoscere compensi in favore dei collaboratori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
- presentare dichiarazioni non veritiere o incomplete o parziali a organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o qualsiasi altro risultato;
- omettere di predisporre e conservare in maniera accurata e conformemente alle disposizioni di legge le scritture contabili;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

La gestione di ogni rapporto con la Pubblica Amministrazione deve essere improntata ai seguenti principi fondamentali:

- soggettivizzazione dell'attività: è opportuno che tendenzialmente sia sempre individuato un responsabile dell'attività in questione, che ne segua lo svolgimento e prenda le relative decisioni;
- soggettivizzazione del rapporto: è opportuno che tendenzialmente sia solo il responsabile individuato ad interfacciarsi con il pubblico ufficiale. Certamente, devono essere esclusi rapporti soggettivamente indeterminati;
- formalità: è opportuno seguire sempre le procedure formali previste dalle norme del procedimento amministrativo ed evitare quanto più possibile rapporti informali, men che meno confidenziali con esponenti di pubbliche amministrazioni;
- tracciabilità: è buona norma lasciare tracce scritte delle principali fasi e dei contatti nel corso di un procedimento amministrativo;
- evidenza delle eccezioni: è opportuno lasciare sempre traccia scritta delle eccezioni che, per ragioni di estrema urgenza, siano operate rispetto alle procedure, con indicazione dei motivi;
- partecipazione: è opportuno organizzare le attività che comportino rischi in modo da far sì che le principali decisioni e gli atti a rilevanza esterna ad esse relative avvengano e siano perfezionati con il contributo di almeno due soggetti aziendali, per favorire il controllo reciproco ed impedire abusi.

In particolare, la Società ha ritenuto di fondamentale importanza l'adozione di processi che regolano i passaggi decisionali, il sistema dei controlli e i flussi informativi relativi alle Attività svolte in contatto con la Pubblica Amministrazione sia per quanto attiene (A) alla fase prodromica, e per così dire, di *lead*, in cui la società viene a conoscenza della possibilità della commessa o viene contattata a tal fine, sia (B) alla fase di partecipazione all'offerta e quindi di relativa predisposizione della documentazione necessaria e richiesta dalla Pubblica Amministrazione, sia (C) alla fase successiva di gestione del progetto, nel caso di esito positivo della selezione, in relazione sia all'effettiva erogazione del servizio/prestazione commissionato, sia alla rendicontazione finale.

Il rispetto di tali processi è dunque fondamentale per tutti i soggetti coinvolti al fine di garantire la tracciabilità degli scambi che intercorrono con la Pubblica Amministrazione, tanto a livello informativo (dati, documenti, informazioni), quanto a livello contabile e finanziario (pagamenti o altro) nelle varie fasi di contatto.

In riferimento alla fase **A)**, si evidenzia in particolare che la Società è impegnata in una costante opera di promozione della propria Attività, che comporta la partecipazione ad eventi fieristici, presentazioni, focus group o altre iniziative ideate allo scopo di mettere in contatto domanda e richiesta nello specifico settore di attività di Data Appeal.

L'area commerciale della Società segnala tempestivamente nel CRM (*Customer Relationship Management*, sistema di gestione dei clienti) aziendale il contatto interessato, sia esso inbound o outbound, tracciando il *lead*, comprensivo della sorgente di provenienza, nello stesso sistema, per iniziare le attività di identificazione del potenziale interesse. Tutte le attività di contatto, e in particolare tutti gli scambi e-mail, vengono registrati nel CRM e associati alla persona/*lead* con cui avviene l'interlocazione.

In caso di concreto interesse commerciale, la *business function* di riferimento, e cioè, quasi sempre, la funzione Vendite, procede a generare a sistema interno una "opportunity", associata all'Ente potenzialmente interessato a generare la fornitura e alle persone di riferimento.

In tale “opportunity” la *business function* di riferimento inserisce fin dalla prima fase la tipologia di servizio/prodotto di interesse, la data di chiusura prevista della fornitura, il valore complessivo previsto per la fornitura. Ogni “opportunity” deve essere collegata anche all’ente che ne è finanziariamente responsabile. Tutti i dati e i cambiamenti apportati nel tempo ai valori citati sono registrati a sistema e quindi sempre soggetti a verifica e controllo.

La successiva fase **B)** è strettamente connessa alle modalità di assegnazione degli incarichi, che, come sopra già evidenziato, avviene a discrezione della Pubblica Amministrazione committente e a seconda delle procedure che ogni Pubblica Amministrazione è tenuta a seguire. Le principali modalità sono:

- a. Affidamento diretto e/o procedura negoziata ai sensi dell’Art. 30 del D.lgs. 50/2016 (cd. Codice degli appalti)
- b. Gara
- c. MePA

(Si tratta, in particolare, di una piattaforma digitale, gestita da Consip, ove vengono riportati cataloghi di servizi/prodotti offerti da fornitori abilitati per importi inferiori alla soglia comunitaria prevista di 207.000 euro ed ordinabili dalla Pubblica Amministrazione... In primis, Consip si occupa di pubblicare i bandi del Mercato elettronico, successivamente i fornitori devono abilitarsi secondo i requisiti richiesti e pubblicano le loro offerte inerenti i bandi. Pertanto, le Pubbliche Amministrazioni interessate ad uno o più servizi possono verificare i servizi disponibili tramite la vetrina del Mercato elettronico o il Catalogo prodotti, e procedere ad effettuare ordini di acquisto, richiedere offerte o negoziare).

Data Appeal ha accesso alla piattaforma e vi conserva il catalogo dei servizi offerti dalla Società, che viene aggiornato periodicamente, ad opera dal Responsabile Vendite Italia e dal *Chief Financial Officer*, il quale ultimo effettua l’ultima revisione prima del caricamento del documento digitale sulla piattaforma.

Operativamente, è possibile accedere alle negoziazioni dalla vetrina dei bandi pubblicati sul MePA cliccando su “Partecipa all’iniziativa.” Ogni sei mesi è necessario aggiornare le dichiarazioni rilasciate, pena l’impossibilità di partecipare alle offerte. Sono ammessi a richiedere l’abilitazione al MePA tutti gli operatori economici che possono partecipare alle procedure di affidamento dei contratti pubblici, come previsto dal Decreto legislativo 50/2016 e dalla normativa comunitaria in materia.

Per avviare la procedura di abilitazione e quindi navigare nel MePA, l’Ente deve quindi registrarsi al portale attraverso proprie credenziali e poi procedere alla partecipazione all’iniziativa, una volta individuata.

Pertanto, la Pubblica Amministrazione interessata ad uno o più servizi offerti da Data Appeal e indicati nel relativo catalogo contatta direttamente, e tramite gli strumenti di comunicazione messi a disposizione dal portale, la Società. Tale portale online garantisce pertanto, proprio in ragione di com’è strutturato, la tracciabilità dei flussi informativi tra la Società e l’Ente fin dalla prima interazione.

Per quanto attiene, invece, alle commesse basate su bandi di gara, le modalità operative relative alla partecipazione alla gara, e quindi alla presentazione dell’offerta tecnica ed economica da parte delle società partecipanti, così come le modalità di interazione e gestione del rapporto, oltre che una serie di linee guida per la presentazione dei relativi documenti sono predeterminate dalla normativa applicabile e dettagliatamente indicate dal bando stesso. Allo stesso modo, il bando di gara indica in maniera predeterminata i criteri in base ai quali verrà selezionato l’aggiudicatario (ad es. economico, tecnico, ecc.).

A seconda del servizio di cui trattasi, può essere consentito e richiesto alla Società di partecipare attraverso un raggruppamento temporaneo di imprese, talvolta già individuate, talvolta a discrezionalità del soggetto partecipante. Si tratta comunque di casi assolutamente poco frequenti e non ricorrenti.

La Società – di norma attraverso l'area commerciale - procede quindi a valutare l'offerta e/o il servizio richiesto e/o selezionarla in base ai criteri individuati nel *business plan* e, dunque, verificare che sia in linea con i criteri di vendita generalmente utilizzati dalla Società. A tal fine, la funzione commerciale dispone altresì di una propria procedura per la corretta stima dei prezzi da proporre al cliente finale (in questo caso, la PA), basata su tre criteri principali:

- stima del valore dei dati coinvolti nella potenziale vendita;
- costi aggiuntivi (ad esempio, lavorazioni, costi esterni);
- ricarichi in misura standard.

La funzione commerciale è tenuta inoltre a richiedere il coinvolgimento, già in questa fase, della funzione Finance nel caso in cui valuti, tenuto conto dei criteri sopra esposti, che i prezzi stimati tramite i normali strumenti interni non siano adeguati al *budget* disponibile dal cliente finale, al fine di verificare se si renda opportuno proporre un prezzo particolare per non perdere l'opportunità. In caso di interesse nella partecipazione ad una gara o ad una procedura di affidamento diretto, il soggetto dell'area commerciale informa l'Area Finance e dunque il CFO e/o il CEO, creando una cartella condivisa nel *file system* aziendale con tutto il materiale di riferimento, per un'ulteriore verifica dei presupposti di partecipazione e della regolarità nonché della convenienza nella partecipazione a tale progetto e /o nello svolgimento di tale incarico. In particolare, nel caso in cui si renda opportuno prevedere un'offerta personalizzata, la funzione commerciale dovrà ottenere l'approvazione della funzione Finance al fine di sottomettere l'offerta così personalizzata. La decisione finale circa la partecipazione al bando e/o all'offerta spetta dunque al CEO, raccolto il parere del CFO.

Qualora la Società intenda partecipare, la predisposizione dei documenti sarà demandata all'area commerciale, sotto la supervisione del CFO e del reparto *Finance* che si occupa di affiancare il commerciale nella revisione integrale del materiale e di vistare tutti i documenti per apporre la firma del CEO prima della sottomissione finale.

Per quanto attiene alla **fase C**), in caso di aggiudicazione del servizio, la Società predispone l'ulteriore documentazione atta a garantire la tracciabilità dei flussi finanziari, quale ad esempio la Dichiarazione Tracciabilità dei Flussi Finanziari redatta ai sensi dell'art. 3, l. 13/08/2010, n. 136, come successivamente modificata e integrata, nonché atta a certificare l'assenza di rapporti promiscui con i soggetti della Pubblica Amministrazione. Si tratta, in particolar modo, della cd. Dichiarazione di *pantouflage* o *revolving doors*, idonea a prevenire fenomeni corruttivi o l'esercizio di illecite influenze, così come fenomeni di clientelismo e/o conflitti di interessi tra privati e Pubblica Amministrazione.

La Società, nella gestione del servizio oggetto di aggiudicazione, rendiconta le varie fasi di sviluppo e provvede a monitorare i rapporti con la Pubblica Amministrazione secondo i processi già sopra descritti.

L'erogazione del servizio da parte di Data Appeal e i pagamenti da parte della Pubblica Amministrazione avvengono, rispettivamente, in un'unica *tranche* o attraverso pagamenti periodici o a SAL, salvo diverse pattuizioni contenute nei bandi di gara. In ogni caso, il CFO e la funzione Finance monitorano l'intero svolgimento dell'attività da parte della Società e il relativo processo di fatturazione, verificando, attraverso comunicazioni tracciabili (es. e-mail) e tramite la dashboard interna di monitoraggio delle commesse posta sul CRM aziendale, l'effettiva erogazione del servizio,

così come la ricezione dei dovuti pagamenti da parte della Pubblica Amministrazione, attraverso l'esame e il controllo di tutti i documenti necessari, ed in particolare le autorizzazioni all'emissione delle fatture, secondo le procedure amministrative in uso presso l'azienda in tema di fatturazione.

Vi sono poi tutta una serie di aree di attività a rischio indiretto in relazione alla commissione di reati di cui al Decreto, per cui si rende ugualmente necessario predisporre e osservare processi virtuosi in ottica preventiva.

5. PRINCIPI DI COMPORTAMENTO NELLE AREE DI ATTIVITÀ A RISCHIO INDIRETTO

Come detto, il Modello deve prevedere ulteriori controlli su alcune aree di attività che, pur non essendo direttamente a rischio di commissione di reati contro la Pubblica Amministrazione, possono tuttavia fornire l'occasione per predisporre somme di denaro da impiegare a scopi corruttivi o di conferire incarichi e vantaggi che possono mascherare illecite dazioni.

Attività di fatturazione e pagamenti

L'attività di fatturazione segue procedure interne che implicano l'intervento e/o l'autorizzazione di almeno due soggetti.

Nessuna fattura, può essere emessa o pagata con modalità diverse rispetto alle procedure amministrative previste e, soprattutto, con l'iniziativa di un solo soggetto.

In riferimento all'attività di pagamento, Data Appeal adotta un piano interno formalizzato che prevede l'individuazione specifica di tutti i soggetti legittimati ad autorizzare ed eseguire i pagamenti che si rendono necessari per l'esercizio dell'attività aziendale: il piano prevede per ciascuna tipologia di pagamento la preventiva verifica presso l'ufficio richiedente la prestazione dell'effettiva ricezione del bene o della prestazione del servizio, l'invio da parte della *business function* coinvolta alla funzione *Finance* della fattura, la proposta da parte del CFO di pianificazione di pagamento della fattura così approvata, l'approvazione dei pagamenti e la successiva firma per l'autorizzazione del bonifico secondo quanto previsto dai poteri di firma (firme singole o congiunte).

In particolare, per i pagamenti di importi fino a 5.000 Euro, l'autorizzazione al bonifico e la relativa firma a disporre il pagamento è data, anche singolarmente, dal CFO e/o dal CEO; per pagamenti di importi ricompresi tra Euro 5.000 a Euro 50.000, la disposizione del pagamento deve essere autorizzata e firmata dal CEO, mentre per pagamenti superiori a Euro 50.000, la disposizione del pagamento deve essere autorizzata da firma congiunta del CFO e del CEO, ferma restando la necessaria approvazione del Consiglio di Amministrazione per le materie di propria competenza.

Chiunque rilevi elementi che possano suscitare il sospetto di illecite attività di fatturazione fittizia o di fatturazione per importi maggiori di quelli reali deve darne immediata notizia al CFO. Della segnalazione è data notizia all'Organismo di Vigilanza.

Politica dei regali e omaggi

Ai sensi dei principi generali di comportamento sopra evidenziati, Data Appeal ha quindi elaborato una politica inerente i regali e gli omaggi.

Ogni omaggio indirizzato ai clienti deve essere inserito nel budget relativo all'area *marketing* dedicata e deve essere in seguito sottoposto all'attenzione del Consiglio di Amministrazione per l'approvazione contestualmente al budget annuale.

Si ritiene utile precisare, in aggiunta a quanto già sopra evidenziato, che in riferimento agli omaggi ed ai regali verso l'esterno, e in particolare verso fornitori e clienti, la procedura prevede che l'area interessata invii le proprie segnalazioni all'area *marketing*, anche in occasione di particolari ricorrenze, per un primo vaglio e al fine di consentirne l'inserimento in una lista complessiva, soggetta ad approvazione finale dell'Amministratore Delegato.

In riferimento, invece, gli omaggi ed ai regali dall'esterno, in ossequio alle linee guida sopra riportate, è infatti richiesto a tutto il personale di non accettare regali di valore superiore a una certa soglia (Euro 100,00) ed è fatto obbligo di segnalare all'area HR eventuali casistiche in cui si prospetti una situazione difforme, per verificare l'eventuale possibilità di accettare comunque la regalia a scopo di condividere il regalo stesso all'interno della realtà aziendale.

Organizzazione di eventi di intrattenimento e di marketing

È consentita l'organizzazione di eventi di intrattenimento a condizione che siano connessi con la presentazione o con la promozione di uno specifico prodotto o servizio offerti dalla Società.

Allo stesso modo, è consentita la distribuzione di prodotti promozionali o di *marketing* ai clienti della Società, a condizione che i prodotti promozionali consegnati siano di quantità e importo ragionevoli e comunque sempre connessi al *business* aziendale. È altresì consentita l'organizzazione di eventi promozionali, a condizione che gli stessi siano indirizzati e coinvolgano la totalità dei possibili destinatari e non invece singoli e specifici soggetti selezionati.

Selezione del personale

La selezione del personale avviene nel rispetto del al cd. *hiring plan*, ossia il piano di assunzioni che viene predisposto annualmente dalla funzione HR e rivisto dal CFO e dal CEO. Il piano di assunzioni, e le successive modifiche ed integrazioni, è sottoposto alla preventiva approvazione del Consiglio di Amministrazione ed è aggiornato trimestralmente dal CFO in collaborazione con l'HR che vi apportano le eventuali variazioni che si rendano necessarie in relazione alle eventuali esigenze sopravvenute.

Il processo di selezione avviene sulla base delle indicazioni dell'*hiring plan* e in funzione dei tempi di ingresso desiderati. Il processo prende impulso dall'HR che propone all'Amministratore Delegato ed al CFO l'apertura delle selezioni in accordo con il responsabile della funzione richiedente, nel rispetto della specifica procedura adottata dalla Società, che prevede comunque sempre il coinvolgimento di almeno due soggetti tanto nella fase di selezione, quanto in quella decisionale.

Al termine della selezione è inoltre previsto un ulteriore passaggio di confronto tra i componenti dell'*hiring team*, per stabilire i parametri dell'offerta economica.

È inoltre previsto il passaggio in Consiglio di Amministrazione per l'approvazione in merito all'assunzione della nuova risorsa nel caso di assunzioni di posizioni dirigenziali o che prevedono un'offerta economica annua superiore a una certa soglia.

Eventuali segnalazioni di candidature da parte del personale di Data Appeal sono consentite nel rispetto della procedura elaborata dalla Società (cd. *referral program*), in ossequio ai principi di terzietà e meritocrazia (es. esclusione dell'*hiring team* e delle figure manageriali dal cd. *referral program*).

Il cd. *referral program* prevede una forma di ricompensa economica, stabilita con cadenza annuale per ciascun dipendente che segnali profili e/o si faccia portavoce di candidature. Tale meccanismo, predisposto dalla Società al fine di acquisire profili di alto livello e di forte motivazione, con relative referenze, è tuttavia presidiato da idonee garanzie, in quanto il compenso (i) è corrisposto solamente all'esito positivo del periodo di prova del profilo eventualmente segnalato e (ii) non è corrisposto ai componenti dell'*hiring team* e alle figure manageriale, al fine di evitare ogni indebita ingerenza.

Successivamente all'entrata in azienda, è prevista una specifica formazione del neo-assunto.

Incarichi a consulenti e professionisti esterni

La Società collabora, quanto alle ordinarie attività di consulenza, con professionisti selezionati con cui ha instaurato un rapporto pluriennale.

Data Appeal provvede comunque alla verifica periodica circa la conservazione, nel tempo, dei necessari requisiti di correttezza e professionalità dei consulenti incaricati. Identiche verifiche vengono compiute in caso di affidamento di incarichi a nuovi consulenti, con cui Data Appeal non abbia in precedenza intrattenuto alcun rapporto, per la cui selezione la Società ha formalizzato una specifica procedura che prevede che la selezione e la scelta vengano effettuate da più soggetti, con tracciabilità del relativo processo.

Gli incarichi a liberi professionisti, consulenti e collaboratori esterni sono assegnati con lettera di incarico scritta che ne indica puntualmente il contenuto e, laddove possibile, l'importo degli onorari che saranno riconosciuti. La lettera di incarico è firmata seconda i poteri di firma previsti, e dunque: (i) per gli incarichi di importi fino a 5.000 Euro, la firma, anche singola, del CFO o del CEO; (ii) per gli incarichi di importi ricompresi tra Euro 5.000 e Euro 50.000, la firma del CEO, (iii) per gli incarichi di importi superiori a Euro 50.000, la firma congiunta del CFO e del CEO, ferma restando la necessaria approvazione del Consiglio di Amministrazione per le materie di sua competenza.

In ogni caso, la gestione del rapporto con i consulenti avviene in modo che non vi sia identità soggettiva tra chi richiede la consulenza e chi verifica l'effettivo adempimento dell'incarico, prima di eseguire il pagamento.

Nomina di amministratori e di membri degli altri organi sociali

Le delibere di nomina degli amministratori e dei membri degli altri organi sociali devono sempre dare conto, seppur sinteticamente, delle ragioni che hanno condotto alla scelta di quel determinato soggetto.

PARTE SPECIALE “B”

Reati societari

1. LA TIPOLOGIA DEI REATI SOCIETARI DI CUI AGLI ARTT. 2621 E SS. C.C. (ART. 25 TER DEL DECRETO)

L'art. 25 *ter* del Decreto, introdotto nel 2002 e oggetto di modifiche successive e più recenti, ha esteso la responsabilità amministrativa degli Enti anche ai c.d. reati societari.

Le sanzioni previste per la tipologia di reati presupposto in esame sono esclusivamente di natura pecuniaria, con un aumento di un terzo se l'Ente ha conseguito dal reato un profitto di rilevante entità.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito, tutte previste dal codice civile.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
2621 c.c.	False comunicazioni sociali	da 200 a 400 quote	No
2621 <i>bis</i> c.c.	False comunicazioni sociali (di lieve entità)	da 100 a 200 quote	No
2622 c.c.	False comunicazioni sociali delle società quotate	da 400 a 600 quote	No
2625 c.c.	Impedito controllo	da 200 a 360 quote	No
2632 c.c.	Formazione fittizia del capitale sociale	da 200 a 360 quote	No
2626 c.c.	Indebita restituzione dei conferimenti	da 200 a 360 quote	No
2627 c.c.	Illecita ripartizione degli utili e delle riserve	da 200 a 260 quote	No
2628 c.c.	Illecite operazioni sulle azioni o quote sociali o della società controllante	da 200 a 360 quote	No
2629 c.c.	Operazioni in pregiudizio dei creditori	da 300 a 660 quote	No
2633 c.c.	Indebita ripartizione dei beni sociali da parte dei liquidatori	da 300 a 660 quote	No

2636 c.c.	Illecita influenza in assemblea	da 300 a 660 quote	No
2637 c.c.	Aggiotaggio	da 400 a 1000 quote	No
2629 <i>bis</i> c.c.	Omessa comunicazione del conflitto di interessi	da 400 a 1000 quote	No
2638 c.c.	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	da 400 a 800 quote	No

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa, seguendo un ordine basato sul bene protetto da ciascuna categoria di reati.

1.1 Ipotesi di falsità

False comunicazioni sociali e False comunicazioni sociale in danno della società, dei soci o dei creditori (artt. 2621, 2621-*bis* e 2622 c.c.)

Le fattispecie delineate dagli artt. 2621, 2621*bis* e 2622 c.c. puniscono le medesime condotte, con la previsione di circostanze attenuanti (art. 2621 *bis* c.c.), o aggravanti (art. 2622 c.c.).

La condotta, descritta dall'art. 2621 c.c., consiste nella rappresentazione - nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico - di fatti materiali rilevanti non veritieri ovvero nell'omissione - nelle medesime comunicazioni - di fatti materiali rilevanti la cui comunicazione sia imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo cui questa appartiene.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori. La condotta, perché sia penalmente rilevante, deve essere posta in essere con il duplice intento di ingannare i soci, i creditori o il pubblico, da un lato, e di ottenere per sé o per altri un ingiusto profitto, dall'altro.

L'articolo 2621 *bis* c.c. punisce le medesime condotte previste dall'art. 2621, ma che sono considerate di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

L'art. 2622 c.c. punisce invece le medesime condotte, che siano commesse nell'ambito di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione Europea.

1.2 Tutela del Capitale Sociale

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

La norma risulta violata quando, fuori dai casi di legittima riduzione del capitale sociale, gli amministratori restituiscano, anche in via simulata, i conferimenti a uno o più soci o li liberino dall'obbligo di eseguirli.

Nel caso di molteplici atti restitutori o liberatori, per l'integrazione del delitto è sufficiente il compimento del primo di questi.

Soggetti attivi del reato, come nei successivi reati di cui agli artt. 2627-2629 c.c., possono essere solo gli amministratori.

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

La condotta individuata dalla norma è integrata quando gli amministratori ripartiscano utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscano riserve che per legge non potrebbero essere distribuite.

La norma prevede tuttavia che la restituzione degli utili o la ricostituzione delle riserve prima del termine per l'approvazione del bilancio d'esercizio estinguono il reato.

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

Il reato si perfeziona quando gli amministratori, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali della società (o della società controllante) cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili.

Come nel caso dell'illegale ripartizione degli utili, la ricostituzione del capitale sociale o delle riserve prima del termine per l'approvazione del bilancio d'esercizio estinguono il reato.

Il concetto di "acquisto" ricomprende qualsiasi negozio valido a trasferire alla società la proprietà di azioni o quote emesse dalla stesa.

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

La fattispecie è finalizzata a tutelare i creditori e sanziona la condotta degli amministratori che, in violazione delle disposizioni di legge, effettuano riduzioni del capitale sociale, o fusioni con altra società, o scissioni, quando queste operazioni provochino un danno ai creditori della società.

Qualora, prima del giudizio, intervenga il risarcimento del danno subito dai creditori, il reato si estingue.

Omessa comunicazione del conflitto di interessi (2629 bis c.c.)

L'art 2629 bis c.c. punisce la violazione dell'art. 2391 comma 1 c.c. (che impone l'obbligo di comunicazione del conflitto di interessi) da parte degli amministratori o dei componenti del consiglio di gestione di una società con titoli quotati in mercati regolamentari italiani o di altro Stato dell'Unione Europea, o diffusi tra il pubblico in misura rilevante ovvero di un soggetto sottoposto a vigilanza ai sensi del TUF.

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

La norma prevede tre possibili condotte, accomunate dal medesimo effetto di provocare la formazione o l'aumento fittizio del capitale sociale:

- attribuzione di quote o azioni in misura complessivamente superiore all'ammontare del capitale sociale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Oltre agli amministratori, soggetti attivi del reato possono essere i soci conferenti.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

La fattispecie punisce la condotta dei liquidatori nel caso in cui provvedano a ripartire i beni sociali tra i soci prima del pagamento dei creditori o dell'accantonamento delle somme necessarie per la loro soddisfazione, con conseguente danno per i creditori stessi.

Il reato è estinto se, prima del giudizio, interviene il risarcimento del danno in favore dei creditori.

Soggetti attivi del reato possono essere, evidentemente, solo i liquidatori.

1.3 Tutela del corretto funzionamento della società

Impedito controllo (art. 2625 c.c.)

La norma prevede, a livello generale, una condotta costituente mero illecito amministrativo, che consiste nel fatto degli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo che la legge attribuisce ai soci o agli altri organi sociali.

Soggetti attivi del reato possono essere quindi solo gli amministratori.

Se però le condotte appena descritte cagionano un danno ai soci, esse assumono rilevanza penale.

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

La norma punisce la condotta di chi, con atti simulati o con frode, determini la formazione della maggioranza assembleare, per procurare a sé o ad altri un ingiusto profitto.

1.4 Tutela contro le frodi

Aggiotaggio (art. 2637 c.c.)

La fattispecie prevista dall'art. 2637 è integrata dalla condotta di chi diffonda notizie false ovvero ponga in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o di gruppi bancari.

È opportuno sottolineare che la norma, a far data dal 2005, sanziona solo le condotte di aggio che influiscono sul valore di titoli non quotati. Da quell'anno, infatti il legislatore ha introdotto gli artt. 184 e 185 nel TUF, con cui ha separatamente disciplinato gli abusi di mercato su titoli di società quotate. La stessa legge ha introdotto un nuovo art. 25 *sexies* nel Decreto, con cui è stata espressamente prevista la responsabilità amministrativa degli Enti anche per queste due nuove figure di reati.

A queste due specifiche fattispecie di abuso di mercato sarà dedicata la successiva Parte Speciale.

1.5 Tutela delle funzioni pubbliche di vigilanza

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

La norma prevede due differenti fattispecie, distinte per modalità di condotta e momento offensivo.

La prima si realizza o con l'esposizione di fatti materiali non rispondenti al vero sulla situazione patrimoniale, economica e finanziaria della società, anche se oggetto di valutazione, nelle comunicazioni previste dalla legge nei confronti di Autorità Pubbliche di Vigilanza o con l'occultamento di fatti, sempre relativi alla situazione economica, patrimoniale e finanziaria della società, che avrebbero dovuto essere comunicati.

La seconda si realizza con ogni altra forma di ostacolo, attuata consapevolmente, alle attività di vigilanza delle Autorità Pubbliche.

Soggetti attivi del reato possono essere solo gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, nonché tutti i soggetti che la legge indica come sottoposti ad autorità pubbliche di vigilanza o come titolari di obblighi specifici nei confronti di queste.

2. AREE A RISCHIO

Alla luce dei reati e delle condotte sopra richiamate, l'analisi delle attività di impresa, delle procedure adottate e dei sistemi di monitoraggio predisposti dalla Società ha rivelato l'esistenza di un rischio di commissione dei reati societari descritti contenuto.

Data Appeal non è una società quotata, non ricorre al pubblico risparmio, non è sottoposta alla relativa Autorità Pubblica di Vigilanza (Consob): questi dati escludono l'esistenza di un rischio specifico di commissione di quelli, tra gli illeciti indicati, relativi a questi profili (prospetti, rapporti con il mercato, rapporti con Autorità di Vigilanza).

I rischi di commissione di illeciti societari, si ricollegano quindi anche in Data Appeal, a quelli fisiologici esistenti in ogni persona giuridica che eserciti attività di impresa e sono, in particolare individuabili nelle seguenti aree di attività:

- A) attività di predisposizione di comunicazioni dirette ai soci o al pubblico e, in particolare, redazione e predisposizione del bilancio d'esercizio;
- B) gestione dei rapporti con le società di revisione ed esercizio di ogni altro controllo interno;
- C) operazioni societarie che possono incidere sulla integrità del capitale sociale e di gestione della *corporate governance*.

L'elenco è suscettibile di ogni integrazione futura; sarà, quindi, sempre possibile l'individuazione di ulteriori aree di rischio (con conseguente predisposizione di norme comportamentali specifiche e di relative procedure). A tal proposito, l'Organismo di Vigilanza potrà proporre al Consiglio di Amministrazione ogni opportuno intervento sul testo della presente Parte Speciale. Il Consiglio di Amministrazione potrà, peraltro, assumere in autonomia analoghe iniziative.

Il rischio di commissione all'interno di Data Appeal risulta peraltro contenuto, anche grazie alle regole generali di condotta adottate dalla Società, e sintetizzate in parte anche nel Codice Etico, nella predisposizione del bilancio d'esercizio, arricchite anche dalla previsione, all'interno della Società, di un sistema di reportistica mensile, finalizzata non solo a garantire il controllo sui dati contabili che confluiscono infine nel bilancio, ma anche ad assicurare una costante e corretta informativa ai soci, attraverso il costante controllo degli organi sociali, come infra riportato.

3. REGOLE DI COMPORTAMENTO GENERALI

Ai Destinatari è fatto espresso obbligo:

- di tenere un comportamento corretto, scrupolosamente trasparente e collaborativo, nel rispetto delle norme di legge e di tutte le procedure aziendali, in tutte le attività correlate e finalizzate alla preparazione del bilancio e delle altre comunicazioni sociali, con lo scopo di fornire sempre ai soci e ai terzi un'informazione veritiera, completa e corretta sulla situazione economica, finanziaria e patrimoniale di Data Appeal nel suo complesso;
- porre la massima attenzione e cautela, attraverso il rispetto delle norme di legge e delle procedure interne a essa indirizzate, alla tutela dell'integrità ed effettività del capitale e del patrimonio sociali, nel rispetto totale delle garanzie dei creditori e dei terzi in genere;

- aver cura e tutelare il regolare funzionamento degli organi sociali di Data Appeal, garantendo e agevolando ogni forma di controllo sulla gestione sociale e garantendo la libera formazione della volontà assembleare;
- aver cura di effettuare, nella piena veridicità, con tempestività e correttezza, tutte le comunicazioni previste dalla disciplina applicabile nei confronti delle Autorità competenti, evitando di frapporre qualsivoglia ostacolo all'esercizio delle loro attività di controllo e verifica;
- non diffondere notizie in merito alle iniziative e le scelte di *partner* commerciali (conclusione di accordi con Data Appeal, collaborazioni con la Società e quant'altro), se non quando strettamente necessarie e con l'accordo del partner stesso.

4. REGOLE DI COMPORTAMENTO PARTICOLARI, RELATIVE ALLE SPECIFICHE AREE DI RISCHIO

4.1 Comunicazioni ai Soci e al pubblico

Bilanci ed altre comunicazioni sociali

Data Appeal ha da tempo elaborato una solida procedura per la redazione del proprio bilancio di esercizio, in cui sono stati puntualmente individuate tutte le funzioni aziendali e quindi i soggetti che devono contribuire a questa attività.

Il sistema gestionale contabile aziendale di cui è dotata Data Appeal consente inoltre, ed in qualunque momento, di accedere ai dati relativi alla fatturazione.

La Società risulta pertanto dotata di un efficace sistema di controllo che consente di monitorare, in tempo reale, la situazione contabile della Società e che consente pertanto di ritenere che, riguardo a questi, il rischio della commissione di taluno dei reati in esame sia fortemente ridotto.

Anche il sistema contabile adottato da Data Appeal consente di considerare contenuto il rischio di commissione dei reati qui in esame. I dati contabili sono infatti soggetti al periodico controllo da parte della funzione *Finance* della Società, che provvede alla redazione di un bilancio mensile, con verifica, controllo e se del caso riallineamento dei valori. La chiusura mensile dei conti viene inoltre, e in aggiunta, condivisa dal CFO e, successivamente, con l'intero Consiglio di Amministrazione.

Tale processo prevede una prima fase di estrazione dal gestionale aziendale ed elaborazione dei dati contabili, economici e finanziari, che confluiscono nel bilancio di verifica mensile, e viene utilizzato anche al fine di predisporre la chiusura mensile della contabilità. I dati raccolti e riportati nel *report* mensile comprendono costi per fatture da ricevere, risconti delle fatture attive e passive, proiezioni dei costi capitalizzati e dei benefici fiscali derivanti da crediti d'imposta, ammortamenti dei cespiti e degli immateriali, i quali vengono rappresentati secondo le politiche stabilite in sede di ultima approvazione del bilancio.

Il sistema adottato di *reporting* mensile consente quindi il monitoraggio e la verifica costante dei dati contabili, attraverso il riesame delle attività finanziarie e contabili effettuate nel periodo di riferimento. Il controllo viene materialmente esercitato dall'area *Finance*, con la supervisione e il controllo del CFO sul *report* elaborato, e la condivisione finale del *report* medesimo con il Consiglio di Amministrazione.

A ciò si aggiunge, infine, l'analisi sui dati contabili, che viene affidata alla revisione di società iscritta all'albo tenuto dalla Consob.

Oltre alle specifiche indicazioni e principi di comportamento che di seguito saranno indicati, resta fermo il richiamo a tutti i principi generalmente accolti da Data Appeal nonché dalla Parte Generale del presente Modello.

Tale procedura, oltre a garantire un controllo analitico e puntuale in materia contabile, concorre anche, ai fini del presente Modello, a circoscrivere il rischio di commissione dei reati di cui alla presente Parte Speciale.

Nella redazione del bilancio annuale e della relazione sulla gestione Data Appeal segue i seguenti principi, indicati nell'apposita procedura adottata dalla Società:

- separazione dei compiti: individuazione dei dati e delle notizie che ciascun soggetto o ciascuna funzione aziendale deve fornire, individuazione dei soggetti o della funzione cui devono essere trasmessi, i criteri per la loro elaborazione, nonché la tempistica del loro trasferimento;
 - trasmissione e conservazione dei dati per via informatica, in modo che esista traccia del loro percorso e sia sempre possibile l'identificazione dei soggetti che hanno immesso i dati;
- previsione di scadenze precise, perché sia consentita la tempestiva trasmissione a tutti i membri del Consiglio di Amministrazione e del Collegio Sindacale della bozza del bilancio e della società di revisione, con un congruo anticipo rispetto alla data di approvazione.

4.2 Gestione dei rapporti con le società di revisione e altri controlli sulla gestione sociale

In ordine alla scelta della società di revisione, saranno seguiti questi accorgimenti:

- l'immediata comunicazione all'Organismo di Vigilanza del nominativo della società di revisione prescelta, nonché delle valutazioni e delle considerazioni che l'hanno determinata;
- la comunicazione sistematica e tempestiva all'Organismo di Vigilanza di qualsiasi altro incarico specifico che sia attribuito alla società di revisione, nonché ogni ulteriore notizia rilevante circa il rapporto tra Data Appeal e la società di revisione;
- in generale, il divieto di concludere con la Società di Revisione prescelta qualsiasi contratto di consulenza.

Quanto, invece, allo svolgimento dell'attività di controllo sulla gestione sociale, le procedure dovranno stabilire:

- i tempi e le scadenze per la tempestiva trasmissione, alla società di revisione e al Collegio Sindacale e a ogni altro soggetto che legittimamente eserciti poteri di controllo, di tutti i dati e di tutte le informazioni necessarie alle loro attività;
- le modalità per la tempestiva trasmissione al Collegio Sindacale di tutti i documenti e le informazioni relativi ad argomenti posti all'ordine del giorno del Consiglio di Amministrazione e delle Assemblee, quando è necessario che il Collegio Sindacale esprima il proprio parere;
- la possibilità di riunioni periodiche e confronti tra Collegio Sindacale, società di revisione e Organismo di Vigilanza su questioni relative all'osservanza delle regole e delle procedure aziendali in tema di normativa societaria da parte degli Amministratori, dei dirigenti e dei dipendenti.

Per quanto riguarda, in particolare, l'attività della società di revisione:

- dovrà essere consentito al responsabile della società di revisione di prendere contatto, in ogni occasione lo ritenga opportuno, con l'Organismo di Vigilanza per verificare e analizzare congiuntamente situazioni che possano presentare aspetti di criticità;
- dovrà essere esplicitamente vietata la possibilità della stipulazione di contratti di lavoro autonomo o subordinato con dipendenti delle società che effettuano la revisione contabile di società controllate per un congruo lasso di tempo dopo la scadenza del contratto tra Data Appeal e la società di revisione o dopo l'interruzione del rapporto del dipendente con la società di revisione.

4.3 Tutela del Capitale Sociale

Tutte le operazioni che, anche indirettamente, possono influire sul capitale sociale di Data Appeal, quali la distribuzione di utili e riserve, l'acquisto o la cessione di partecipazioni o rami d'azienda, di fusione, scissione o scorporo, devono prevedere:

- la precisa attribuzione delle responsabilità decisionali e di quelle operative nell'ambito dei singoli progetti, nonché i meccanismi di coordinamento tra le funzioni così individuate;
- l'informazione all'Organismo di Vigilanza, fin dal principio del progetto, in modo che sia possibile che questo segua l'intero *iter* decisionale;
- la messa a disposizione allo stesso Organismo di Vigilanza dell'intera documentazione relativa a ogni progetto;
- la possibilità di riunione e confronto tra Collegio Sindacale, società di revisione, e Organismo di Vigilanza in merito a profili di criticità relativi ai progetti in parola.

Per quanto riguarda l'eventuale conflitto di interessi, l'obbligo per gli amministratori di comunicare al Consiglio di Amministrazione, al Collegio Sindacale e all'Organismo di Vigilanza, che ne cura l'archiviazione e l'aggiornamento, tutte le informazioni relative alle cariche assunte o alle partecipazioni di cui sono titolari, direttamente o indirettamente, in altre società o imprese, nonché le cessazioni o le modifiche delle medesime, le quali, per la natura o la tipologia, possono lasciar ragionevolmente prevedere l'insorgere di conflitti di interesse ai sensi dell'art. 2391 c.c.

4.4 Rapporti con le Autorità competenti

Per quanto riguarda eventuali rapporti con le Autorità competenti, sono tre i potenziali ambiti di attività rilevanti:

- la predisposizione e la trasmissione delle informazioni, periodiche e non, richieste dalla legge e dai regolamenti;
- la predisposizione e la trasmissione di ogni altra informazione che sia ulteriormente richiesta dalle Autorità competenti;
- le condotte da tenere nel caso di verifiche ispettive delle stesse Autorità.

In questi casi, le attività dovranno essere rette dai seguenti principi:

- i termini e i modi della trasmissione e della circolazione interna dei dati necessari alla predisposizione delle informazioni alle Autorità competenti, con la previsione di meccanismi e procedure che assicurino la massima veridicità e completezza degli stessi;

- l'individuazione di responsabili, che curino il rispetto delle procedure previste e rilascino una dichiarazione di veridicità e completezza delle informazioni raccolte e predisposte;
- nel caso di verifiche ispettive, la massima collaborazione da parte di tutte le unità aziendali coinvolte, la tempestiva individuazione di un responsabile delle attività necessarie, che possa assicurare il massimo coordinamento tra le unità aziendali coinvolte e la massima rapidità nella messa a disposizione delle informazioni richieste dagli ispettori;
- in generale, la possibilità, per tutti i responsabili individuati, di rivolgersi e riferire all'Organismo di Vigilanza in merito allo svolgimento delle attività relative ai rapporti con le Autorità competenti, segnalando altresì eventuali carenze delle procedure e dei metodi operativi predisposti;
- per quanto riguarda il responsabile individuato nel caso di verifiche ispettive la redazione di una relazione all'Organismo di Vigilanza sull'indagine avviata, che dovrà essere periodicamente aggiornata in relazione agli sviluppi dell'indagine stessa e al suo esito.

PARTE SPECIALE “C”

Abusi di mercato

1. I DELITTI DI CUI AGLI ARTT. 184 E 185 TUF (ART. 25 *SEXIES* DEL DECRETO)

Nel corso del 2005, con la L. 18 aprile 2005 n. 62, in esecuzione della Direttiva 2003/6/CE del Parlamento Europeo e del Consiglio del 28 gennaio 2003, relativa all’abuso di informazioni privilegiate e alla manipolazione del mercato, è stato introdotto nel Decreto l’art. 25 *sexies*, che ha esteso la responsabilità amministrativa degli Enti anche a condotte di esponenti aziendali che integrino una delle due fattispecie di abuso di mercato previste negli articoli citati del TUF.

La stessa legge, peraltro, ha provveduto a ridelineare il quadro degli illeciti di abuso di mercato, introducendo, agli artt. 184 e 185 nel TUF, due distinti delitti, su cui si sono registrati interventi normativi successivi, l’ultimo dei quali nel 2018.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
184 TUF	Abuso di informazioni privilegiate	da 400 a 1.000 quote	no
185 TUF	Manipolazione del mercato	da 400 a 1.000 quote	no

Si noti che per entrambi i reati se il prodotto o il profitto conseguito dall’Ente è di rilevante entità, la sanzione è aumentata fino a 10 volte tale prodotto o profitto.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

Abuso di informazioni privilegiate (art. 184 TUF)

La norma sanziona l’abuso di informazioni privilegiate, consistente nella condotta di chi, in virtù:

- (i) della sua qualità di membro di organi di amministrazione, direzione o controllo dell’emittente, o
- (ii) della partecipazione al capitale della emittente, ovvero
- (iii) dell’esercizio di un’attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio,

è in possesso di informazioni privilegiate e

- a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o di terzi, su strumenti finanziari utilizzando le informazioni stesse,
- b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell’ufficio o di un sondaggio di mercato (effettuato ai sensi dell’art. 11 del Regolamento (UE) n. 596/2014, relativo agli abusi di mercato);
- c) raccomanda o induce altri, sulla base di tali informazioni, a compiere una delle operazioni di cui alla lettera a).

Soggetti attivi del reato, pertanto, possono essere sia soggetti rientranti nell’organigramma societario (c.d. “*corporate insiders*”) sia soggetti estranei ad essa (c.d. “*temporary insiders*”).

Si noti che l'art. 181 TUF definisce espressamente la nozione di informazione privilegiata: si tratta di un'informazione di carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di tali strumenti finanziari.

Un'informazione si ritiene di carattere preciso se: (i) si riferisce ad un complesso di circostanze esistenti o che si possa ragionevolmente prevedere che verranno ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà; (ii) è sufficientemente specifica da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento sui prezzi degli strumenti finanziari.

Per informazione che, se resa pubblica, potrebbe influire in modo sensibile sui prezzi di strumenti finanziari, si intende un'informazione che presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento.

Manipolazione del mercato (art. 185 TUF)

La norma punisce le condotte di chi:

- 1) diffonde notizie false;
- 2) compie operazioni simulate; o
- 3) realizzazione altri artifici

nel caso in cui tali condotte siano idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari.

2. GLI ILLECITI AMMINISTRATIVI DI CUI AGLI ARTT. 187-BIS E 187-TER DEL TUF

La nuova disciplina degli abusi di mercato introdotta nel 2005 è stata poi completata dagli artt. 187-*bis* e 187-*ter* del TUF, che stabiliscono che fatti di abuso di informazioni privilegiate e di manipolazione del mercato possano anche costituire illeciti amministrativi, colpiti da sanzioni pecuniarie alquanto gravi, che vanno da un minimo di centomila ad un massimo di quindici milioni di euro, per i fatti di abuso di informazioni, e fino a 25 milioni di euro nel caso di manipolazioni del mercato. Le sanzioni sono comminate dalla Consob.

Lo stesso fatto, quindi può avere rilevanza sia amministrativa che penale, e l'Ente che commette una delle condotte sopra descritte, nel proprio interesse o vantaggio, potrebbe essere colpito sia dalle sanzioni inflitte dalla Consob, sia da quelle comminate in sede penale.

L'art. 187 *quinquies* del TUF stabilisce che a questo caso si applichino, in quanto compatibili, gli artt. 5, 6 e 7 del Decreto, che, come noto, introducono la possibilità di esonero da responsabilità dell'ente che si sia dotato, attraverso un proprio Modello, di misure e prescrizioni idonee a prevenire gli illeciti: è previsto in altri termini un regime analogo a quello della responsabilità *ex* Decreto e le misure e le prescrizioni del Modello, quindi, devono mirare a prevenire anche questi illeciti amministrativi.

Il sistema sanzionatorio predisposto dal legislatore per gli abusi di mercato è dunque binario: vi è un piano penale, con reati che sono accertati dalla magistratura penale, sia per quanto riguarda la responsabilità penale personale sia per quella amministrativa degli Enti; vi è un piano amministrativo, con illeciti che sono accertati, sia per le persone fisiche che per quelle giuridiche, dall'Autorità Amministrativa (Consob).

I due profili possono coesistere, quindi: uno stesso fatto può essere oggetto di valutazione sia in sede penale che in sede amministrativa: l'art. 187-*duodecies* del TUF espressamente prevede che il procedimento amministrativo di accertamento e quello penale proseguano parallelamente, senza la prevalenza dell'uno sull'altro.

3. DEFINIZIONE DI STRUMENTI FINANZIARI RILEVANTE PER GLI ILLECITI EX ARTT. 184, 185, 187 BIS E 187 TER DEL TUF

L'art. 180 in collegamento con l'art. 1, comma 2 del TUF indica espressamente quali siano gli strumenti finanziari in relazione ai quali possano essere commessi i delitti di cui alla presente Parte Speciale.

Il minimo comun denominatore è l'essere strumenti quotati, sul mercato italiano o sul mercato di altro Paese comunitario: deve trattarsi di uno degli strumenti di cui all'art. 1 del TUF ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato di un Paese dell'Unione europea.

4. AREE A RISCHIO

Data Appeal non è una società quotata: il dato esclude il rischio che, nell'ambito della sua attività, possano essere compiuti abusi di mercato che siano relativi a titoli della società.

Al tempo stesso, Data Appeal non detiene partecipazioni in società quotate e, quindi, non opera in alcun modo sul mercato borsistico.

Residua, come area di rischio, unicamente la gestione delle informazioni, eventualmente *price sensitive*, relative a terze società in ipotesi quotate: si pensi al caso di notizie relative a conclusioni di accordi tra Data Appeal e tali società, rinnovi di accordi, interruzioni di collaborazioni. Ed è il motivo per cui, nonostante il rischio di commissione dei reati in esame sia stato ritenuto minimo all'interno della Società, si è deciso tuttavia di dedicarvi la presente Parte Speciale.

Le aree della Società ritenute a rischio di commissione di attività di abusi di mercato devono pertanto essere così individuate:

- gestione delle informazioni relative ad eventuali rapporti con terzi quotati o collegati con altri soggetti quotati, prima della loro formalizzazione/ufficializzazione;
- attività di comunicazione relativa a nuovi accordi, nuovi servizi e nuove *partnership* che coinvolgano terzi soggetti quotati o collegati a terzi quotati.

5. REGOLE GENERALI DI COMPORTAMENTO

Per norma generale, tutte le informazioni relative alla gestione dell'azienda, alle scelte imprenditoriali, a conclusioni di accordi e a nuove iniziative commerciali o nuovi prodotti e servizi sono trattate e gestite come informazioni riservate e diffuse solo tra i soggetti strettamente necessari, prima della formalizzazione delle decisioni.

Con specifico riferimento ad eventuali attività di comunicazione verso l'esterno, Data Appeal indica le seguenti norme di condotta:

- ogni forma di comunicazione aziendale con terzi e con il pubblico deve essere improntata a principi di trasparenza, veridicità e completezza;
- la comunicazione aziendale evita di includere dati e notizie che non siano strettamente attinenti alla Società, ma che riguardino altri soggetti, con l'eccezione delle notizie necessariamente connesse a fatti della Società;
- deve essere individuato un solo soggetto aziendale, direttamente dipendente dal Consiglio di Amministrazione, che curi la materia della comunicazione con il pubblico;

- allo stesso modo, la decisione sulle informazioni da diffondere al pubblico, sul contenuto delle informazioni, sulle forme della loro diffusione e, più in generale, su tutto ciò che concerne l'informazione e la sua diffusione, devono essere adottate da almeno due persone, d'accordo con loro, e secondo regole che consentano sempre di tracciare ogni passaggio dell'*iter* per la diffusione a terzi dell'informazione;
- è fatto obbligo a tutti i Destinatari di segnalare prontamente ogni comportamento ed ogni fatto che possa lasciar intendere lo sfruttamento o le rivelazioni di notizie riservate, se non anche la commissione di un abuso di mercato.

PARTE SPECIALE “D”

Reati in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

1. OMICIDIO COLPOSO E LESIONI PERSONALI GRAVI E GRAVISSIME IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (ART. 25 *SEPTIES* DEL DECRETO)

L'art. 25 *septies* del Decreto, introdotto dalla L. 23 agosto 2007 n. 123, e sostituito dall'art. 300 del Testo Unico, ha esteso la responsabilità amministrativa dell'Ente anche ai reati di omicidio colposo e lesioni gravi e gravissime, commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

A sua volta il Testo Unico, oltre a riformare e riorganizzare in maniera sistematica la vasta disciplina esistente in materia di tutela della salute e della sicurezza sui luoghi di lavoro, ha dettato alcune norme specifiche in merito alla predisposizione del Modello.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
589 c.p.	Omicidio colposo in violazione dell'art. 55 del Testo Unico	1.000 quote	si, per una durata non inferiore a 3 mesi e non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
589 c.p.	Omicidio colposo	da 250 a 500 quote	si, per un periodo non inferiore a 3 mesi e non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
590 c.p.	Lesioni colpose	personali fino a 250 quote	si, per non più di 6 mesi: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione dei reati per cui è prevista la responsabilità amministrativa.

Omicidio colposo (art. 589 c.p.)

La norma sanziona la condotta di chi cagiona per colpa la morte di una persona. La pena è aggravata, tra l'altro, se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro.

Sotto il profilo della responsabilità dell'Ente, la condotta più grave, e per la quale quindi è previsto un regime sanzionatorio più severo, è l'omicidio colposo determinato dalle violazioni indicate dall'art. 55 comma 2 del Testo Unico (consistenti, sommariamente, nell'omessa redazione o nell'inadeguata redazione del documento di valutazione dei rischi imposto dalla legge in aziende le cui attività sono caratterizzate da particolare pericolosità).

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

La condotta sanzionata è quella di chi cagiona ad altri per colpa una lesione personale, grave o gravissima, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

È opportuno precisare che, ai sensi dell'art. 583 comma 1 c.p., la lesione personale è da considerarsi "grave" se: (i) dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore a 40 giorni; (ii) il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione è invece considerata "gravissima", ai sensi del medesimo art. 583 comma 2 c.p., se dal fatto deriva: (i) una malattia certamente o probabilmente insanabile; (ii) la perdita di un senso; (iii) la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà dell'uso della parola; (iv) la deformazione, ovvero lo sfregio permanente del viso.

2. DESTINATARI DELLA PRESENTE PARTE SPECIALE

In considerazione della finalità delle fattispecie in esame, risulta di tutta evidenza come ogni attività di impresa costituisca un rischio, tanto per chi la esegue quanto per la collettività in generale.

Immediata conseguenza di tali premesse è che devono ritenersi destinatari della presente Parte Speciale, in aggiunta ai Destinatari del Modello:

- tutti i soggetti che svolgono funzioni e ricoprono incarichi in materia di salute e sicurezza nei luoghi di lavoro (a titolo esemplificativo, il datore di lavoro, il RSPP, i responsabili per la sicurezza, i medici competenti, gli addetti alle emergenze, i rappresentanti dei lavoratori per la sicurezza, ecc.);
- i prestatori esterni di servizi che operino all'interno delle aree aziendali (inclusi i lavoratori somministrati o di cooperative che operino presso la Sede della Società);
- altri collaboratori, anche solo occasionali.

3. FINALITÀ DELLA PRESENTE PARTE SPECIALE

Si deve anzitutto evidenziare che i delitti di cui alla presente Parte Speciale, a differenza di tutti gli altri previsti dal Decreto, non consistono in condotte illecite volontarie; essi sono integrati da condotte meramente colpose, e quindi involontarie.

Nel caso di lesioni colpose, quindi, nessuno vuole la realizzazione dell'evento lesivo: esso avviene per causa di un'omissione precedente circa il rispetto delle norme antinfortunistiche determinata da colpa (ossia da negligenza o imprudenza o imperizia), non certo dalla volontà di cagionare quell'evento.

Al fine di conciliare la previsione dei reati di natura colposa (quali quelli in esame) con i criteri dell'interesse e del vantaggio dell'Ente, che costituiscono comunque la fonte e l'origine, nel sistema delineato dal Decreto, della sua responsabilità, la dottrina e soprattutto la giurisprudenza in materia hanno individuato la condotta tipica dei reati qui in esame nel risparmio di costi conseguente alla mancata adozione di misure di sicurezza che avrebbero potuto evitare, se adottate, l'evento (morte o lesioni).

La presente Parte Speciale ha la finalità di descrivere le attività poste in essere da Data Appeal al fine di prevenire questo tipo di reati, attraverso misure organizzative interne che mirino all'assunzione puntuale ed esaustiva di tutti i rimedi e di tutti gli adempimenti imposti dalla normativa di settore per la piena tutela della sicurezza del lavoro e la riduzione al minimo del rischio che si possano verificare omissioni e carenze in questo ambito di attività.

Data Appeal ha adottato, conformemente alle disposizioni del Testo Unico, un proprio Documento di Valutazione dei Rischi. Il documento e le disposizioni ivi contenute costituiscono ovviamente parte integrante della presente Parte Speciale, e gli stessi si devono intendere qui espressamente richiamati.

Nel predisporre il Documento di Valutazione dei Rischi, Data Appeal ha in particolare fornito particolare attenzione alle seguenti attività, nel rispetto delle indicazioni del Testo Unico e della prassi consolidata in materia:

- a) rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici, dispositivi di protezione individuali;
- b) valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti;
- c) organizzazione delle emergenze e del primo soccorso;
- d) gestione degli appalti, con l'organizzazione di riunioni periodiche per il monitoraggio della sicurezza aziendale, e consultazioni del rappresentante dei lavoratori per la sicurezza;
- e) sorveglianza sanitaria;
- f) informazione e formazione dei lavoratori;
- g) vigilanza sul rispetto delle procedure e delle istruzioni affinché il lavoro sia svolto dai lavoratori in sicurezza;
- h) acquisizione di documentazioni e certificazioni obbligatorie di legge;
- i) periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il Documento di Valutazione dei Rischi si propone inoltre espressamente di:

- j) prevedere misure e metodi idonei a monitorare: (i) lo stato complessivo del sistema di tutela della sicurezza da parte di Data Appeal, (ii) la persistente adeguatezza delle misure assunte, e (iii) l'insorgere di nuove esigenze di tutela;
- k) prevedere l'estensione del sistema disciplinare già esistente anche alle carenze, alle omissioni ed alle violazioni in materia antinfortunistica.

L'intento di Data Appeal nella redazione della presente Parte Speciale non è quindi quello di dettare una serie di norme di condotta volte alla prevenzione degli infortuni e degli incidenti, essendo tale complesso di regole già indicato nel Documento di Valutazione dei Rischi di cui la Società è munita,

e che è soggetto a periodica revisione ed aggiornamento. Quello che Data Appeal intende porre in luce in questa Parte Speciale sono piuttosto le regole fondamentali del sistema organizzativo con cui mira a gestire la sicurezza nell'ambito della sua Attività.

La materia, quindi, richiede un approccio non solo normativo, ma anche esecutivo e dinamico, che tenga conto della continua evoluzione dell'organizzazione aziendale, tecnologica e della normativa, con un approccio di costante verifica dell'adeguatezza delle misure in essere.

4. SOGGETTI DEDICATI A COMPITI IN MATERIA DI SICUREZZA

I soggetti che hanno un ruolo per la tutela della sicurezza e della salute del lavoro sono:

1. Datore di lavoro, per i compiti da questo non delegabili;
2. Responsabile del Servizio di Prevenzione e Protezione (RSPP);
3. Medico competente;
4. Rappresentante dei Lavoratori per la Sicurezza (RLS);
5. Lavoratori.

La struttura dell'organizzazione del sistema di prevenzione, all'interno della Società, è la seguente.

Il datore di lavoro è stato individuato con delibera del Consiglio di Amministrazione del 10 maggio 2019 nella figura del sig. Mirko Lalli, già consigliere e nominato Amministratore Delegato con la medesima delibera. Il datore di lavoro adempie ai propri compiti indelegabili con riferimento alla valutazione del rischio e alla designazione del RSPP.

La Società ha poi provveduto ad individuare, conformemente alle disposizioni del Testo Unico, quale RSPP un soggetto esterno, dotato delle competenze e dei poteri necessari per l'assolvimento dei suoi compiti, ed è stato eletto dai lavoratori il Rappresentante dei lavoratori per la sicurezza (RLS).

La Società ha altresì provveduto ad individuare tra i lavoratori i preposti in materia di sicurezza, nonché i componenti delle squadre di emergenza, che sono stati specificamente formati, mediante appositi corsi, per affrontare le varie tipologie di emergenze che possono accadere all'interno delle aree aziendali, e che effettuano esercitazioni periodiche.

Infine, la Società ha proceduto alla nomina del Medico Competente.

Ai soggetti sin qui richiamati devono aggiungersi anche tutti i lavoratori: il contributo conoscitivo, informativo e di vigilanza di tutti i soggetti coinvolti nell'attività dell'impresa è infatti fondamentale per un sistema interno che miri ad una tutela quanto più efficace della sicurezza, anche con riferimento al più rapido e tempestivo rilevamento di eventuali carenze, eventuali punti deboli ed eventuali esigenze di adeguamento, in caso di modifiche organizzative.

5. POLITICA AZIENDALE DELLA SICUREZZA

Data Appeal considera la tutela della salute e della sicurezza non semplicemente un obbligo di legge, ma un dovere morale.

La tutela della sicurezza del luogo di lavoro, il rifiuto di sottoporre i propri dipendenti a condizioni di lavoro stressanti, la garanzia di un luogo di lavoro sicuro, sono principi da sempre perseguiti dalla Società, e sono espressamente sanciti anche dal suo Codice Etico.

Conformemente a tali principi, nell'esercizio della propria Attività, la Società persegue pertanto i seguenti obiettivi:

1. diminuzione nel tempo della frequenza e della gravità dei fenomeni infortunistici e delle malattie professionali, al minimo livello tecnicamente raggiungibile;
2. adozione, in ogni scelta tecnica ed organizzativa, delle misure di prevenzione e protezione necessarie per eliminare i rischi, o comunque per ridurli a livelli accettabili;
3. mantenimento nel tempo dei livelli di sicurezza desiderati, compatibilmente con il mantenimento di una gestione ottimale dei costi della sicurezza, anche attraverso l'impiego efficiente e pianificato delle risorse umane, tecnologiche e materiali in possesso dell'impresa.

A tal fine, Data Appeal si impegna, tra l'altro, anche nel costante aggiornamento degli strumenti e delle tecnologie messe a disposizione dei propri dipendenti per l'esercizio delle attività aziendali.

Per perseguire gli obiettivi che caratterizzano la propria politica aziendale in materia di tutela della salute e della sicurezza, la Società si impegna a:

4. rispettare la normativa vigente e ad adeguarsi ai futuri aggiornamenti, modifiche ed integrazioni;
5. assicurare comprensione, attuazione e sostegno della propria politica a tutti i livelli aziendali al fine di garantire la partecipazione al sistema in funzione delle proprie competenze e responsabilità, nella consapevolezza che per il raggiungimento degli obiettivi indicati è necessario l'impegno di tutti;
6. valorizzare la formazione e l'opera di tutte le persone direttamente impegnate nella tutela della salute e della sicurezza dei lavoratori, con la consapevolezza che il perseguimento degli obiettivi indicati necessita di idonee competenze tecniche e gestionali;
7. valorizzare le competenze specifiche in materia di tutti i lavoratori, fornendo ad essi la necessaria informazione e formazione sui rischi e sulle misure di eliminazione o riduzione degli stessi, riconoscendo che i principali artefici del miglioramento dei livelli di sicurezza in azienda sono i lavoratori stessi;
8. pretendere da parte di tutto il personale che opera in azienda, interno ed esterno, il rispetto della vigente normativa in materia di salute e sicurezza sul lavoro, nonché di tutte le disposizioni interne che l'azienda ha stabilito o stabilirà, con l'obiettivo di migliorare e mantenere i livelli di sicurezza;
9. garantire ai propri dipendenti il costante adeguamento delle attrezzature, e dei dispositivi di protezione individuale, con la consapevolezza che l'aggiornamento delle apparecchiature in uso ai dipendenti per l'esercizio delle Attività, sulla base degli adeguamenti tecnico scientifici, contribuisce al raggiungimento degli obiettivi perseguiti in materia dalla Società;
10. promuovere l'applicazione delle norme di tutela della salute e della sicurezza anche mediante richiesta che ogni dipendente segnali eventuali carenze o anomalie di funzionamento di macchine, attrezzature di lavoro o dispositivi di sicurezza, che possano causare dei danni alla salute ed alla sicurezza dei lavoratori, nonché eventuali violazioni alle vigenti disposizioni normative ed alle disposizioni interne.

6. PIANIFICAZIONE E ORGANIZZAZIONE DEL SISTEMA

Per dare attuazione concreta ai principi della propria politica di sicurezza, Data Appeal:

11. indica ai soggetti coinvolti nell'attività aziendale regole di comportamento sia generali che specifiche, con riferimento a particolari attività;
12. valuta costantemente i rischi esistenti con riferimento alle diverse attività aziendali;
13. prende in considerazione, ponendovi grande attenzione e stabilendo le procedure del caso, anche i casi e le situazioni che eccedono l'ordinaria attività aziendale.

7. PRINCIPI E REGOLE DI CONDOTTA GENERALI

La Società ha già adottato da tempo una serie di regole di condotta generali che devono in ogni caso caratterizzare il comportamento di tutti indistintamente i soggetti coinvolti nelle attività dell'azienda.

Data Appeal si attiene anzitutto - e chiede a tutti i Destinatari della presente Parte Speciale, per quanto di competenza, che si attengano - ai seguenti principi generali:

- rigoroso rispetto di tutta la normativa in materia di salute e sicurezza nei luoghi di lavoro e realizzazione di un efficace, idoneo e competente sistema per la gestione, l'esecuzione e l'aggiornamento delle attività e delle misure relative;
- redazione e diffusione di regolamenti e comunicazioni interne, recanti informazione ed istruzioni circa i comportamenti e le cautele che devono essere adottati dai lavoratori;
- identificazione e delimitazione, all'interno dell'azienda, delle aree di particolare pericolo per la sicurezza;
- predisposizione di procedure interne che prevedano il periodico aggiornamento del Documento di Valutazione dei Rischi, e la necessità del suo aggiornamento in caso di rilevanti modifiche organizzative delle attività di lavoro o di modifiche legislative della normativa in materia;
- adozione di procedure interne per il caso di emergenza, evacuazione ed incendio;
- conferimento di deleghe al responsabile per la sicurezza, ed eventuali subdeleghe di questi ad altri soggetti dell'organizzazione aziendale, in forma scritta e sufficientemente dettagliata;
- riconoscimento al RSPP di tutti i poteri per l'effettivo esercizio dell'attività di vigilanza e di prevenzione;
- adempimento di tutti gli obblighi di formazione ed informazione previsti dal Testo Unico;
- tutela delle segnalazioni di eventuali anomalie relative a fasi di lavoro o strumenti di lavoro che si presentino rischiosi o carenti dal punto di vista della tutela della sicurezza sul lavoro garantendo idonei canali informativi che abbiano come destinatari il datore di lavoro e il RSPP;
- verifica costante del rispetto delle norme in materia di sicurezza da parte anche di fornitori, prestatori d'opera e di servizi ed ogni altro soggetto terzo,

nell'esecuzione di opere e nella prestazione di servizi a favore della Società in ogni caso in cui vi sia un rischio da interferenze;

- valutazione dei rischi chimici, da rumori, da vibrazioni, nonché dei nuovi ed ulteriori rischi indicati e previsti dal Testo Unico (quali, a titolo esemplificativo, lo stress da lavoro correlato);
- verifiche periodiche sulla *compliance* aziendale in materia di sicurezza nei luoghi di lavoro e sul rispetto degli standard fissati a livello aziendali e delle regole di comportamento interne. Le informazioni raccolte in sede di tale indagine dovranno poi condivise con il *management* della Società.

In aggiunta ai principi generali sopra elencati, la Società impone espressamente a tutti i Destinatari l'obbligo di porre in essere le seguenti condotte:

- rispettare rigorosamente ogni norma di legge in materia di sicurezza sul lavoro, di igiene e di tutela della salute dei lavoratori;
- rispettare, con lo stesso rigore, ogni regolamento ed ogni disposizione interna relativi alle stesse materie;
- seguire scrupolosamente le indicazioni ed i divieti eventualmente presenti su cartelli e comunicazioni interne;
- impiegare, secondo quanto previsto da manuali di istruzione, indicazioni del produttore, indicazioni dell'azienda ecc., tutti i dispositivi di protezione presenti in azienda;
- rispettare le delimitazioni di aree di lavoro ritenute pericolose, accedendovi solo se autorizzati;
- partecipare ai corsi di formazione, di aggiornamento ed alle esercitazioni periodiche in tema di sicurezza organizzate dalla Società ed attenersi alle informazioni e ai documenti informativi relativi alla sicurezza sul lavoro ricevute da superiori e preposti;
- non impiegare strumenti di lavoro o di protezione diversi da quelli forniti dall'azienda.

Con riferimento al RSPP e al Datore di lavoro, spetta loro, secondo le relative competenze:

- garantire un monitoraggio periodico e costante dei rischi emergenti, che consenta un continuo aggiornamento della valutazione dei rischi, in modo che sia sempre aggiornata e attualizzata a nuovi profili di rischio;
- far sì che i risultati del monitoraggio si traducano: (i) nell'assunzione di nuove ed idonee misure di sicurezza e nel miglioramento di quelle esistenti; (ii) quando necessario, in appositi documenti cui sia data corretta diffusione in azienda tra i soggetti interessati; (iii) nell'emissione delle necessarie direttive ed istruzioni che siano diffuse presso i soggetti interessati;
- curare che la valutazione dei rischi si fondi su criteri obiettivi, in linea con la letteratura scientifica in materia;
- garantire che la valutazione dei rischi e la predisposizione di linee guida, di regolamenti e di documenti informativi interni tenga sempre conto anche di ipotetiche situazioni di emergenza, oltre che dell'attività ordinaria;

- ricevere le segnalazioni dei lavoratori, in materia di sicurezza del lavoro, provvedere alla loro evasione e alla puntuale verifica dei fatti segnalati, nonché alla trasmissione al RSPP per l'archiviazione;
- riferire immediatamente all'Organismo di Vigilanza l'esistenza di anomalie, di situazioni di rischio, così come di segnalazioni di rilievo, tra quelle eventualmente effettuate da singoli lavoratori;
- riunirsi periodicamente, al fine di coordinare le rispettive attività e azioni da intraprendere;
- proporre l'assunzione di sanzioni disciplinari nei confronti degli esponenti aziendali che non rispettano le norme di legge e regolamento o le disposizioni interne in materia di sicurezza sul lavoro.

8. REGOLE DI COMPORTAMENTO SPECIFICHE

Le norme sopra elencate sono integrate da ogni altra disposizione emessa da ciascuno dei soggetti cui sono affidati compiti e funzioni in tema di sicurezza, con appositi documenti, che contengano ogni istruzione necessaria al compimento di specifiche attività o all'uso di specifici strumenti.

Anzitutto, e conformemente alle disposizioni di cui al Testo Unico, Data Appeal ha provveduto ad effettuare la valutazione dei rischi relativamente alle attività svolte all'interno della propria Sede.

I risultati di tale analisi, unitamente alle procedure predisposte ai fini dell'eliminazione, o quanto meno della riduzione dei rischi, sono confluite nel Documento di Valutazione dei Rischi, predisposto conformemente a quanto previsto dal Testo Unico, e che si articolano in diverse sezioni, aventi ad oggetto, tra l'altro: (i) l'individuazione dei pericoli presenti in azienda; (ii) l'indicazione delle misure di prevenzione e di protezione attuate a seguito della valutazione dei rischi; (iii) il programma per il miglioramento nel tempo dei livelli di sicurezza.

Al Documento di Valutazione dei Rischi si aggiunge poi tutta la documentazione predisposta in materia di sicurezza, relativa, a titolo esemplificativo, alle certificazioni relative agli impianti, ai videoterminali (siano essi utilizzati negli spazi comuni o in *smartworking*), ai manuali per la gestione delle emergenze predisposti per le infrastrutture di Nana Bianca e applicabili anche alla Società, in virtù del contratto di coworking con Nana Bianca, alla procedura dettata per lo *smartworking*.

Tra i documenti sopra citati devono essere ricordati i piani di emergenza, che disciplina le attività da compiere e le misure da adottare in caso di emergenze, quali incendio, evacuazione, e primo soccorso, e le schede di formazione del personale, che registrano e attestano gli incontri formativi predisposti in caso di nuova assunzione e di impiego in differenti mansioni, nonché gli ulteriori incontri destinati in generale all'aggiornamento di tutto il personale.

La documentazione sopra illustrata è, in parte, predisposta da Nana Bianca, condivisa con la Società e comunque conservata presso le infrastrutture di Nana Bianca. In riferimento al DVR, esso è conservato presso la sede sociale.

In tutti i casi, la documentazione in esame è a disposizione di chiunque vi abbia titolo per la consultazione in ogni momento.

9. VALUTAZIONE DEI RISCHI ESISTENTI

Presupposto necessario ed imprescindibile per un'efficace attività di prevenzione dei rischi per la salute e per la sicurezza del lavoro è un'effettiva, approfondita e continuativa rilevazione e valutazione dei rischi esistenti nell'organizzazione aziendale.

Data Appeal ha ben presente il problema e si impegna ad adeguarsi costantemente alle disposizioni introdotte dal Testo Unico.

L'Attività di Data Appeal, per quanto riguarda il profilo della sicurezza, consiste esclusivamente in attività di ufficio, con la conseguenza che per la Società risulta quanto mai ridotto il rischio della commissione di uno dei reati di cui alla presente Parte Speciale.

Pertanto la Società è ben consapevole che la redazione dei documenti previsti dal Testo Unico non esaurisce il compito in vista della tutela della salute e della sicurezza dei lavoratori: decisivo è, per l'appunto, che ad una costante e continuativa attività di valutazione - sempre pronta a rilevare nuove aree di rischio rese evidenti da nuove conoscenze tecnico-scientifiche o conseguenti a modificazioni dell'attività aziendale (nuovi procedimenti e metodi di lavoro, nuove sedi di lavoro, e nuove modalità di esecuzione del lavoro, ecc.), così come a verificare elementi di carenza e di insufficienze nelle misure già esistenti – si accompagni una puntualità negli interventi che tale valutazione renda di volta in volta necessari o anche solo opportuni. Sotto tale profilo, il Documento di Valutazione dei Rischi prevede, tra l'altro, una revisione generale delle valutazioni in esso contenute ogni qual volta intervengano modifiche e/o nuovi fattori di rischio conseguenti ad aggiornamenti e/o variazioni dell'attività e del progresso tecnico.

Altro profilo fondamentale è dato dalla valutazione di eventuali rischi sanitari. Ruolo fondamentale, al riguardo, è ovviamente svolto dal Medico Competente e dall'archivio della documentazione medica. Sotto tale profilo, l'analisi condotta ha comunque permesso di pervenire ad esiti rassicuranti, non essendosi mai verificati infortuni a carico dei lavoratori.

Si segnala che in ragione dell'insorgenza dell'emergenza sanitaria legata alla diffusione del virus da Sars-Cov-9 (cd. "Coronavirus" e malattia "Covid-19"), la Società ha proceduto all'analisi del rischio cd. biologico, ovvero il rischio descritto come connesso alla possibilità di sviluppare una malattia, generalmente di tipo infettivo, a seguito dell'esposizione ad agenti biologici. La Società ha pertanto provveduto a una revisione generale del DVR, effettuata congiuntamente dal CEO nonché datore di lavoro, dal RSPP, dal RLS e dal Medico Competente, nella versione adottata in data 20 maggio 2020, predisponendo una serie di misure (utilizzo di dispositivi di protezione, regole di distanziamento, regole di cautela generale), al fine di limitare e/o ridurre al minimo il rischio da contagio da COVID-19.

Nell'elaborazione della revisione in questione, la Società ha preso in considerazione: (i) le istruzioni del Ministero della Salute e dell'Organizzazione Mondiale della Sanità; (ii) le informazioni sulle misure di prevenzione igienico-sanitarie di cui all'Allegato 11 del D.P.C.M. 17/05/2020, nonché (iii) il Protocollo condiviso tra il Governo e le parti sociali di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro.

Coerentemente con le linee guida nazionali, la Società ha adottato nella maggior misura possibile il lavoro da remoto (o cd. *smart-working*).

La Società ha inoltre predisposto nella propria Sede i necessari dispositivi di protezione, effettuato una specifica formazione ai propri dipendenti e predisposto, in maniera integrata al DVR, delle procedure per la gestione del contagio.

10. CASI PARTICOLARI E/O STRAORDINARI RISPETTO ALL'ATTIVITÀ AZIENDALE ORDINARIA

Ulteriore elemento decisivo per un'efficace prevenzione è che essa fondi le proprie misure e le proprie iniziative non solo sull'esame dell'ordinaria attività, ma anche sui casi e sulle situazioni che da essa esulino: sono proprio i casi in cui ad essere coinvolti siano soggetti non direttamente appartenenti all'organizzazione di persone della Società, o che riguardino situazioni in senso lato di emergenza quelli che portano con sé i maggiori rischi di attività che si rivelano pericolose o di un abbassamento del livello delle cautele di prevenzione.

Per questa ragione, Data Appeal ha analizzato i rischi (ed a redigere i relativi documenti di valutazione) anche con riferimento a casi di emergenza di vario genere, con eventuale esigenza di attivare le squadre di primo soccorso e lotta antincendio.

In aggiunta, gli addetti alle emergenze sono stati altresì sottoposti a specifica formazione in materia. Informazioni sul piano di emergenza interno sono inoltre collocate nelle varie aree aziendali attraverso appositi pannelli informativi destinati a dipendenti e ad eventuali visitatori.

11. DOCUMENTAZIONE E VERBALIZZAZIONE DELLE ATTIVITÀ

Altri aspetti fondamentali del sistema di gestione interno della sicurezza sono la registrazione e la verbalizzazione delle principali attività compiute, con la conseguente loro tracciabilità, quanto a soggetti coinvolti e contenuti. La tracciabilità delle attività svolte garantisce una forma di autocontrollo sulle stesse e consente una più agevole lettura di insieme dell'attività aziendale di tutela della salute e della sicurezza del lavoro.

Tutti i soggetti che ricoprono ruoli rilevanti in materia sono dunque tenuti a procedere alla verbalizzazione, seppure in via sintetica, dello svolgimento delle principali attività (riunioni, emissione di nuove direttive e circolari ecc.).

Data Appeal ha già previsto la verbalizzazione e documentazione delle attività di formazione ed informazione tanto dei lavoratori già esperti, quanto dei lavoratori neoassunti e di quelli cui siano state assegnate nuove e differenti mansioni

Allo stesso modo, Data Appeal ha già proceduto a descrivere dettagliatamente su supporto documentale tutte le procedure previste in materia di salute e sicurezza nei luoghi di lavoro, tanto per quanto attiene allo svolgimento ordinario dell'attività lavorativa, quanto per la gestione dei casi eccezionali e di emergenza (incendi, primo soccorso, ecc.).

Tali procedure vengono portate debitamente a conoscenza dei lavoratori attraverso le procedure di informazione e formazione loro destinate e la consegna degli appositi materiali informativi.

Altro aspetto fondamentale, per un'effettiva ed efficace gestione della sicurezza del lavoro, è la raccolta, la tenuta e la conservazione di tutti i documenti interni, le direttive, i regolamenti, le norme di condotta diffuse presso i lavoratori.

La documentazione così conservata deve ritenersi accessibile per ogni soggetto avente titolo che lo richieda.

12. DIVULGAZIONE, INFORMAZIONE E FORMAZIONE

Aspetto fondamentale per un'efficace attività di tutela della salute e della sicurezza sul lavoro è costituito dalla previsione di ogni iniziativa utile a garantire forme efficaci ed esaustive di formazione ed informazione dei dipendenti e di ogni altro soggetto interessato sui temi necessari perché ciascuno abbia ogni conoscenza utile per tenere la migliore e più sicura condotta in ogni occasione.

Si è poi già detto dell'importanza fondamentale, per un'effettiva e quanto più efficace prevenzione in materia di sicurezza, della collaborazione di tutti i soggetti coinvolti nell'attività aziendale.

Decisiva al riguardo è l'esistenza di un costante scambio d'informazioni tra tutti i soggetti aziendali interessati alla tutela della salute e della sicurezza del lavoro.

Data Appeal, con il possibile contributo del RSPP e del Datore di Lavoro, stabilisce le forme ed i modi per garantire:

- l'efficace formazione ed informazione dei lavoratori e di tutti gli altri soggetti coinvolti nell'attività aziendale;
- il contributo conoscitivo e di esperienza da parte dei lavoratori, quotidianamente impiegati nelle attività aziendali.

Quanto al primo punto, sono state già svolte e sono periodicamente pianificate attività di:

- formazione collettiva *una tantum* o su base periodica (riunioni periodiche per i lavori già in servizio);
- formazione individuale, all'ingresso in azienda ed in ogni caso di cambio di mansioni ;.

Quanto al secondo punto, invece, Data Appeal prevede forme di coinvolgimento sulla base di:

- riunioni periodiche con i lavoratori ed i loro rappresentanti;
- possibilità di segnalazioni di disfunzioni e carenze attraverso idonei canali di comunicazione destinati al RSPP.

Delle attività di formazione ed informazione dei lavoratori deve essere data prova scritta, su apposita documentazione, che deve essere sottoscritta dal lavoratore interessato.

Sia della documentazione relativa alla formazione, sia delle segnalazioni ricevute, è tenuta raccolta presso la sede della Società.

13. CONTROLLO E RIVALUTAZIONE DEL SISTEMA DI SICUREZZA INTERNO

L'azione aziendale in tema di sicurezza sul lavoro deve essere dinamica e continuativa, per garantire la possibilità di un costante ed efficace aggiornamento delle misure di tutela.

A tal proposito, è fondamentale che un'azienda non solo adotti tutte le misure necessarie per la tutela della sicurezza nei luoghi di lavoro, ma che essa provveda anche al controllo ed alla vigilanza sulla tutela, così come il mantenimento di un loro livello ottimale e della loro efficacia.

Questo controllo si deve svolgere su un doppio livello:

- primo livello: costante e continuativo, insito nell'azione dei soggetti aziendali con compiti in tema di sicurezza, che devono svolgere la propria attività rispettando scrupolosamente tutte le norme contenute nella presente Parte Speciale e tenendo sempre presente l'efficacia delle loro iniziative e la reale tutela di ogni aspetto rilevante della sicurezza;
- secondo livello: riesame interno attraverso forme di rivalutazioni e controlli periodici, svolti da controllori interni o consulenti esterni.

Con riferimento a questo secondo profilo, Data Appeal ha già previsto nel proprio Documento di Valutazione dei Rischi la sua periodica revisione.

PARTE SPECIALE “E”

Reati contro il patrimonio commessi mediante frode

1. LA TIPOLOGIA DEI REATI DI RICETTAZIONE, RICICLAGGIO, REIMPIEGO DI DENARO, BENI O ALTRE UTILITÀ, AUTO – RICICLAGGIO (ART. 25 *OCTIES* DEL DECRETO)

L'art. 25 *octies* è stato inserito nel Decreto dal d.lgs. 21 novembre 2007 n. 231 di “Attuazione della direttiva 2005/60/Ce concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio di proventi di attività criminose e di finanziamento del terrorismo, nonché della direttiva 2007/70/CE che ne reca misure di esecuzione”, e prevede la responsabilità amministrativa dell'Ente per i reati di 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.); a queste fattispecie è stata più di recente aggiunta anche quella di autoriciclaggio (art. 648 *ter1* c.p.).

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
648 c.p.	Ricettazione	da 200 a 800 quote	sì, per non più di 2 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
648 <i>bis</i> c.p.	Riciclaggio	da 200 a 800 quote	sì, per non più di 2 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
648 <i>ter</i> c.p.	Impiego di denaro, beni o utilità di provenienza illecita	da 200 a 800 quote	si, per non più di 2 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
648 <i>ter</i> 1 c.p.	Autoriciclaggio	da 200 a 800 quote	si, per non più di 2 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
--	--	--	---

La sanzione pecuniaria è aumentata da 400 a 1.000 quote nel caso in cui il denaro, i beni o le altre utilità provengano da un delitto per il quale è stabilita la pena della reclusione superiore nel massimo a 5 anni.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

Ricettazione (art. 648 c.p.)

Il reato si configura quando un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto o, comunque, si intromette nel farli acquistare, ricevere od occultare.

Il reato si configura solo nel caso in cui l'agente non abbia preso parte al delitto originario, dal quale è derivato il provento (c.d. "delitto presupposto").

Per acquisto si deve intendere ogni negozio, oneroso o gratuito, idoneo al trasferimento della cosa nella sfera patrimoniale dell'acquirente.

Per ricezione deve intendersi ogni conseguimento di possesso del bene proveniente dal delitto, anche se solo temporaneamente o per mera compiacenza.

L'occultamento, infine, si attua con la semplice attività di nascondere il bene proveniente da delitto.

La ricettazione, inoltre, può realizzarsi in tutti i casi in cui vi sia un'intromissione nell'acquisto, nella ricezione o nell'occultamento della cosa.

In quest'ultimo caso, il delitto si consuma per il solo fatto di essersi il colpevole intromesso allo scopo di fare acquistare, ricevere od occultare la cosa di provenienza delittuosa, senza che sia necessario che l'intromissione abbia raggiunto il fine propostosi dall'agente.

Per espressa disposizione dell'art. 648 comma 3 c.p., la ricettazione ricorre anche quando l'autore del delitto da cui il denaro o le cose provengano, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità.

Riciclaggio (art. 648 *bis* c.p.)

La norma punisce chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo tale da ostacolare l'identificazione della loro provenienza delittuosa.

La condotta criminosa può quindi configurarsi in due modi distinti:

- i. nel sostituire o trasferire denaro, beni e altre utilità provenienti da delitto non colposo (è il caso di chi, ad esempio, esporta all'estero denaro o valori e li cambi con moneta o valori diversi);
- ii. nel compiere operazioni su denaro, beni ed altre utilità.

in entrambi i casi, per costituire reato, la condotta sopra descritta deve essere finalizzata allo scopo di ostacolare l'identificazione della provenienza delittuosa dei beni.

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

Il reato si configura nel caso in cui, fuori dei casi di ricettazione e riciclaggio, qualcuno impieghi consapevolmente in attività economiche o finanziarie beni o altre utilità provenienti da delitto.

Il delitto in esame ha un duplice scopo: impedire che il cd. "denaro sporco", frutto dell'illecita accumulazione venga trasformato in denaro "pulito", ed evitare che il capitale così "ripulito" venga legittimamente utilizzato.

La condotta punibile è descritta con il verbo "impiegare", che non ha una precisa valenza tecnica e finisce con l'avere una portata particolarmente ampia, potendosi intendere qualunque forma di utilizzazione di denaro beni o altre utilità provenienti da delitto indipendentemente da qualsiasi risultato utile per l'agente.

La norma prevede una circostanza aggravante, con conseguente aumento di pena, nel caso in cui il fatto sia commesso nell'esercizio di attività professionale.

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

Il reato, che ha avuto ingresso nel nostro ordinamento negli anni più recenti, consiste nell'attività di occultamento dei proventi derivanti da crimini propri.

In particolare, la condotta sanzionata è quella di chi - avendo commesso o concorso a commettere un delitto non colposo - impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

A seguito dell'introduzione del reato in esame è divenuto possibile perseguire le condotte di "pulizia" di proventi da reato anche quando attuate dallo stesso autore del delitto presupposto.

Dal novero delle condotte punibili sono escluse solo quelle per cui il denaro, i beni o le altre utilità vengano destinate alla mera utilizzazione o al godimento personale.

L'oggetto del reato è costituito dal denaro ovvero da qualsiasi altro bene od utilità proveniente da delitto non colposo.

2. VALUTAZIONE DELLE AREE DI RISCHIO

In considerazione del fatto che la finalità dichiarata della previsione dei reati qui in esame è quella di evitare che il sistema finanziario venga utilizzato al fine di riciclare i proventi di attività criminose (sotto forma di denaro o di altre utilità), è evidente che costituiscono aree a rischio, all'interno di qualsiasi realtà aziendale, i processi finanziari e contabili e, in generale, il ciclo attivo e quello passivo. A queste devono poi aggiungersi tutte le attività relative ai rapporti instaurati dalla Società con soggetti terzi, fornitori di beni e/o servizi e clienti. L'inserimento tra i Reati Presupposto qui in esame anche del reato di autoriciclaggio, che consiste in estrema sintesi nel reimpiego di denaro o altre utilità provenienti da un reato "proprio", ossia commesso direttamente dall'Ente, comporta necessariamente l'inclusione, tra le aree di rischio, anche delle attività nel cui ambito potrebbero essere commessi anche gli altri Reati Presupposto per i quali è prevista la responsabilità dell'Ente, e da cui potrebbe derivare, come conseguenza, il reimpiego del prodotto o del profitto di quel Reato Presupposto.

Si deve però tenere presente che, ai sensi del Decreto, i criteri cardine per l'individuazione della responsabilità amministrativa a carico dell'Ente rimangono pur sempre l'interesse e il vantaggio della società, di modo che la responsabilità potrà essere esclusa in tutti i casi in cui la commissione del reato, seppure all'interno della Società e da parte di suoi dipendenti o comunque esponenti, sia finalizzata al perseguimento di un interesse o di un vantaggio meramente personale.

Con specifico riferimento alla realtà di Data Appeal, si può osservare che la stessa ha adottato delle procedure relativamente al ciclo attivo e a quello passivo che prevedono il coinvolgimento ed il controllo, sia in fase di autorizzazione dei pagamenti e relativa esecuzione attraverso il sistema bancario, sia in fase di verifica della provenienza dei pagamenti ricevuti, da parte di almeno due soggetti, appartenenti a due funzioni distinte all'interno della Società.

Il sistema di contabilità interno, come già precedentemente illustrato, prevede la chiusura mensile dei conti, con eventuale loro riallineamento, da parte della funzione *Finance* della Società, e ciò consente anche la verifica ed il monitoraggio costante dei flussi finanziari, e la loro adeguatezza e congruità rispetto ai rapporti conclusi dalla Società nel periodo di riferimento. Ad ulteriore garanzia e tutela dei controlli sui dati contabili, le chiusure mensili dei conti vengono sottoposte all'esame e al vaglio del Consiglio di Amministrazione, con la medesima cadenza mensile.

Data Appeal si avvale in via esclusiva dei fornitori indicati e censiti nel sistema di contabilità aziendale (c.d. fornitori approvati) e con la maggior parte di questi intrattiene rapporti commerciali consolidati da tempo. Il fornitore è considerato approvato quando ha già eseguito con successo una fornitura nei confronti di Data Appeal, secondo la procedura debitamente predisposta, ed è registrato nell'elenco dei fornitori disponibile in azienda.

In caso invece si debba selezionare un fornitore "nuovo", si dovrà seguire la specifica procedura adottata dalla Società per la selezione di fornitori con cui la Società non abbia intrattenuto rapporti in precedenza, e che prevede l'impulso da parte della funzione che ne ha necessità e quindi si fa promotrice dell'iniziativa; tale richiesta (cd. "*request for proposal*"), indirizzata a CFO deve contenere i seguenti elementi: chiara esposizione dei requisiti e necessità da soddisfare tramite la fornitura; richiesta per quotazione economica che copra tutti gli aspetti della fornitura, compresi eventuali extra, costi accessori e manutenzioni; ove praticabile, la richiesta di fornire una prova delle capacità di realizzare la fornitura richiesta (può trattarsi di una demo o *proof of concept*, della richiesta di esecuzione di un progetto teorico o di semplici referenze da clienti).

La valutazione dell'offerta viene effettuata su un elenco di almeno 3 nominativi di possibili fornitori, e sulla base di criteri tecnici ed economici, congiuntamente dal responsabile della funzione che ne ha la necessità e dal CFO.

La fase di contrattualizzazione avviene seguendo la procedura prevista e con l'utilizzo, per quanto possibile, degli standard contrattuali predisposti dalla Società nonché esplicitando, nel modo più esaustivo possibile, l'oggetto, le tempistiche di esecuzione nonché le modalità di fatturazione.

La *Business function* responsabile della fornitura effettua costanti verifiche durante l'arco della fornitura, informando il CFO, attraverso reportistica tracciabile la chiusura della fornitura, secondo quanto previsto nella relativa procedura.

Al termine di ogni prestazione da parte di un nuovo fornitore, nonché nell'ambito di un processo di revisione periodica delineato nella procedura la *business function* di riferimento e/o il dipartimento che si è avvalso di tale fornitore e/o del servizio, scrive una scheda di valutazione con la finalità di fornire una recensione, non solo qualitativa, del servizio reso. Nella formalizzazione del giudizio la *business function* che tiene conto: (i) della corretta evasione dell'ordine rispetto alle modalità concordate, (ii) della conformità tecnica di quanto realizzato o consegnato rispetto a quanto richiesto, (iii) del rispetto dei tempi e dei costi concordati, (iv) della correttezza del rapporto: tempestività, proattività, professionalità dell'interazione durante il rapporto di fornitura, (v) del rispetto delle formalità documentale (ad esempio, la corretta messa a disposizione nei tempi previsti o concordati della documentazione legale, fiscale o comunque richiesta dal cliente). Tale giudizio, comunicato al CFO e archiviato in apposita sezione del *file system* aziendale, consente, ove positivo, l'inserimento del fornitore nella lista dei fornitori cd. approvati.

3. PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE A RISCHIO

Nell'espletamento di ogni attività nell'ambito aziendale, e più specificamente nello svolgimento delle attività considerate a rischio, i Destinatari dovranno attenersi ai principi indicati nel Codice Etico, nonché alle procedure (quali, in via esemplificativa, quelle relative al ciclo attivo e a quello passivo), adottate dalla Società.

In particolare, la Società impone a tutti i Destinatari di attenersi ai seguenti principi generali di condotta:

- astenersi da comportamenti tali da integrare le fattispecie di reato sopra descritte;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- astenersi dal procedere a qualsivoglia transazione ed operazione relativa a somme di denaro o beni, qualora vi siano, nelle circostanze dell'operazione o nelle caratteristiche della controparte, elementi che lascino supporre la provenienza illecita dei beni e del denaro in questione (a titolo esemplificativo, prezzo notevolmente sproporzionato rispetto ai valori medi di mercato)
- tenere un comportamento corretto, trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di collaboratori, fornitori, clienti e partner commerciali, anche stranieri;
- rifornirsi di beni e servizi solo attraverso il ricorso ai fornitori selezionati dalla Società che siano inseriti nell'anagrafica dei fornitori, ovvero, in alternativa, attenersi scrupolosamente alla procedura adottata per la selezione di nuovi fornitori nel caso in cui per il bene e/o servizio sia necessario ricorrere ad un fornitore con cui la Società non ha ancora intrattenuto rapporti commerciali;

- monitorare in maniera continuativa l'operato dei fornitori, anche attraverso i *feed back* inseriti nella scheda di valutazione del fornitore, segnalando anche all'Organismo di Vigilanza eventuali condotte potenzialmente a rischio o anche solo anomale;
- non intrattenere rapporti commerciali con soggetti dei quali sia conosciuta o sospettata l'appartenenza diretta od indiretta ad organizzazioni criminali o comunque operanti al di fuori della liceità;
- in ogni caso, verificare l'attendibilità commerciale e professionale dei nuovi fornitori e/o partner commerciali, con cui la Società in precedenza non abbia mai intrattenuto alcun rapporto, e che non rientrano nell'anagrafica dei fornitori della Società, sulla base degli indicatori di anomalia forniti dalla normativa in materia di antiriciclaggio, quali dati pregiudizievoli pubblici (protesti, procedure concorsuali), acquisendo informazioni commerciali sull'azienda, sui soci e sugli amministratori (i.e. certificazione anti mafia), ed estendendo anche ai nuovi fornitori/partner commerciali le valutazioni sui fornitori che la Società periodicamente effettua a campione;
- effettuare le medesime operazioni previste al punto che precede anche in occasione dell'avvio di nuovi rapporti commerciali con soggetti con cui la Società in precedenza non ha mai intrattenuto alcun tipo di rapporto;
- registrare ogni movimentazione bancaria nei sistemi informativi utilizzati da Data Appeal al fine di consentirne comunque il controllo periodico e la relativa registrazione contabile di tali dati;
- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- effettuare un costante monitoraggio dei flussi finanziari aziendali, attraverso il rispetto delle procedure in uso all'interno della Società, che prevedono in ogni caso la verifica della corrispondenza tra il soggetto beneficiario/autore del pagamento e la documentazione contabile relativa, attraverso il coinvolgimento e il controllo di almeno due soggetti.

È fatto divieto in particolare di:

- acquistare beni o servizi verso un corrispettivo palesemente inferiore al valore di mercato di tali beni o servizi, senza avere prima effettuato le necessarie verifiche sulla loro provenienza;
- effettuare il trasferimento di denaro, beni o altre utilità quando vi sia sospetto che essi provengano da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita degli stessi beni;
- acquistare beni o servizi da fornitori che non siano registrati nell'anagrafica della Società. Per eventuali acquisti di beni o servizi da fornitori "nuovi" sarà necessario procedere alle verifiche preventive sopra indicate;
- effettuare o ricevere pagamenti in contanti, salvo che si tratti di somme non solo al di sotto dei limiti di legge, ma anche di modico valore;
- effettuare operazioni che possano apparire volte a mascherare l'origine illecita di denaro, beni, altre utilità o di autoveicoli;

- effettuare operazioni che possano apparire volte a rimettere i capitali o autoveicoli, oggetto di riciclaggio, nel sistema economico.

4. REGOLE DI COMPORTAMENTO PARTICOLARI, RELATIVE ALLE SINGOLE AREE DI RISCHIO

Al fine dell'attuazione delle regole elencate al precedente capitolo, devono rispettarsi, oltre ai principi contenuti nella Parte Generale del presente Modello, le seguenti regole:

- identificare le controparti commerciali verificandone l'identità a mezzo di documenti, dati e informazioni di fonte affidabile, con la sola esclusione delle vendite effettuate tramite il Sito della Società e con la Pubblica Amministrazione, ove vengono raccolte le sole informazioni necessarie alla fornitura del servizio, e l'utente/cliente viene identificato sulla base delle informazioni che lo stesso fornisce
- raccogliere informazioni sulle controparti commerciali sufficienti per comprendere pienamente la natura delle sue attività;
- verificare l'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata che tengano conto della sede legale della società controparte (ad esempio paradisi fiscali, Paesi a rischio terrorismo), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- tutte le operazioni di natura commerciale e finanziaria derivanti da rapporti continuativi con soggetti terzi devono essere precedute da un'adeguata attività di verifica volta ad accertare l'assenza del rischio di coinvolgimento nella commissione dei reati di riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita, attraverso una chiara identificazione della controparte e della natura dell'operazione;
- i contratti con i fornitori ed i partner devono essere definiti per iscritto in tutte le loro condizioni e termini;
- in occasione della stipulazione di contratti con fornitori e partners, questi ultimi devono dichiarare:
 - di essere a conoscenza della normativa di cui al Decreto;
 - di impegnarsi al rispetto del Decreto;
 - se siano stati mai implicati in procedimenti giudiziari relativi ai reati contemplati nel Decreto.

PARTE SPECIALE “F”

Criminalità informatica

1. LA TIPOLOGIA DEGLI ILLECITI INFORMATICI RILEVANTI (ART. 24 *BIS* DEL DECRETO)

La legge 18 marzo 2008 n. 48, nel ratificare e dare esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, ha introdotto nel nostro ordinamento una nuova serie di reati informatici. Ad alcune di tali nuove fattispecie è stata estesa la responsabilità amministrativa degli Enti, attraverso la previsione dell'art. 24 *bis* nel Decreto.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
491 <i>bis</i> c.p.	Falsità in un documento informatico	fino a 400 quote	si: divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti, contributi o sussidi e revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
640 <i>quinquies</i> c.p.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	fino a 400 quote	si: divieto di contrattare con la pubblica amministrazione; esclusione di agevolazioni, finanziamenti, contributi o sussidi e revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
615 <i>ter</i> c.p.	Accesso abusivo ad un sistema informatico o telematico	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi

615 <i>quater</i> c.p.	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematico	fino a 300 quote	si: sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
615 <i>quinqües</i> c.p.	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	fino a 300 quote	si: sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
617 <i>quater</i> c.p.	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
617 <i>quinqües</i> c.p.	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
635 <i>bis</i> c.p.	Danneggiamento di informazioni, dati e programmi informatici	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni,

			licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
635 <i>ter</i> c.p.	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
635 <i>quater</i> c.p.	Danneggiamento di sistemi informatici o telematici	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
635 <i>quinqües</i> c.p.	Danneggiamento di sistemi informatici o telematici di pubblica utilità	da 100 a 150 quote	si: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi
640 <i>quinqües</i> c.p.	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	Fino a 400 quote	si: divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti,

			contributi o sussidi e revoca di quelli già concessi; divieto di pubblicizzare beni o servizi
--	--	--	---

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa. Nella disamina, viene seguito il medesimo ordine dell'art. 24 *bis* del Decreto.

Accesso abusivo ad un sistema informatico (art. 615 *ter* c.p.)

La norma sanziona il fatto di chi, similmente a quanto avviene per la violazione fisica del domicilio, si introduce abusivamente o si trattiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo in un sistema informatico protetto da misure di sicurezza.

L'accesso al sistema informatico è considerato abusivo quando vi sia una obiettiva violazione delle condizioni e dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne l'accesso.

Al pari dell'accesso, la norma punisce anche la condotta di chi si mantenga in un sistema informatico contro la volontà – sia essa espressa o tacita – del titolare del sistema.

La giurisprudenza ha ritenuto configurabile il reato anche nel caso in cui un soggetto che sia legittimato ad accedere ad un sistema e a mantenersi vi operi per conseguire finalità illecite o, comunque, diverse da quelle per cui era stato autorizzato dal titolare dello stesso sistema.

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

La norma punisce la condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema telematico o intercorrenti tra più sistemi, ovvero volontariamente le interrompe o le impedisce.

La stessa norma punisce anche chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di dette comunicazioni.

Per “intercettazione” si intende la presa di cognizione del contenuto della comunicazione, che si realizza tramite l'intromissione in questa; per “interruzione” ed “impedimento” si intende il compimento di atti idonei rispettivamente a far cessare una comunicazione in corso e ad impedire che una nuova abbia inizio.

Installazione di apparecchiature atte ad intercettare impedire o interrompere comunicazioni telematiche (art. 617 *quinquies*)

La norma sanziona l'installazione di apparecchiature adatte ad intercettare, impedire o interrompere le comunicazioni relative ad un sistema informatico, anche quando non sia seguita da alcuna effettiva attività di intercettazione, interruzione o impedimento.

Fattispecie di danneggiamento (635 *bis* e 635 *quinquies* c.p.)

Gli artt. 635 *bis* e seguenti sanzionano una serie articolata di fattispecie che hanno il proprio elemento comune in condotte di danneggiamento volontario di dati e sistemi informatici.

L'art. 635 *bis*, anzitutto, sanziona il danneggiamento volontario di programmi o dati informatici. Il comportamento punito è quello di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

L'art. 635 *ter* punisce chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

L'art. 635 *quater* punisce il danneggiamento di sistemi informatici o telematici ed in particolare il fatto di chi, ponendo in essere una delle condotte di cui all'art. 635 *bis* finalizzate al danneggiamento di programmi e dati, ovvero mediante l'introduzione o trasmissione di dati, informazioni o programmi, danneggia il funzionamento di un intero sistema informatico.

L'art. 635 *quinquies* punisce le medesime condotte indicate dall'art. 635-*quater*, quando abbiano ad oggetto sistemi informatici o telematici di pubblica utilità.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematica (art. 615 *quater* c.p.)

La norma sanziona la condotta di chi, al fine di ottenerne un profitto od arrecare un danno, abusivamente diffonde, comunica, consegna, riproduce o si procura codici, parola chiave o altri mezzi idonei a consentire l'accesso ad un sistema informatico protetto da misure di sicurezza.

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

La norma sanziona la condotta di chi, allo scopo di: (i) danneggiare illecitamente un sistema informatico o telematico, ovvero le informazioni, i dati e i programmi in esso contenuti o ad esso pertinenti; ovvero (ii) favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento del sistema, si procura, produce, riproduce, importa, diffonde, comunica, consegna o comunque mette a disposizione di altri apparecchiature, dispositivi o programmi informatici (cd. virus informatici)

La diffusione può avvenire sia con la messa in circolazione di virus attraverso le reti telematiche sia con la materiale introduzione degli stessi nei sistemi sia con la loro incorporazione in supporti informatici sia con la messa a disposizione di detti supporti.

Falsità in documenti informatici (art. 491 *bis* c.p.)

La norma in questione estende le fattispecie di reato previste dal capo dedicato alle falsità in atti, ai casi in cui esse si la falsità abbia ad oggetto documenti di tipo informatico, intendendosi con "documento informatico", la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.)

L'articolo sanziona il fatto del soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

2. AREE A RISCHIO

Alla luce della descrizione delle fattispecie di reato sopra riportata, devono ritenersi, astrattamente, aree a rischio tutte le attività di soggetti che accedono, nell'ambito delle loro competenze aziendali, alla rete informatica della Società e ne facciano uso.

In concreto, la tipologia delle fattispecie delittuose in esame consente di limitare le possibili attività illecite nell'interesse di Data Appeal alle seguenti attività:

- alterazioni e falsificazioni di documenti elettronici pubblici o privati;
- attività di spionaggio o sabotaggio per via informatica dirette a concorrenti, pubblici o privati (creazione, modifica, alterazione di dati altrui; accesso abusivo in altrui sistemi; modifiche non autorizzate e programmi altrui e loro danneggiamento;

detenzione indebita di *password* di accesso a sistemi altrui; intercettazione fraudolenta di altrui comunicazioni informatiche; installazione di dispositivi volti a tale illecita attività; diffusione di virus...).

3. REGOLE DI CONDOTTA E PROCEDURE

In generale, tutti i Destinatari:

- devono impiegare la rete aziendale esclusivamente per scopi, operazioni e comunicazioni strettamente professionali;
- devono accedere, connettersi e scambiare dati con reti informatiche di terzi solo per ragioni professionali, nei casi e per il tempo strettamente necessari;
- devono utilizzare gli strumenti informatici ed i supporti elettronici messi a loro disposizione dalla Società ai fini esclusivamente professionali;
- devono utilizzare i soli programmi ufficialmente indicati dalla Società al momento della consegna del dispositivo informatico e /o successivamente durante lo svolgimento del rapporto di lavoro. Non è pertanto consentito inoltre agli utenti di installare, senza previa autorizzazione di un Amministratore di Sistema o dell'Amministratore delegato, programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti;
- devono evitare di lasciare incustoditi e/o accessi in loro assenza i dispositivi portatili utilizzati qualora si trovino presso le infrastrutture di Nana Bianca, e devono garantire la custodia del pc portatile attraverso un sistema di blocco automatico in caso di non utilizzo;
- devono consultare e visionare i dati informatici cui hanno accesso in ragione del ruolo e delle funzioni svolte, ed eventuali accessi che esulino dalle loro competenze e dal loro ruolo devono essere preventivamente approvati dal Responsabile della funzione IT;
- provvedono a comunicare all'Amministratore di Sistema e all'Organismo di Vigilanza qualsiasi fatto, evento, anomalia che possa rendere fondato il sospetto che sia in corso un abuso informatico.

Con riferimento alla tipologia dei reati di cui alla presente Parte Speciale, una loro reale prevenzione può e deve fondarsi su due punti:

- la certa identificazione dell'identità del soggetto che di volta in volta accede ed agisce sulla rete informatica;
- misure di prevenzione di accessi alla rete da parte di soggetti terzi e non titolati, perché sia escluso che taluno possa agire in modo anonimo sulla rete informatica aziendale.

Il monitoraggio del rispetto della procedura e l'implementazione delle misure informatiche idonee a prevenire la commissione di reati informatici nonché i rischi connessi all'utilizzo dei dispositivi utilizzati, è affidata ad un Amministratore di Sistema, individuato tra i dipendenti della Società impiegati nella funzione IT

La Società ha inoltre adottato una procedura interna, denominata *Regolamento per l'utilizzo dei sistemi e strumenti informatici di The Data Appeal Company S.p.A.*, che detta in maniera analitica e dettagliata le regole volte a garantire la sicurezza e l'integrità dei beni aziendali, tra cui rientrano gli

apparati informatici e telematici, il sistema informatico e i servizi di *Information & Communication Technology*, la tecnologia fissa e mobile, la posta elettronica, le connessioni a reti di comunicazione elettronica di qualsiasi tipo, i *software* di proprietà dell'azienda o a questa conferiti in licenza d'uso, i personal computer e gli apparati portatili. In particolare, il Regolamento specifica le modalità di utilizzo consentite di tali apparecchi e le *best practices* da seguire per garantire un'adeguata conservazione e tutela dei dati e delle informazioni ivi contenute e trasmesse. Al fine di assicurare il rispetto della procedura e delle regole dalla stessa fissate per il corretto trattamento dei beni aziendali, e per la corretta gestione e trasmissione delle informazioni in via telematica tramite le strutture e la Rete, il Regolamento prevede l'applicazione di specifiche sanzioni disciplinari a carico dei dipendenti che violino in qualsiasi modo le sue prescrizioni.

Tale procedura è indirizzata non solo ai dipendenti ma anche a tutti i collaboratori e consulenti di Data Appeal a prescindere dal rapporto contrattuale con la stessa, che vengono autorizzati a far uso degli strumenti tecnologici della Società o di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi trattati e conservati e disciplina l'uso della rete aziendale e degli *account* degli utenti (incluse la gestione e l'assegnazione delle credenziali di autenticazione); dei dispositivi fissi e portatili; della posta elettronica; le modalità di navigazione in internet, nonché le verifiche approntate dall'azienda per monitorare e il corretto uso di tutti i beni aziendali.

In particolare, è fatto obbligo a tutti i Destinatari di utilizzare e conservare i dispositivi elettronici con cura e di restituirli alla fine del rapporto in buono stato di manutenzione e conservazione.

Il sistema di accesso agli strumenti e dispositivi informatici si basa sull'autenticazione per credenziali personali.

Le credenziali di autenticazione per l'accesso alla Rete vengono assegnate al momento dell'assunzione dall'HR. Successivamente al momento dell'assunzione, l'Amministratore di Sistema ed il *Chief Technology Officer* (CTO) creano l'utenza di dominio che consente ad ogni utente l'accesso in via personale all'account aziendale tra cui alla posta aziendale e alle risorse della G-suite aziendale (programmi e spazi di archiviazione personali e condivisi). In particolare, è fatto obbligo per tutti i Destinatari che si trovino ad impiegare computer aziendali e, più in generale, ad accedere alla rete aziendale, l'impiego di un sistema di *password* compiutamente delineato. Questo consente di tracciare costantemente tutti gli accessi al sistema informatico aziendale, e di verificare, se necessario, le attività compiute da ciascun utente. I profili degli ex dipendenti vengono disattivati non appena cessa il rapporto di lavoro (o di collaborazione a qualsiasi titolo), e l'utente dovrà inoltre coordinarsi con HR e con l'Amministratore di Sistema al fine di effettuare la cancellazione dei Dati presenti sul PC, dopo essersi assicurato con l'assistenza delle figure sopra citate di consegnare o trasferire tutti i Dati di interesse aziendale secondo le istruzioni ricevute.

L'accesso ad ogni account aziendale e alle relative risorse avviene attraverso l'impiego delle "*credenziali di autenticazione*", consistenti in un codice di identificazione dell'utente ("*user id*"), assegnato dall'Amministratore di Sistema e comunicato all'utente dallo stesso o dall'HR, associato ad una parola chiave ("*password*") riservata.

La *password*:

- viene inizialmente fornita dall'Amministratore di Sistema, al momento dell'assegnazione del dispositivo aziendale e deve essere modificata dall'utente al suo primo accesso e periodicamente, ogni sei mesi;
- deve essere nota solo all'utente, che deve custodirla con la massima diligenza, senza divulgarla o comunicarla a terzi;
- deve essere individuata in base a specifiche regole indicate puntualmente nel *Regolamento* (numero minimo di caratteri, combinazione alfanumerica);

- in caso di necessità di sostituzione della password, per qualsiasi motivo, essa verrà sostituita dall'Amministratore di Sistema che provvederà a resettare le credenziali ed impostarne di nuove;
- è consigliabile evitare di annotarla in luoghi facilmente accessibili, se si ritiene necessario annotarla, deve essere conservata in un luogo sicuro e non facilmente accessibile, possibilmente lontano dalla postazione di lavoro;
- qualora vi sia il sospetto che sia stata identificata o utilizzata da terzi non autorizzati, è necessario modificarla immediatamente, segnalando senza ritardo la circostanza all'Amministratore di Sistema.

Le credenziali dei Server vengono custodite dall'ADS e dal CTO.

Da un punto di vista telematico, Data Appeal previene intrusioni di terzi nella propria rete (cd. *spyware*) anche con apposite componenti di log file e VPN presenti nei server in *cloud*, sempre aggiornate dal fornitore del servizio (cd. firewall meraki) e soggette al costante controllo da parte dell'Amministratore di Sistema. È inoltre specificato che, allo stato attuale, i dispositivi in uso sono equipaggiati con il sistema operativo MAC OS al cui interno ha già una tecnologia che permette di criptare, monitorare, aggiornare e proteggere il dispositivo.

Si rileva, inoltre, che il rispetto dei beni aziendali e la tutela della loro integrità sono principi ribaditi anche dal Codice Etico di Data Appeal.

Seppure quella introdotta dal GDPR costituisca una disciplina normativa che non ha alcuna incidenza diretta sulle previsioni e sulla responsabilità previste dal Decreto, è comunque di tutta evidenza che il sistema preventivo adottato in esecuzione delle prescrizioni del GDPR – che impone l'adozione di misure di protezione dei dati, e quindi anche di sicurezza per l'accesso e l'uso dei sistemi informatici - costituisce un utile strumento anche ai fini della prevenzione dalla commissione dei reati qui in esame.

La Società ha quindi ultimato le attività di aggiornamento alla normativa dettata in materia di trattamento dei dati personali dal GDPR. Data Appeal ha predisposto il Registro del Trattamento dei Dati Personali, in cui sono analiticamente indicati il Responsabile del Trattamento, il tipo di trattamento ed i dati trattati, gli incaricati dei trattamenti, nonché tutte le misure di sicurezza adottate dalla Società per impedire accessi abusivi ai dati sensibili trattati dalla Società.

In tale Registro, sono state inoltre previste una serie di misure a tutela della sicurezza dei dati personali, indicando le modalità materiali di custodia di tali dati, sia riferibili ai dipendenti sia ai clienti, e le modalità di conservazione in *cloud* di particolari dati personali sensibili.

La Società ha inoltre provveduto a formalizzare le nomine a responsabile del trattamento ai consulenti esterni.

Inoltre, data la novità dell'intervento normativo e degli adempimenti posti in essere dalla Società, questa ha previsto periodici *audit* interni in materia di *privacy*, in modo da tenere costantemente monitorato il sistema così implementato, ed individuare aree e/o attività su cui si rendono necessari interventi correttivi.

In particolare, la Società ha predisposto una procedura riguardante le ipotesi di cd. Data Breach, ossia la notifica delle eventuali violazioni dei dati personali e loro gestione.

La Società ha infine programmato una serie di incontri formativi destinati a tutti i dipendenti, il cui programma è già stato definito di concerto con la funzione HR, aventi ad oggetto le procedure e gli adempimenti necessari ai fini del rispetto della normativa dettata dal GDPR, a cui si aggiungeranno incontri formativi più specifici e mirati per determinati ruoli aziendali.

Preliminare alla trattazione del presente punto, è il rilievo relativo alla rete informatica attraverso cui Data Appeal svolge la propria Attività. Infatti, la Società non dispone di server o dispositivi di interconnessione di proprietà, non dispone di una propria rete LAN né di un proprio esclusivo accesso alla rete internet, non dispone di dispositivi di protezione perimetrale di proprietà, avvalendosi della rete informatica di Nana Bianca (la *Rete*), in forza di un contratto di coworking stipulato con lo stesso e in virtù del quale dispone di alcuni spazi e postazioni lavorative ed accede alla Rete.

Allo stato attuale, l'infrastruttura di Nana Bianca è dotata di misure di accesso al centro e di utilizzo delle postazioni, il cui rispetto è demandato ai dipendenti. Tra le prescrizioni contenute nel vigente contratto, si rilevano inoltre quelle attinenti al corretto utilizzo dei dispositivi messi a disposizione da Nana Bianca ed il corretto trattamento dei dati in ottemperanza al GDPR, sia da parte dei dipendenti di Data Appeal, sia da parte di Nana Bianca. Allo stato attuale, è pertanto rimessa alla Società la valutazione circa l'idoneità della Rete (*networking* e Internet) fornita da Nana Bianca nella propria infrastruttura, e in capo alla Società l'obbligo di attuare sistemi di sicurezza logici, fisici e organizzativi idonei a impedire l'accidentale o incontrollata consultazione, esportazione, lettura, copiatura, distribuzione, comunicazione, diffusione di dati o dei documenti trattati nell'esecuzione del contratto.

Come rilevato anche dai recenti audit interni, l'attuale infrastruttura di Rete di Nana Bianca presenta alcune criticità, che saranno tuttavia mitigate per effetto del prossimo trasferimento del centro Nana Bianca. Data Appeal, infatti, in virtù di accordi contrattuali, ha previsto il trasferimento delle proprie Attività entro la fine dell'anno presso nuove infrastrutture di proprietà di Nana Bianca, che saranno dotate di una rete a standard di sicurezza di nuova generazione (il trasferimento, inizialmente previsto entro il primo trimestre 2020, è stato posticipato per cause dovute all'insorgenza dell'emergenza epidemiologica da COVID-19).

Tale requisito di sicurezza viene formalizzato dalla Società anche attraverso una previsione contrattuale che impone a Nana Bianca l'adozione di standard e misure di sicurezza elevate in riferimento alla nuova Rete, che costituiscono un elemento essenziale dell'accordo.

Rimane fermo che qualunque proposta di integrazione e implementazione motivata al *Regolamento* potrà essere inviata al CEO, e in caso di sua assenza e/o impedimento, al CFO.

PARTE SPECIALE “G”

Delitti contro il diritto d'autore, l'industria ed il commercio

1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ARTT. 25 *BIS*.1, 25 *NOVIES* E 25 *BIS* COMMA 1 LETT. F *BIS* DEL DECRETO)

La legge 23 luglio 2009 n. 99 ha esteso l'elenco dei Reati Presupposto introducendo nel Decreto i nuovi articoli 25 *bis*1 e 25 *novies*. All'esame di questi reati, nella presente Parte Speciale, e per evidenti ragioni di connessione quanto alla materia, è stata aggiunta anche la trattazione delle fattispecie di reato previste dagli artt. 473 e 474 c.p., inserite nel Decreto dall'art. 25 *bis* comma 1 lett. f *bis*, e integranti condotte in violazione del diritto d'autore.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
513 c.p. (art. 25 <i>bis</i> 1)	Turbata libertà dell'industria o del commercio	fino a 500 quote	no
515 c.p. (art. 25 <i>bis</i> 1)	Frode nell'esercizio del commercio	fino a 500 quote	no
516 c.p. (art. 25 <i>bis</i> 1)	Vendita di sostanze alimentari non genuine vendute come genuine	fino a 500 quote	no
517 c.p. (art. 25 <i>bis</i> 1)	Vendita di prodotti industriali con segni mendaci	fino a 500 quote	no
517 <i>ter</i> c.p. (art. 25 <i>bis</i> 1)	Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale	fino a 500 quote	no
517 <i>quater</i> c.p. (art. 25 <i>bis</i> 1)	Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari	fino a 500 quote	no
513 <i>bis</i> c.p. (art. 25 <i>bis</i> 1)	Illecita concorrenza con minaccia o violenza	fino a 800 quote	sì: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
514 c.p. (art. 25 <i>bis</i> 1)	Frodi contro le industrie nazionali	fino a 800 quote	si: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
171 comma 1 lett. a <i>bis</i>) l.a. (art. 25 <i>novies</i>)	Divulgazione, in un sistema di reti telematiche, di opera dell'ingegno protetta o di parte di essa	fino a 500 quote	sì, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
171 comma 3 l.a. (art. 25 <i>novies</i>)	Diffusione, rappresentazione, riproduzione di un'opera dell'ingegno non destinata alla pubblicazione, ovvero con usurpazione della paternità, ovvero con deformazione, mutilazione o altra modifica dell'opera	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
171 <i>bis</i> l.a. (art. 25 <i>novies</i>)	Reati in materia di <i>software</i> e banche dati	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
171 <i>ter</i> l.a. (art. 25 <i>novies</i>)	Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografici, e in materia di opere letterarie, scientifiche e didattiche	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

171 <i>septies</i> l.a. (art. 25 <i>novies</i>)	Violazioni nei confronti della SIAE	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
171 <i>octies</i> l.a. (art. 25 <i>novies</i>)	Manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di

			quelli già concessi; divieto di pubblicizzare beni o servizi.
473 c.p. (art. 25 <i>bis</i> comma 1 lett. f <i>bis</i>)	Contraffazione, alterazione o uso di marchi o segni distintivi overro di brevetti, modelli e disegni	fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
474 c.p. (art. 25 <i>bis</i> comma 1 lett. f <i>bis</i>)	Introduzione nello Stato e commercio di prodotti con segni falsi	Fino a 500 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da

			agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
--	--	--	--

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa, seguendo l'ordine degli articoli del Decreto che li prevedono.

(I) DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (Art. 25 bis)

Turbata libertà dell'industria o del commercio (art. 513 c.p.)

Il reato si configura quando vengono adoperati violenza sulle cose oppure mezzi fraudolenti al fine di impedire o turbare l'esercizio di un'industria o di un commercio altrui.

L'art. 513 c.p., pur essendo rivolto alla tutela dell'ordine economico nazionale, tutela anche il diritto individuale al libero svolgimento di un'attività economica, proteggendolo da turbative o da impedimenti illeciti. La norma in esame è sussidiaria, trovando applicazione solamente qualora il fatto non costituisca un più grave reato.

Il delitto in esame è un reato di pericolo, per la cui consumazione è quindi sufficiente che, dall'azione violenta e fraudolenta, derivi una semplice minaccia al libero svolgimento dell'attività commerciale del singolo. Per la sussistenza del delitto sono necessari alternativamente l'uso della violenza o di mezzi fraudolenti.

Un comportamento può considerarsi fraudolento quando sia subdolo o sleale, quando cioè tenda a mascherare o nascondere con l'inganno il proprio carattere di illiceità. La violenza sulle cose è, invece, l'impiego della forza fisica che comporti il danneggiamento o la trasformazione o il mutamento della destinazione di un oggetto.

Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.)

Il delitto si configura in tutti quei casi in cui, nell'esercizio di un'attività commerciale, industriale o comunque produttiva, vengono compiuti atti di concorrenza con violenza o minaccia. È prevista un'aggravante se gli atti di concorrenza riguardano un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.

La fattispecie in esame mira a sanzionare quei comportamenti minacciosi e violenti finalizzati al controllo o, quantomeno, al condizionamento di altrui attività commerciali, industriali o produttive, incidendo tale condotta sul corretto confronto concorrenziale tra i vari operatori del mercato.

Anche questa ipotesi delittuosa va inquadrata nella categoria dei reati di pericolo, in quanto si perfeziona già nel momento in cui vengono attuati gli atti di violenza o minaccia diretti ad impedire o a rendere più gravoso il libero esercizio dell'attività economica altrui, la cui commissione è considerata dal legislatore quale atto concreto di concorrenza sleale.

Costituiscono violenza o minaccia comportamenti che hanno l'effetto di coartare la volontà altrui: la prima, attraverso la forza fisica; la seconda attraverso prospettazione di un male ingiusto la cui verifica dipende dalla volontà del minacciante.

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

La norma punisce la condotta di chi, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, abbia cagionato un danno all'industria nazionale.

Ai fini della configurabilità del delitto in esame è sufficiente la messa in vendita di prodotti con segni alterati o contraffatti (a cui consegua un danno all'industria nazionale), indipendentemente dall'osservanza delle norme sulla tutela della proprietà industriale.

Frode nell'esercizio del commercio (art. 515 c.p.)

Il reato si configura quando, nell'esercizio di una attività commerciale, si consegna all'acquirente una cosa mobile per un'altra, ovvero si consegna una cosa mobile che - per origine, provenienza, qualità o quantità - è diversa da quella dichiarata o pattuita.

È prevista un'aggravante nel caso in cui la cosa mobile sia costituita da oggetti preziosi.

Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)

Il reato si configura quando sono poste in vendita o sono messe altrimenti in commercio come genuine sostanze alimentari che genuine non sono.

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

Il reato si configura quando sono messi in vendita o distribuiti opere di ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti a indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.

Il reato in esame si consuma nel momento stesso in cui il prodotto viene posto in vendita o altrimenti in commercio: la condotta illecita deve pertanto ritenersi sussistente ogni qualvolta la merce irregolare sia stata semplicemente messa a disposizione del pubblico.

Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (517 ter c.p.)

Il reato punisce la condotta di chi, pur potendo conoscere l'esistenza di un titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in sua violazione. È punita anche la condotta di chi introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i predetti oggetti o beni, usurpando un titolo di proprietà industriale o in sua violazione.

La pena è aggravata nel caso in cui i reati descritti siano commessi in modo sistematico o mediante allestimento di mezzi e attività organizzate ovvero quando oggetto del reato siano alimenti o bevande la cui denominazione o specificità siano protette dalle norme vigenti.

Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (517 quater c.p.)

Il reato si configura quando viene contraffatto o vengono alterate le indicazioni geografiche o denominazioni di origine di prodotti agroalimentari.

La norma in esame punisce anche chi, al fine di trarne profitto, introduce nel territorio dello Stato, detiene per la vendita, pone in vendita con offerta diretta ai consumatori o mette comunque in circolazione i medesimi prodotti con le indicazioni o denominazioni contraffatte.

(II) DELITTI IN MATERIA DI DIRITTO D'AUTORE (Art. 25 novies)

Divulgazione di opere dell'ingegno attraverso rete telematica (art. 171 comma 1 lett. A bis e comma 3 l.a.)

La norma punisce la condotta di chi mette a disposizione del pubblico un'opera dell'ingegno protetta, o anche solo parte di essere, immettendola in un sistema di reti telematiche.

Quella medesima condotta assume rilievo anche quando sia stata commessa su un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, quando da tale condotta risulti un'offesa all'onore o alla reputazione dell'autore.

Reati in materia di software e banche dati (art. 171 bis l.a.)

Gli illeciti previsti all'art. 171 bis sono posti a tutela dei software e delle banche dati informatiche. Il primo comma della norma sanziona la duplicazione di software protetti dal diritto d'autore e la loro commercializzazione. Allo stesso modo è sanzionata la diffusione di strumenti informatici diretti a rimuovere filtri e altre protezioni di software protetti da diritto d'autore. Il secondo comma, invece, sanziona la duplicazione e la commercializzazione abusive di banche dati informatiche.

Reati in materia di opere dell'ingegno destinate ai circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche (art. 171 ter l.a.)

Questa articolatissima norma sanziona una serie di illeciti. È forse il caso di riportarla testualmente, perché sia sempre disponibile alla consultazione di tutti i Destinatari del Modello.

Il primo comma della norma sanziona il fatto di chi, per uso non personale, ed a fini di lucro:

“a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;

f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse”.

Il secondo comma sanziona ancor più gravemente chi:

“a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti commessi, si rende colpevole dei fatti previsti dal comma 1”.

Violazioni nei confronti della SIAE e Manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato (artt. 171 *septies* e 171 *octies*)

Si tratta di fattispecie meno frequenti e certamente più particolari delle precedenti, che pertanto vengono esaminate congiuntamente.

La prima norma si applica “ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi” o a chi rilascia false dichiarazioni in merito all’assolvimento di simili obblighi.

La norma successiva colpisce invece la produzione e la diffusione 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*”.

Contraffazione di segni distintivi e introduzione nello Stato di oggetti con segni contraffatti (artt. 473 e 474 c.p.) (art. 25 bis comma 1 lett. f bis)

In aggiunta alle norme appena citate, e sempre in materia di reati in violazione del diritto d'autore, si devono ricordare anche gli artt. 473 e 474 c.p., cui fa espresso riferimento l'art. 25 bis comma 1 lett. f bis) del Decreto.

Le due fattispecie sanzionano la contraffazione o l'alterazione di marchi, opere di ingegno e altri prodotti industriali; l'impiego di segni contraffatti o alterati nonché l'introduzione nel territorio dello Stato di prodotti recanti segni contraffatti o alterati.

Secondo la giurisprudenza, si deve qualificare come “contraffazione” la riproduzione abusiva integrale del marchio nella la sua configurazione emblematica e denominativa e come “alterazione” la modifica del segno, ricomprendente anche l'imitazione fraudolenta (vale a dire la riproduzione parziale, ma tale da permettere che vi sia confusione con il marchio originale o con il segno distintivo).

2. AREE A RISCHIO

L'esame della tipologia di Attività svolta da Data Appeal consente di individuare, con riguardo ai Reati Presupposto qui in esame, fondamentalmente quattro aree di rischio. Due di queste solo legate alla specifica Attività svolta dalla Società, e consistono in particolare in quello che è il *core business* di Data Appeal, ossia la raccolta e nella successiva rielaborazione dei dati (soprattutto recensioni, *feedback*) pubblicati su internet, e nelle attività a questa correlate di sviluppo, protezione e titolarità degli specifici strumenti ed applicativi utilizzati per lo svolgimento dell'Attività (*i.e. software*, algoritmi, licenze, etc.). A queste si possono aggiungere ancora le aree di rischio comuni a tutte le attività aziendali, consistenti nell'acquisto e nella cessione di beni e servizi, e nel confronto commerciale con i concorrenti.

L'Attività di Data Appeal consiste quindi sostanzialmente in un'attività di c.d. *scraping*, consistente nell'estrazione massiva di informazioni presenti su una pagina *web*. Le informazioni (*big data*) utilizzate da Data Appeal sono a disposizione di tutti gli utenti, perché pubblicati su siti e pagine *web* pubblici, e il cui accesso è quindi consentito indistintamente a tutti, senza necessità di registrazioni o *log-in* a pagamento.

Sotto tale profilo, pertanto, l'unico profilo di rischio ipotetico che potrebbe configurarsi è quello dell'accesso, da parte di un esponente della Società, ad una banca dati per il riutilizzo dei dati ivi conservati. Il rischio però è escluso dalla semplice descrizione, nel dettaglio, dell'Attività effettivamente svolta da Data Appeal e dalle modalità con cui questa provvede a rielaborare i dati pubblici a disposizione sul *web*.

A sua maggior tutela, e al fine comunque di escludere quanto più possibile ogni rischio, la Società ha provveduto a dettare anche le regole di condotta qui sintetizzate.

Quanto invece alla ideazione, allo sviluppo e all'utilizzo di *software*, algoritmi o altri applicativi, per lo svolgimento dell'Attività – come detto – Data Appeal utilizza un proprio algoritmo, ideato e sviluppato al proprio interno. Sotto tale profilo, pertanto, il rischio per la Società potrebbe essere, semmai, quello di essere soggetto passivo di uno dei reati qui contemplati.

Quanto invece all'ideazione e sviluppo di *software*, la Società si affida a società specializzate del settore, previa sottoscrizione di specifici accordi aventi ad oggetto lo sviluppo, oppure la licenza d'uso di un particolare *software*. Tali contratti disciplinano anche in maniera analitica i diritti di proprietà intellettuale relativi allo specifico servizio oggetto dell'accordo.

Parimenti circoscritto è anche il rischio di commissione di delitti in materia di segni distintivi: Data Appeal ha infatti depositato in data 11 luglio 2019 domanda di registrazione del marchio figurativo  **TRAVEL APPEAL** presso l'UEIPO (l'Ufficio dell'Unione europea per la proprietà intellettuale). La domanda è stata pubblicata, ma risulta ancora pendente. Tale marchio si riferisce alla classe di Nizza n. 9, 35, 38, 39, 42 in materia di software, piattaforme software, analisi e monitoraggio di algoritmi di sistema per l'elaborazione dei dati e trasmissione elettronica dei dati.

Va poi ancora sottolineato che Data Appeal tendenzialmente non sfrutta segreti industriali o brevetti. L'area astrattamente a rischio, per Data Appeal, è quindi rappresentata dal confronto commerciale con i concorrenti: seppure le fattispecie relative agli abusi nell'esercizio della concorrenza (articoli 513 e 513-bis c.p.) individuano fattispecie molto particolari e non facilmente realizzabili, Data Appeal ha ritenuto di creare comunque una Parte Speciale per questo settore di attività, poiché crede profondamente nel valore di una concorrenza che sia corretta e sia sempre correttamente esercitata e ritiene doveroso richiamare tutti i Destinatari del Modello su questi fondamentali punti.

3. REGOLE DI CONDOTTA

Con riferimento alla tipologia dei reati di cui alla presente Parte Speciale, la loro reale prevenzione può e deve fondarsi sui seguenti principi di condotta:

- tutti i Destinatari del Modello devono svolgere la propria attività commerciale secondo le politiche commerciali, le metodologie, le regole e le condizioni stabilite da Data Appeal, senza possibilità di eccezioni;
- la raccolta e la rielaborazione dei dati devono avvenire quanto più possibile nel rispetto dei termini e condizioni previste dal sito da cui vengono raccolti tali dati;
- i Destinatari e i dipendenti si impegnano a monitorare eventuali cambiamenti di termini e condizioni dei siti frequentati per la raccolta dei dati, segnalando eventuali cambiamenti, profili di rischio e violazioni degli altrui diritti di proprietà o in contrasto con la normativa in materia di tutela delle banche dati altrui;
- eventuali confronti, contrasti e/o controversie con la concorrenza o con suoi esponenti sono attività per definizione a rischio, che devono essere gestite con particolare cura ed in via esclusiva dalla sede centrale di Data Appeal;
- nell'esercizio dell'attività aziendale possono essere impiegati solo loghi, insegne, marchi e simili che siano quelli indicati ed approvati da Data Appeal.

Il primo principio di condotta è volto ad escludere la possibilità che vi sia, per ottenere un vantaggio concorrenziale, l'autonoma adozione di iniziative e metodi commerciali che si possano rivelare illeciti.

Una concorrenza efficace, ma al contempo del tutto lecita è considerata da Data Appeal un elemento decisivo della propria attività aziendale, pertanto, Data Appeal ritiene necessario che le modalità per l'esercizio concorrenziale della propria attività d'impresa vengano necessariamente determinate e gestite a livello centralizzato, da parte delle direzioni competenti.

È pertanto fatto espresso divieto a tutti i Destinatari di esercitare l'attività aziendale a condizioni e modalità differenti rispetto a quelle stabilite da Data Appeal, di adottare autonomamente iniziative promozionali o effettuare tipologie di servizi non previste.

Quanto al secondo ed al terzo principio di condotta, lo scopo è quello di prevenire un utilizzo scorretto delle banche dati altrui e consentire un monitoraggio costante che permetta alla Società, in tempo utile, di prendere adeguate misure e contromisure in riferimento a eventuali criticità per scongiurare la commissione dei reati.

Per quanto attiene al quarto principio di condotta, l'obiettivo è quello di garantire il pieno controllo di Data Appeal sull'ambito maggiormente a rischio di commissione degli illeciti concorrenziali indicati dal Decreto, che è costituito da eventuali casi di confronto o contrasto con imprese concorrenti.

Anche se l'eventuale controversia è particolare o locale (a titolo esemplificativo, riguarda solo un centro ed i suoi rapporti con un centro di imprese concorrenti), è fatto espresso divieto ai Destinatari di volta in volta interessati di gestire autonomamente il confronto o la controversia in corso.

Al contrario è fatto obbligo a quei soggetti di comunicare la controversia alla sede di Data Appeal e di astenersi da ogni iniziativa che non sia da essa indicata.

In ogni caso, Data Appeal pone un esplicito divieto a tutti i Destinatari di accedere, per qualunque ragione, alle aree di pertinenza di imprese concorrenti e di avere qualunque contatto fisico con beni, strumenti e strutture di loro proprietà.

Allo stesso modo, in caso di contrasti o confronti con imprese concorrenti, sono vietati contatti diretti con i dipendenti delle stesse.

L'ultimo principio di condotta è volto alla prevenzione di eventuali illeciti tra quelli relativi all'impiego dei segni distintivi.

È fatto espresso divieto a tutti i Destinatari di impiegare altri segni distintivi rispetto a quelli ufficiali di Data Appeal ed è, parallelamente, espressamente fatto obbligo agli stessi di impiegare sempre, nell'esercizio di ogni aspetto dell'attività commerciale, in via esclusiva i segni distintivi di Data Appeal.

La Società ha inoltre delineato alcune linee guida e regole comportamentali per i propri dipendenti e collaboratori, al fine di prevenire la commissione di illeciti civili e penali in materia di proprietà intellettuale. Nel *Regolamento per l'utilizzo dei sistemi e strumenti informatici di Data Appeal S.p.A.* è precisato che ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Azienda; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi dell'Azienda, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Generale dell'Azienda.

PARTE SPECIALE “H”

Delitti contro l'attività giudiziaria

1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 25 *DECIES* DEL DECRETO)

L'articolo 25 *decies* è stato inserito nel Decreto nel 2009, e ha introdotto la responsabilità dell'Ente per il reato di induzione a non rendere dichiarazioni e/o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Si tratta, in particolare, della seguente fattispecie di reato, schematicamente riassunta qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
377 <i>bis</i> c. p.	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	fino a 500 quote	no

Il reato si configura quando con violenza o minaccia oppure con offerta o promessa di denaro o altra utilità, si induce la persona chiamata a rendere dichiarazioni davanti alla autorità giudiziaria a non rendere dichiarazioni o a rendere dichiarazioni mendaci (dichiarazioni utilizzabili in un procedimento speciale).

2. AREA A RISCHIO

L'attività imprenditoriale, commerciale o industriale di ogni azienda è sempre passibile di essere sottoposta ad investigazione da parte dell'autorità giudiziaria.

Ciò, a maggior ragione, proprio dal momento in cui è stato introdotto il regime della responsabilità amministrativa degli Enti.

Per qualunque Ente, quindi, deve ritenersi astrattamente configurabile un rischio di commissione dell'illecito in parola, nel caso in cui uno o più esponenti dell'ente fossero chiamati dall'autorità procedente a fornire informazioni e chiarimenti sull'ente e su aspetti rilevanti per la verifica dell'ipotesi accusatoria.

3. REGOLE GENERALI DI CONDOTTA

Nel caso in cui Data Appeal o un proprio esponente si trovino coinvolti in indagini da parte dell'autorità giudiziaria, tutti i Destinatari, se chiamati a rendere dichiarazioni alla medesima autorità, devono ritenersi completamente liberi di rispondere secondo verità.

Data Appeal assicura infatti a tutti i Destinatari che il fatto della loro collaborazione con gli inquirenti non potrà mai essere fonte di pregiudizio, discriminazione o valutazione negativa da parte dell'azienda.

Data Appeal, anzi, indica come espresso obbligo di ogni Destinatario il dovere di rispondere secondo verità, completezza e trasparenza alle richieste di informazioni dell'autorità giudiziaria.

Data Appeal tutela la riservatezza del Destinatario di volta in volta interessato: nessuno dovrà mai ritenersi in obbligo di comunicare alla società la circostanza di un'eventuale convocazione o di un'avvenuta audizione, così come mai potrà essere fonte di un giudizio negativo dell'azienda il fatto del dipendente di aver mantenuto quelle circostanze riservate.

Più in generale, qualora emergesse l'esistenza di un'indagine nei confronti dell'azienda o di un suo esponente, Data Appeal provvederà ad individuare, tra i propri dirigenti, un soggetto responsabile del

procedimento, cui competeranno l'apertura e la tenuta di un apposito fascicolo in cui saranno conservati tutti gli atti ufficiali del procedimento (eventuali avvisi di garanzia, verbali di perquisizione, di sequestro e quant'altro), nonché sarà registrata una cronologia dei principali sviluppi della vicenda.

Tendenzialmente, all'emersione dell'esistenza di indagini, Data Appeal investirà immediatamente della questione un legale di fiducia, da cui si farà assistere sin dalle prime fasi del procedimento.

Dell'esistenza delle indagini sarà prontamente informato l'Organismo di Vigilanza, cui sarà altresì indicata l'identità del soggetto incaricato della tenuta del fascicolo e del difensore di fiducia.

È fatto obbligo a qualunque Destinatario di informare di ogni eventuale tentativo di condizionamento (o comunque di ogni altra circostanza che possa aver indotto il sospetto di un simile tentativo) l'Organismo di Vigilanza, che provvederà ad assumere al riguardo ogni idonea iniziativa.

PARTE SPECIALE “I”

Reati ambientali

1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 25 UNDECIES)

A partire dal 2011, con il d.lgs. 7 luglio 2011 n. 121 (entrato in vigore il 16 agosto 2011), la responsabilità amministrativa delle società è stata estesa anche ad alcune tipologie di reati ambientali.

La norma ha infatti inserito nel Decreto l'art. 25 *undecies* che include tra i Reati Presupposto anche alcuni illeciti di natura ambientale, previsti sia da diverse disposizioni di legge, tra cui in particolare il codice penale e il d. lgs. 3 aprile 2006 n. 152 (*Norme in materia ambientale*, c.d. **Codice dell'Ambiente**), cui si aggiungono alcune specifiche fattispecie previste dalla legge 7 febbraio 1992 n. 150 (*Disciplina dei diritti relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione (..) nonché norme per la commercializzazione e la detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica*), dalla legge 28 dicembre 1993 n. 549 (*Misure a tutela dell'ozono stratosferico e dell'ambiente*), e dal d. lgs. 6 novembre 2007 n. 202 (*Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni*).

In particolare, gli illeciti per i quali oggi è quindi prevista la responsabilità amministrativa degli enti in materia ambientale sono i seguenti (riportati con le relative sanzioni).

1. Codice penale

Articolo	Illecito	Sanzione pecuniaria	Sanzioni interdittive
452 bis	Inquinamento ambientale	da 250 a 600 quote	si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

452 <i>quater</i>	Disastro ambientale	da 400 a 800 quote	si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
452 <i>quinqies</i>	Delitti colposi contro l'ambiente	da 200 a 500 quote	no
452 <i>sexies</i>	Traffico e abbandono di materiale ad alta radioattività	da 250 a 600 quote	no
452 <i>octies</i>	Delitti associativi aggravati	da 300 a 1.000 quote	no
452 <i>quaterdecies</i> (ex art. 260 Codice dell'Ambiente)	Attività organizzate per il traffico illecito di rifiuti, con l'aggravante del traffico illecito di rifiuti ad alta radioattività	da 300 a 500 quote per il traffico illecito di rifiuti, da 400 a 800 quote se si tratta di rifiuti ad alta radioattività	si, per una durata non superiore a 6 mesi: si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi. È prevista inoltre l'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16 comma 3 del Decreto se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato
727 bis	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette	fino a 250 quote	no
733 bis	Distruzione o deterioramento di habitat all'interno di un sito protetto	da 150 a 250 quote	no

2. Codice dell'Ambiente

Articolo	Illecito	Sanzione pecuniaria	Sanzioni interdittive
137 (commi 3, 5 primo periodo e 13)	Scarico di acque reflue industriali contenenti sostanze pericolose e scarico in mare da	da 150 a 250	no

	parte di navi od aeromobili di sostanze e materiali per i quali è previsto il divieto assoluto di sversamento		
137 (commi 2, 5 secondo periodo e 11)	Scarico di acque reflue industriali contenenti sostanze pericolose, scarico di acque reflue industriali con valori oltre i limiti fissati dalla tabella 3/A dell'Allegato 5 e violazione dei divieti di scarico	da 200 a 300 quote	si, per una durata non superiore a sei mesi: si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
256 (comma 1, lett. a) e 6 primo periodo)	Raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti non pericolosi senza la prescritta autorizzazione, deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi	fino a 250 quote	no
256 (comma 1, lett. b), 3 primo periodo e 5)	Raccolta, trasporto, recupero, smaltimento, commercio ed	da 150 a 250 quote	no

	intermediazione di rifiuti pericolosi senza la prescritta autorizzazione, realizzazione e gestione di discarica non autorizzata, attività non consentita di miscelazione di rifiuti		
256 (comma 3 secondo periodo)	Realizzazione e gestione di una discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi	da 200 a 300 quote	si, per una durata non superiore a sei mesi: si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
256 (comma 4)	Attività di gestione di rifiuti effettuata con inosservanza, delle prescrizioni contenute o richiamate nelle autorizzazioni, in carenza dei requisiti e delle condizioni richiesti per le	fino a 125 quote in caso di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti non pericolosi; da 75 a 125 quote per le medesime attività che riguardino rifiuti pericolosi, da 100 a	no

	iscrizioni e comunicazioni	150 quote in caso di realizzazione e gestione di una discarica	
257 (comma 1)	Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio	fino a 250 quote	no
257 (comma 2)	Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio provocato da sostanze pericolose	da 150 a 250 quote	no
258 (comma 4)	False indicazioni nella predisposizione di un certificato di analisi di rifiuti sulla natura, sulla composizione sulle caratteristiche chimico-fisiche dei rifiuti, e uso di un certificato falso durante il trasporto	da 150 a 250 quote	no
259 (comma 1)	Spedizione di rifiuti costituente traffico illecito, spedizione di rifiuti elencati nell'Allegato II del Regolamento CEE 1° febbraio 1993 n. 259	da 150 a 250 quote	no
260 bis	Violazione del sistema informatico di controllo della tracciabilità dei rifiuti, con l'aggravante nel caso si tratti di rifiuti pericolosi	da 150 a 250 quote, da 200 a 300 nel caso si tratti di rifiuti pericolosi	no

279 (comma 5)	Violazione dei limiti di emissione nell'esercizio di uno stabilimento quando il superamento determini anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa	fino a 250 quote	no
---------------	--	------------------	----

3. **L. 7 febbraio 1992 n. 50 Disciplina dei reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione, firmata a Washington il 3 marzo 1973, di cui alla L. 19 dicembre 1975 n. 874, e del Regolamento (CEE) n. 3626/82, e successive modificazioni, nonché norme per la commercializzazione e la detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica**

Articolo	Illecito	Sanzione pecuniaria	Sanzioni interdittive
1 (comma 1), 2 (commi 1 e 2) e 6 (comma 4)	Importazione, esportazione, omissione delle prescrizioni per preservare incolumità, utilizzo, trasporto, commercio ecc. di animali appartenenti alle specie elencate negli Allegati B e C del Regolamento CE n. 338/97; detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e l'incolumità pubblica	fino a 250 quote	no
1 (comma 2)	Recidiva nei reati di importazione, esportazione, ecc. di cui al punto che	da 150 a 250 quote	no

	precede, oppure commissione dei medesimi reati nell'esercizio di un'attività di impresa		
3 bis	Falsificazione o alterazione di certificati licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati	fino a 250 quote, se per il reato è prevista la pena non superiore nel massimo a un anno di reclusione, da 150 a 250 quote se è prevista la pena non superiore nel massimo a due anni, da 200 a 300 quote se la pena non è superiore nel massimo a tre anni di reclusione, da 300 a 500 quote se la pena è superiore nel massimo a 3 anni di reclusione	No

4. L. 28 dicembre 1193 n. 549 Misure a tutela dell'ozono stratosferico e dell'ambiente

Articolo	Illecito	Sanzione pecuniaria	Sanzioni interdittive
3 (comma 6)	Produzione, consumo, importazione, esportazione, detenzione e commercializzazione delle sostanze lesive di cui alla Tabella A	da 150 a 250 quote	No

5. D.lgs. 6 novembre 2007 Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni

Articolo	Illecito	Sanzione pecuniaria	Sanzioni interdittive
9 (comma 1)	Inquinamento colposo prodotto da una nave, nonché dai membri dell'equipaggio	fino a 250 quote	No
8 (comma 1) e 9 (comma 2)	Inquinamento doloso prodotto da una nave nonché dai membri dell'equipaggio e inquinamento colposo	da 150 a 250 quote	si, per una durata non superiore a 6 mesi. È prevista inoltre l'interdizione definitiva

	che causi danni permanenti o, comunque, di particolare gravità		dall'esercizio dell'attività ai sensi dell'art. 16 comma 3 del Decreto se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato
8 (comma 2)	Inquinamento colposo prodotto da una nave nonché dai membri dell'equipaggio che causi danni permanenti o, comunque, di particolare gravità	da 200 a 300 quote	si, per una durata non superiore a 6 mesi È prevista inoltre l'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16 comma 3 del Decreto se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

1. Codice Penale

Come anticipato, con diversi interventi normativi sono stati inseriti nel codice penale alcuni reati in materia ambientale. Con l'ultimo di questi interventi, il d.lgs. 1° marzo 2018 n. 21, è stato "spostato" nel codice penale il reato di *Attività organizzate per il traffico illecito di rifiuti*, collocato all'art. 452 *quaterdecies*, con conseguente abrogazione dell'art. 260 del Codice dell'Ambiente che prima disciplinava tale fattispecie, rimasta comunque, quanto al suo contenuto, immutata.

Inquinamento ambientale (art. 452 bis c.p.)

La norma punisce chiunque abusivamente cagiona una compromissione o un deterioramento significativi e misurabili dell'acqua o dell'aria o di porzioni estese o significative del suolo o del sottosuolo; ovvero di un ecosistema, della biodiversità, anche agraria, della flora o della fauna. Costituiscono circostanze aggravanti il fatto che l'inquinamento sia prodotto in un'area naturale protetta o sottoposta a vincolo paesaggistico, ambientale, storico, artistico, architettonico o archeologico, ovvero in danno di specie animali o vegetali protette.

Disastro ambientale (art. 452 quater c.p.)

La norma punisce chiunque abusivamente cagiona un disastro ambientale.

La stessa norma definisce il disastro ambientale quale, in alternativa, un'alterazione irreversibile dell'equilibrio di un ecosistema oppure un'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali.

Delitti colposi contro l'ambiente (art. 452 *quinqies* c.p.)

La norma punisce le medesime condotte che costituiscono i reati di Inquinamento ambientale e *Disastro ambientale* (rispettivamente previste dagli artt. 452-bis e 452-quater c.p.), estendendone la punibilità anche ai casi di fattispecie commesse con semplice colpa.

Traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.)

Il reato punisce chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività.

Associazione (art. 452 *octies* c.p.)

La norma punisce l'associazione (comune o di tipo mafioso) finalizzata alla commissione dei reati ambientali.

Attività organizzata per il traffico illecito di rifiuti (ex art. 260 Codice dell'Ambiente, oggi art. 452 *quaterdecies* c.p.)

La norma punisce chi, al fine di conseguire un ingiusto profitto, in più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, si occupa del traffico illecito di ingenti quantitativi di rifiuti.

Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727 *bis* c.p.)

La norma punisce la condotta di chi, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.

È inoltre punito chi distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta.

Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733 *bis* c.p.)

È punito chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione.

2. Codice dell'Ambiente

Scarichi di acque reflue (art. 137)

comma 2

La norma punisce la condotta di chi apra o comunque effettui nuovi scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del Codice dell'Ambiente, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata.

comma 3

Punisce chiunque effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del Codice dell'Ambiente senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a norma degli articoli 107, comma 1, e 108, comma 4.

comma 5

È punita la condotta di chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del Codice dell'Ambiente, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del Codice dell'Ambiente, oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1.

Circostanza aggravante è che vengano superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5 al Codice dell'Ambiente.

comma 11

La norma punisce la condotta di chi non osservi i divieti di scarico previsti dagli articoli 103 e 104 del Codice dell'Ambiente, con la sanzione pecuniaria da 200 a 300 quote. È prevista inoltre l'applicazione delle misure interdittive di cui all'art. 9 comma 2 del Decreto, per un periodo massimo di sei mesi.

comma 13

È punito lo scarico nelle acque del mare da parte di navi od aeromobili che contenga sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente.

Attività di gestione di rifiuti non autorizzata (art. 256)

comma 1 lettere a) e b)

La norma punisce la condotta di chiunque effettua un'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione ai sensi degli articoli 208- 212 e 214-216 del Codice dell'Ambiente.

La pena è aggravata se si tratta di rifiuti pericolosi.

comma 3

La condotta punita è quella di chiunque realizza o gestisce una discarica non autorizzata.

La pena è aggravata se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi.

comma 4

Sono altresì punite l'inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché la carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni.

comma 5

La norma punisce chi, in violazione del divieto di cui all'articolo 187 del Codice dell'Ambiente, effettua attività non consentite di miscelazione di rifiuti.

comma 6 primo periodo

La norma punisce la condotta di chi effettua il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b) del Codice dell'Ambiente.

Bonifica dei siti (art. 257)

comma 1

La norma punisce la condotta di chi cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti del Codice dell'Ambiente. È inoltre punito chi non effettua la comunicazione di cui all'articolo 242.

comma 2

Se l'inquinamento in esame è provocato da sostanze pericolose, si la pena è aggravata.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258)

comma 4

La norma è indirizzata alle imprese che raccolgono e trasportano i propri rifiuti non pericolosi di cui all'articolo 212, comma 8, e che non aderiscono, su base volontaria, al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all'articolo 188-bis, comma 2, lettera a). La condotta punita consiste nella predisposizione di un certificato di analisi di rifiuti, con indicazione di informazioni false circa la natura, la composizione e le caratteristiche chimico-fisiche dei rifiuti. È infine punito anche l'uso di un certificato falso durante il trasporto.

Traffico illecito di rifiuti (art. 259)

comma 1

La norma punisce la condotta di chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del Regolamento (CEE) 1° febbraio 1993 n. 259 o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d) del regolamento stesso.

La sanzione è aumentata se si tratta di rifiuti pericolosi.

Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis)

comma 6

La norma punisce la condotta di chi, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e di chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.

comma 7 secondo e terzo periodo

È altresì punita la condotta del trasportatore di rifiuti pericolosi che omette di accompagnare il trasporto con la copia del formulario per il trasporto dei rifiuti. È punita altresì la condotta di colui che, durante il trasporto, fa uso di un certificato di analisi per il trasporto dei rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.

comma 8 primo e secondo periodo

È punita infine, la condotta del trasportatore che accompagna il trasporto di rifiuti con una copia cartacea del formulario per il trasporto fraudolentemente alterata. Se si tratta di rifiuti pericolosi, la sanzione è aumentata.

Sanzioni (Violazioni dei limiti di emissioni art. 279)

comma 5

È punita la condotta di chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del Codice dell'Ambiente, dai piani e dai programmi o dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente, se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.

3. L. 7 febbraio 1992 n. 150

Artt. 1, 2 e 6

comma 1

La norma punisce l'importazione, l'esportazione, il trasporto e l'uso illecito di specie animali e il commercio di piante riprodotte artificialmente.

Art. 3 bis

La norma punisce la falsificazione o alterazione di certificazioni e licenze nonché l'uso di certificazioni e licenze falsi o alterati per l'importazione di animali.

La sanzione pecuniaria varia a seconda della specifica condotta da un minimo 150 quote a un massimo di 500.

4. L. 28 dicembre 1993 n. 549

Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3)

La norma punisce la violazione delle disposizioni sull'impiego delle sostanze nocive per lo strato di ozono.

5. D. lgs. 6 novembre 2007 n. 202

Inquinamento doloso (art. 8)

La condotta punita è lo sversamento doloso in mare da navi di sostanze inquinanti. Nel caso invece in cui dallo sversamento derivino danni permanenti, la sanzione pecuniaria è elevata.

Inquinamento colposo (art. 9)

La norma punisce lo sversamento colposo in mare da navi di sostanze inquinanti.

Se la medesima condotta causa danni permanenti, la pena è aggravata.

2. VALUTAZIONE DELLE AREE DI RISCHIO

L'ampio ambito dei reati ambientali introdotto nel Decreto comporta evidentemente un rischio per la società di commissione dei reati in questione.

Data Appeal pone il rispetto dell'ambiente tra i principi cardine della propria attività aziendale. Il Codice Etico della Società sottolinea infatti l'impegno suo e dei suoi dipendenti a far sì che l'azienda possa operare nel pieno rispetto dell'ambiente e in modo minimizzare quanto più possibile l'impatto dello svolgimento della sua Attività.

Al di là di fattispecie limite, che non si ritiene possano comportare nemmeno astrattamente un rischio per la Società tenuto conto dell'Attività dalla stessa esercitata – quali, a titolo esemplificativo, l'inquinamento doloso o colposo da navi, ovvero il commercio illecito di specie animali e vegetali – è evidente che altre fattispecie tra quelle sopra descritte, concernenti le attività e le modalità di smaltimento dei rifiuti, nonché l'inquinamento del suolo, del sottosuolo, e delle acque, coinvolgono, in maniera più o meno incisiva, l'esercizio di qualsiasi attività di impresa.

Ed è appunto in relazione a queste specifiche fattispecie che si è riscontrato un potenziale rischio di commissione anche per Data Appeal.

Va subito precisato che la Società non svolge attività produttiva industriale.

Sulla base dell'analisi di rischio condotta, si può quindi ritenere che l'unica area più a rischio è solamente quella che riguarda la gestione aziendale del ciclo dei rifiuti.

L'analisi condotta ha comunque consentito di evidenziare un rischio remoto di commissione dei reati di cui alla presente Parte Speciale da parte della Società.

La tipologia di rifiuti prodotta da Data Appeal attiene alla tipica attività d'ufficio, e consiste nello smaltimento di rifiuti quale carta, cartone, imballaggi, plastica, ecc. La raccolta e il conferimento dei rifiuti al pubblico servizio è gestita, secondo specifiche previsioni contrattuali, da Nana Bianca, in quanto dispone e gestisce delle infrastrutture di *coworking*. I rifiuti vengono quindi smaltiti direttamente dagli esercenti il pubblico servizio, secondo le disposizioni comunali.

Altra tipologia di prodotti oggetto di smaltimento, una volta cessato il loro uso, è quella delle apparecchiature elettroniche, e dei materiali da questa prodotti e/o di scarto (es. toner esauriti). Data Appeal non è proprietaria di dispositivi e/o apparecchi elettronici d'ufficio (pc, stampanti, telefoni, etc.), in quanto utilizza tali dispositivi in forza di contratti di *leasing* stipulati con diverse società, le quali si occupano di ritirare le apparecchiature da Data Appeal ogni volta che si renda necessario sostituirle, e provvedono poi al loro successivo smaltimento. La Società di norma non è proprietaria di dispositivi elettronici, nei casi sporadici in cui ciò accade (es. telefoni cellulari), Data Appeal si fa carico del relativo smaltimento.

3. PRINCIPI GENERALI DI COMPORTAMENTO

Data Appeal si impegna al rispetto dei seguenti principi generali e regole di comportamento, che costituiscono adempimenti richiesti anche a tutti i Destinatari del Modello:

- astenersi da comportamenti tali da integrare le fattispecie di reato sopra descritte;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- verificare costantemente la conformità alle prescrizioni normative in materia ambientale dell'attività aziendale, nonché degli ambienti, degli strumenti e dei macchinari utilizzati per il suo esercizio;
- adeguare l'attività aziendale, gli ambienti, gli strumenti e i macchinari utilizzati per il suo esercizio alle prescrizioni normative ogni qual volta si renda necessario;
- attenersi alle disposizioni contenute nelle autorizzazioni previste dalle norme di legge ed emanate dalle competenti autorità e uffici pubblici;
- rispettare le indicazioni aziendali previste in materia di raccolta differenziata dei rifiuti e loro smaltimento ed in particolare conformarsi alla gestione dei rifiuti in forza presso le infrastrutture di Nana Bianca;
- monitorare lo stato di integrità degli apparecchi e dei sistemi utilizzati, avendo cura di segnalare ogni difetto e/o vizio che possa ritenersi fonte di possibile inquinamento;
- conservare adeguatamente i beni messi a disposizione dalla Società;

- monitorare costantemente eventuali incidenti e situazioni di emergenza e predisporre adeguate attività di prevenzione.

Resta salvo comunque l'obbligo, a carico di tutti i Destinatari del presente Modello, di segnalare immediatamente e senza indugio all'Organismo di Vigilanza qualsiasi fatto che costituisca violazione – o qualsiasi condotta anomala che possa costituire violazione – delle regole di condotta e delle procedure previste dalla presente Parte Speciale.

PARTE SPECIALE “L”

Delitti contro la personalità individuale

1. LA TIPOLOGIA DELL’ILLECITO RILEVANTE (ART. 25 QUINQUIES DEL DECRETO)

La legge 11 agosto 2003, n. 228 ha inserito nel Decreto l’articolo 25 *quinquies*, che ha introdotto tra i Reati Presupposto i delitti contro la personalità individuale.

Si tratta, in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
600 c.p.	Riduzione o in mantenimento schiavitù	da 400 a 1.000 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l’eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
601 c.p.	Tratta di persone	da 400 a 1.000 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
602 c.p.	Acquisto e alienazione di schiavi	da 400 a 1.000 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
603 bis c.p.	Intermediazione illecita e sfruttamento del lavoro	da 400 a 1.000 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
600 <i>bis</i> c.p. comma 1	Sfruttamento della prostituzione minorile	da 300 a 800 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
600 <i>ter</i> c.p. comma 1 e 2	Pornografia minorile	da 300 a 800 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
600 <i>quinquies</i> c.p.	Iniziative turistiche volte allo sfruttamento della prostituzione minorile	da 300 a 800 quote	si, per una durata non superiore ad un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di

			pubblicizzare beni o servizi.
600 <i>bis</i> c.p. comma 2	Prostituzione minorile	da 200 a 700 quote	no
600 <i>ter</i> c.p. comma 3 e 4	Commercio e divulgazione di materiale pedopornografico	da 200 a 700 quote	no
600 <i>quater</i> c.p.	Pornografia virtuale	da 200 a 700 quote	no
609 <i>undecies</i> c.p.	Adescamento di minorenni	da 200 a 700 quote	no

L'art. 25 *quinquies* del Decreto prevede inoltre che nel caso in cui l'Ente venga stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati qui in esame, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa, seguendo un ordine basato sul bene protetto da ciascuna categoria di reati.

Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)

La norma punisce la condotta di chi eserciti su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduca o mantenga una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento.

La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

Prostituzione minorile (art. 600 *bis* c.p.)

Le condotte punite dalla norma in esame sono quelle di chi:

- 1) recluta o induce alla prostituzione una persona di età inferiore agli anni diciotto;
- 2) favorisce, sfrutta, gestisce, organizza o controlla la prostituzione di una persona di età inferiore agli anni diciotto, ovvero altrimenti ne trae profitto.

Salvo che il fatto costituisca più grave reato, è punito anche chi compie atti sessuali con un minore di età compresa tra i quattordici e i diciotto anni, in cambio di un corrispettivo in denaro o altra utilità, anche solo promessi (comma 2).

Pornografia minorile (art. 600 *ter* c.p.)

È punito chi:

- 1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico;

2) recluta o induce minori di anni diciotto a partecipare a esibizioni o spettacoli pornografici ovvero dai suddetti spettacoli trae altrimenti profitto.

Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.

È inoltre punito anche chi, al di fuori delle ipotesi sopra descritte, distribuisce, divulga, diffonde o pubblicizza con qualsiasi mezzo, anche per via telematica, il materiale pedopornografico, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, o ancora offre o cede a terzi, anche a titolo gratuito, materiale pedopornografico.

Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

Detenzione di materiale pornografico (art. 600 quater c.p.)

La norma punisce la condotta di chi, al di fuori delle ipotesi previste dall'articolo 600-ter sopra descritte, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto.

Pornografia virtuale (art. 600 quater1 c.p.)

Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse.

Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.)

La condotta sanzionata è quella di chi organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività.

Tratta di persone (art. 601 c.p.)

La condotta sanzionata in questo è quella di chi recluta, introduce nel territorio dello Stato, trasferisce anche al di fuori di esso, trasporta, cede l'autorità sulla persona, ospita una o più persone che si trovano nelle condizioni di cui all'art. 600 c.p. (e quindi siano stati ridotti o mantenuti in schiavitù), ovvero, realizza le stesse condotte su una o più persone, mediante inganno, violenza, minaccia, abuso di autorità o approfittamento di una situazione di vulnerabilità, di inferiorità fisica, psichica o di necessità, o mediante promessa o dazione di denaro o di altri vantaggi alla persona che su di essa ha autorità, al fine di indurle o costringerle a prestazioni lavorative, sessuali ovvero all'accattonaggio o comunque al compimento di attività illecite che ne comportano lo sfruttamento o a sottoporsi al prelievo di organi.

Sono punite anche le condotte sopra descritte, compiute nei confronti di persona minore di età.

Acquisto e alienazione di schiavi (art. 602 c.p.)

La condotta punita è quella di chi, al di fuori dei casi indicati nell'art. 601 c.p. (i.e. Tratta di persone), acquista o aliena o cede una persona che si trova in una delle condizioni di cui all'art. 600 c.p. (Riduzione e mantenimento in schiavitù).

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

Le condotte punite dalla norma sono quelle di chi:

- 1) recluta manodopera allo scopo di destinarla al lavoro presso terzi in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori;
- 2) utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

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

- 1) la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
- 2) la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
- 3) la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
- 4) la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

Adescamento di minorenni (art. 609 undecies c.p.)

La norma punisce la condotta di chi, allo scopo di commettere uno dei reati sopra descritti, adesci un minore di anni sedici.

Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione.

2. AREE A RISCHIO

L'Attività di Data Appeal non comporta di per sé un rischio di commissione dei reati oggetto della presente Parte Speciale.

La Società, inoltre, non stipula contratti di appalto di servizi con Cooperative e con altri fornitori che impiegano o potrebbero impiegare tra i propri soci lavoratori e dipendenti anche individui provenienti da paesi extra – comunitari ed in particolare da Paesi del Terzo Mondo, ciò che comporterebbe il rischio, quanto meno indiretto, che possa configurarsi una responsabilità amministrativa a carico della Società per il caso in cui la Cooperativa commetta uno dei reati in esame, ed in particolare quelli di “*Riduzione o mantenimento in schiavitù o servitù*” (art. 600 c.p.), e di “*Tratta di persone*” (art. 601 c.p.).

Pertanto, dall'analisi dei rischi effettuata, il profilo di rischio relativo alla commissione di tali fattispecie di reati si può, allo stato attuale, ragionevolmente escludere.

Data Appeal ha tuttavia ritenuto opportuno predisporre la presente Parte Speciale, anche nell'ottica di eventuali e futuri contratti di appalti di servizi, al fine di delineare alcuni principi generali di condotta.

3. REGOLE GENERALI DI CONDOTTA

Data Appeal ha sempre fatto del rispetto della normativa in materia di lavoro e sindacale, con riguardo in particolare al lavoro minorile ed alle disposizioni in materia di tutela della salute e della sicurezza nei luoghi di lavoro, i principi ispiratori della propria attività d'impresa.

Allo stesso modo, il rispetto della libertà e della dignità della persona sono principi che regolano tutta l'Attività della Società e sono ribaditi dal Codice Etico adottato dalla Società e su cui viene periodicamente fatta specifica formazione nei confronti di tutti i dipendenti.

Data Appeal promuove attivamente il rispetto di tali principi anche da parte dei propri collaboratori, fornitori e *partner* commerciali.

Anche la violazione di tali principi da parte di uno dei soggetti terzi con cui Data Appeal sottoscrive contratti o accordi commerciali costituisce violazione delle regole di condotta stabilite dal presente Modello e, pertanto, causa di risoluzione automatica del contratto in essere.

Data Appeal verifica inoltre espressamente, in sede di assunzione del proprio personale, che non sussistano condizioni tali per cui l'individuo da assumere si trovi in una delle situazioni previste dai Reati Presupposto qui in esame. A tal fine, costituiscono elementi che dovranno indurre ad una particolare attenzione in sede di assunzione la nazionalità della persona, la sua età ed il costo della manodopera offerta. Al fine di ridurre quanto più possibile il rischio di commissione dei reati in esame, in ogni caso, i contratti stipulati tra Data Appeal con i propri partner commerciali e fornitori prevedono espressamente l'impegno di questi ultimi al rispetto della normativa esistente, per quel che qui interessa, in materia di immigrazione, di sicurezza ed igiene sul luogo di lavoro.

Per tutti questi motivi, come sopra illustrato, Data Appeal non ritiene che sussista un rischio concreto e diretto della commissione di alcuno dei reati oggetto di esame nella presente Parte Speciale.

La Società prevede inoltre, a carico di tutti i Destinatari del presente Modello, l'obbligo specifico di segnalare tempestivamente all'Organismo di Vigilanza qualsiasi situazione che comporti, anche solo astrattamente, il rischio di commissione di uno dei reati qui oggetto di esame.

PARTE SPECIALE “M”

Impiego di immigrati irregolari

1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 DUODECIES)

Il 9 agosto 2012 è entrato in vigore il d.lgs. 16 luglio 2012 n. 109 che ha dato attuazione alla direttiva 2009/52/CE, e ha introdotto norme minime relative a sanzioni e a provvedimenti nei confronti dei datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare.

La norma ha inoltre introdotto nel Decreto il nuovo art. 25 *duodecies*, intitolato “*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*”, che ha esteso la responsabilità dell’ente anche al delitto previsto dall’art. 22 comma 12 *bis* del d.lgs. 25 luglio 1998 n. 286. Con un ulteriore intervento del 2017 (in particolare, la l. 17 ottobre 2017 n. 16), la responsabilità dell’Ente è stata estesa anche ai reati previsti dall’art. 12 commi 3, 3 *bis*, 3 *ter* e comma 5 del medesimo decreto legislativo 25 luglio 1998 n. 286, c.d. Testo Unico sull’Immigrazione.

Si tratta quindi, e in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito e tutte previste, come anticipato, dal Testo Unico sull’Immigrazione.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
22 comma 12 <i>bis</i>	Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare	da 100 a 200 quote, entro il limite comunque di Euro 150.000	no
12 comma 3	Trasporto di stranieri nello Stato per il loro ingresso illecito	da 400 a 1.000 quote	si, per una durata non inferiore a un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l’eventuale revoca di quelli già concessi; divieto di

			pubblicizzare beni o servizi.
12 comma 3 <i>bis</i>	Trasporto di stranieri nello Stato per il loro ingresso illecito (ipotesi aggravata)	da 400 a 1.000 quote	si, per una durata non inferiore a un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
12 comma 3 <i>ter</i>	Trasporto di stranieri nello Stato per il loro ingresso illecito ai fini dello sfruttamento della prostituzione	da 400 a 1.000 quote	si, per una durata non inferiore a un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti,

			contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
12 comma 5	Favoreggiamento della illecita presenza nello Stato di stranieri irregolari	da 100 a 200 quote	si, per una durata non inferiore a un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti oggetto della presente Parte Speciale.

Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 bis Testo Unico sull'Immigrazione)

La norma in esame, a sua volta modificata dal d.lgs. 16 luglio 2012 n. 109, punisce la condotta del datore di lavoro che occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, ovvero, ancora, il cui rinnovo del permesso di soggiorno sia stato revocato o annullato.

La norma punisce il datore di lavoro che impiega cittadini di Paesi il cui soggiorno nel territorio italiano è irregolare per uno dei motivi sopra descritti, quando i lavoratori irregolari impiegati sono (i) in numero superiore a tre, (ii) sono minori in età lavorativa, (iii) sono sottoposti a condizioni lavorative di particolare sfruttamento ai sensi dell'art. 603 *bis* comma 3 c.p. (ossia sono esposti a

situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro).

Trasporto di stranieri nello Stato per il loro ingresso illecito (art. 12 commi 3, 3 bis, 3 ter e 5 del Testo Unico sull'Immigrazione)

Si tratta di nuove fattispecie di recente introduzione tra i Reati Presupposto.

La condotta punita dal comma 3 è quella di chi, violando le disposizioni del Testo Unico sull'Immigrazione, promuove, dirige, organizza, finanzia o effettua il trasporto di stranieri nel territorio dello Stato, ovvero compie altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato o di un altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente.

La rilevanza penale del comportamento è peraltro subordinata alla sussistenza di almeno una delle seguenti condizioni:

- il fatto riguarda l'ingresso o la permanenza nel territorio dello Stato di cinque o più persone;
- la persona trasportata è stata esposta a pericolo per la sua vita o per la sua incolumità per procurarne l'ingresso o la permanenza illegale;
- la persona trasportata è stata sottoposta a trattamento inumano o degradante per procurarne l'ingresso o la permanenza illegale;
- il fatto è commesso da tre o più persone in concorso tra loro o utilizzando servizi internazionali di trasporto ovvero documenti contraffatti o alterati o comunque illegalmente ottenuti;
- gli autori del fatto hanno la disponibilità di armi o materiali esplosivi.

Comma 3-bis

La norma prevede una fattispecie aggravata per il caso in cui il reato previsto dal comma 3 del medesimo articolo venga commesso in presenza di più di una delle condizioni richieste per la configurazione dello stesso.

Comma 3-ter

Un'ulteriore ipotesi aggravata è prevista per il caso in cui le condotte sopra descritte:

- sono commesse allo scopo di reclutare persone da destinare alla prostituzione, allo sfruttamento sessuale o lavorativo, ovvero riguardano l'ingresso di minori da impiegare in attività illecite al fine di favorirne lo sfruttamento;
- sono commesse al fine di trarne profitto, anche indiretto.

Comma 5

La norma punisce infine chi, fuori dai casi previsti dai commi precedenti e salvo che il fatto non costituisca più grave reato, favorisca la permanenza di un soggetto straniero nel territorio dello Stato al fine di trarre un profitto ingiusto dalla condizione di illegalità di quest'ultimo o nell'ambito delle attività unite a norma dello stesso articolo.

2. VALUTAZIONE DELLE AREE DI RISCHIO

Data Appeal può impiegare alle proprie dipendenze lavoratori stranieri, soprattutto studenti e/o dottorandi di ricerca dunque solitamente per periodi brevi e circoscritti. In ogni caso, la Società provvede sempre ad accertare in via preventiva la regolarità della permanenza nel territorio italiani di cittadini stranieri che dovessero essere eventualmente assunti, anche per brevi periodi. Non solo,

la funzione HR esegue uno specifico controllo periodico circa il mantenimento dei requisiti di regolarità per il soggiorno nel territorio italiano.

La Società, invece, non assume lavoratori minori di età.

Il rischio di commissione del reato di cui alla presente Parte Speciale è quindi molto contenuto.

Ciononostante, Data Appeal ha deciso di dedicare al reato di impiego di personale irregolare una specifica Parte Speciale del Modello per dettare alcune norme generali di comportamento, cui i Destinatari sono tenuti ad uniformarsi, da un lato, per sottolineare il principio del rispetto della persona, che costituisce uno dei cardini della Società ed è sintetizzato nel suo Codice Etico; dall'altro lato, la Società ha deciso di dettare una serie di regole generali di comportamento da utilizzarsi in tutti i casi – comunque possibili – di assunzione di cittadini stranieri.

A tal fine, si precisa che nonostante il c.d. reato di “caporalato” previsto dall’art. 603 *bis* c.p. (“*Intermediazione illecita e sfruttamento del lavoro*”) non sia incluso nell’ambito dei Reati Presupposto (con esclusione quindi per tale fattispecie della responsabilità amministrativa dell’Ente), la Società, dato il richiamo indiretto a tale reato contenuta nell’art. 22 comma 12 *bis* del Testo Unico sull’Immigrazione (a sua volta richiamato dal nuovo art. 25 *duodecies* del Decreto), ha deciso di dettare anche in relazione a tale condotta, ad ulteriore tutela della correttezza del proprio operato in tema di assunzioni, alcuni principi specifici di comportamento.

L’area eventualmente a rischio di commissione del reato in esame è quella relativa all’assunzione di nuovo personale, affidata alla funzione HR o quella dell’utilizzo di fornitori ai quali vengono appaltati specifici servizi.

3. PRINCIPI GENERALI DI COMPORTAMENTO

Data Appeal si impegna al rispetto dei seguenti principi generali e regole di comportamento, che costituiscono adempimenti richiesti anche a tutti i Destinatari del Modello:

- astenersi da comportamenti tali da integrare le fattispecie di reato sopra descritte;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- è fatto assoluto divieto di impiegare lavoratori stranieri del tutto privi del permesso di soggiorno, o con un permesso revocato o scaduto, del quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale;
- verificare in sede di assunzione di lavoratori stranieri il rilascio in loro favore di valido documento di soggiorno che li abiliti a prestare lavoro in Italia;
- in caso di assunzione di lavoratori stranieri, verificare periodicamente la regolarità del documento di soggiorno, verificando altresì che il lavoratore abbia tempestivamente provveduto alla richiesta di rinnovo prima della sua scadenza;
- è fatto divieto assoluto di procedere all’assunzione di personale per il tramite di intermediari per il reclutamento del lavoro che non siano le Agenzie per il lavoro autorizzate dal Ministero del Lavoro;
- verificare, in caso di ricorso alle Agenzie autorizzate dal Ministero del lavoro per il reclutamento del personale, il rispetto della normativa vigente in merito alla corresponsione dei trattamenti retributivi e dei contributi previdenziali, attraverso l’obbligo a carico di tali Agenzie, e pena la risoluzione del rapporto con la Società,

di fornire idonea documentazione comprovante l'adempimento dei relativi obblighi retributivi e previdenziali.

PARTE SPECIALE “N”

Delitti di criminalità organizzata

1. LA TIPOLOGIA DELL'ILLECITO RILEVANTE (ART. 24 *QUATER* DEL DECRETO)

La legge 15 luglio 2009 n. 94 ha inserito nel Decreto l'articolo 24 *quater*, che ha esteso la responsabilità amministrativa dell'Ente anche ai reati c.d. di criminalità organizzata.

Si tratta quindi, e in particolare, delle seguenti fattispecie di reato, schematicamente riassunte qui di seguito.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
416 c.p. comma 6	Associazioni delinquere per	da 400 a 1.000 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
416 bis c.p.	Associazioni di tipo mafioso	da 400 a 1.000 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
416 <i>ter</i> c.p.	Scambio elettorale politico – mafioso	da 400 a 1.000 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
630 c.p.	Sequestro di persona a scopo di estorsione	da 400 a 1.000 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
art. 74 D.P.R. 9 ottobre 1990 n. 309	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	da 400 a 1.000 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
416 c.p. (escluso il comma 6)	Associazione per delinquere	da 300 a 800 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
407 comma 2 lett. a) n. 5 c.p.p.	Delitti in materia di armi	da 300 a 800 quote	si, per una durata non superiore a 1 anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di

			pubblicizzare beni o servizi.
--	--	--	-------------------------------

Per tutti i reati previsti dall'art. 24 *ter*, è prevista la sanzione dell'interdizione definitiva dall'esercizio dell'attività se l'Ente viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei reati descritti.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

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

La norma punisce la condotta di tre o più persone che si associano allo scopo di commettere più delitti. È punita in particolare non solo la promozione, la costruzione o l'organizzazione dell'associazione, ma anche la semplice partecipazione alla stessa.

Pene più severe sono previste per il caso in cui gli associati ricorrano all'uso di armi, e nell'ipotesi in cui gli associati siano dieci o più.

Costituiscono condotte aggravanti quelle descritte dal comma 6 della norma, per le quali l'art. 24 *bis* comma 1 del Decreto prevede una sanzione pecuniaria più grave; si tratta dei casi in cui l'associazione sia diretta a commettere uno dei delitti di cui agli artt. 600 (*Riduzione o mantenimento in schiavitù o in servitù*), 601 (*Tratta di persone*) e 602 c.p. (*Acquisto e alienazione di schiavi*), nonché all'art. 12, comma 3-bis, del Testo Unico sull'Immigrazione.

Associazioni di tipo mafioso anche straniera (art. 416 bis c.p.)

La condotta punita è la partecipazione ad un'associazione di tipo mafioso formata da tre o più persone.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Scambio elettorale politico-mafioso (art. 416 ter c.p.)

La norma punisce la condotta di chi ottiene la promessa di voti in cambio della erogazione di denaro.

Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.)

La condotta punita è quella di chi sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione.

Pene più severe sono previste nel caso in cui dal sequestro derivi la morte della persona sequestrata.

Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990 n. 309)

La norma punisce la condotta di tre o più persone che si associano allo scopo di commettere più delitti tra quelli previsti dall'articolo 73 (ossia, Produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope). Le condotte sanzionate sono non solo la promozione, la costituzione, la direzione, l'organizzazione e il finanziamento dell'associazione, ma anche la semplice partecipazione alla stessa.

Delitti in materia di armi (art. 407 comma 2 lett. a) n. 5 c.p.p.)

La norma punisca la illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo.

2. AREA A RISCHIO

L'Attività di Data Appeal non comporta di per sé un rischio di commissione dei reati oggetto della presente Parte Speciale.

Per molti di essi (quelli legati agli stupefacenti, alla tratta di persone, allo scambio elettorale politico-mafioso e di sequestri di persona) il rischio è addirittura pressoché solo teorico.

Da un diverso punto di vista, però, deve essere chiaro che il reato di associazione a delinquere per così dire comune (art. 416 c.p.) rappresenta una fattispecie amplissima e frequentissimamente ricorrente.

Sarebbe, infatti, un errore pensare che si abbia violazione di questa norma solo nei casi di bande armate o simili: in realtà, la fattispecie è, come detto, integrata ogni volta che tre persone diano vita ad un che si propone di commettere una serie non precisata di illeciti.

Ciò sta a dire che se più dipendenti cooperassero per commettere una serie di illeciti a vantaggio della società, ben potrebbe esservi la contestazione, oltre a quella dei reati materialmente realizzati (cd. reati fine dell'associazione) anche del reato di associazione per delinquere.

Ciò equivarrebbe in ogni caso ad un sensibile aggravio della responsabilità amministrativa della società, che dovrebbe rispondere anche della violazione dell'art. 416 c.p.

Addirittura, potrebbe persino accadere che la commissione, da parte di tre o più soggetti, di delitti non ricompresi tra quelli sanzionati dal Decreto (e che quindi in sé non produrrebbero conseguenze per la società) potrebbe comunque portare alla responsabilità dell'ente proprio per effetto della violazione dell'art. 416 c.p.

Non vi devono peraltro essere equivoci sotto un diverso profilo: perché si integri il reato non è certo necessario che i membri dell'associazione siano tutti dipendenti o comunque soggetti ricollegabili alla società. Ben può accadere che il reato sia contestato, quindi, anche nel caso in cui il dipendente di una società commetta alcuni illeciti a vantaggio della stessa, avvalendosi o cooperando con due o più soggetti esterni all'ente: ciò rende certamente rilevanti tutti i rapporti con collaboratori e professionisti esterni, partner commerciali, dirigenti e dipendenti di altre società che, in ipotesi, si trovino a cooperare con Data Appeal.

3. REGOLE GENERALI DI CONDOTTA

Data Appeal si è sempre preoccupata di improntare la propria attività d'impresa a regole generali di condotta volte a garantire, nei rapporti anche tra i dipendenti, il rispetto di principi etici e di legalità.

Data Appeal inoltre ha sempre fatto del rispetto della normativa in materia di lavoro e sindacale, con riguardo in particolare, per quel che in questa sede interessa, al diritto di associazione, i principi ispiratori della propria attività d'impresa.

Data Appeal promuove attivamente il rispetto di tali principi anche da parte dei propri collaboratori, fornitori e partner commerciali.

Se quindi, da un lato, la Società promuove e garantisce il diritto di tutti i propri dipendenti di associarsi liberamente, dall'altro, l'associazione e la cooperazione tra i dipendenti (che sono parte essenziale e strutturale dell'organizzazione di impresa) devono comunque essere oggetto di cautela ed attenzione.

È espressamente vietata pertanto all'interno della Società qualsiasi forma di collaborazione, associazione e cooperazione tra dipendenti che si fondi su modalità operative e procedurali difformi

da quelle dettate dal Modello, dalle Parti Speciali e da ogni altro atto regolamentare aziendale. Analoga regola deve valere per ogni forma di cooperazione tra dipendenti o soggetti comunque appartenenti alla società e soggetti esterni alla stessa.

Più in generale è fatto espresso divieto ad ogni dipendente della Società, nell'esercizio dell'attività aziendale, di avvalersi, in ogni forma, del contributo o della collaborazione di soggetti esterni che non siano collegati (o non appartengano a soggetti collegati) alla società da un formale rapporto contrattuale.

Sotto questi profili, si rende sempre necessaria la attiva e concreta partecipazione di tutti i Destinatari del Modello affinché lo stesso possa avere efficace attuazione all'interno della Società.

La Società prevede quindi, a carico di tutti i Destinatari del presente Modello, l'obbligo specifico di segnalare tempestivamente all'Organismo di Vigilanza qualsiasi situazione che comporti, anche solo astrattamente, il rischio di commissione di uno dei reati qui oggetto di esame.

PARTE SPECIALE “O”

Corruzione tra privati e istigazione alla corruzione tra privati

1. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 TER, COMMA 1, LETT. S-BIS)

La l. 6 novembre 2012 n. 190, oltre ad apportare significative modifiche nel nostro ordinamento in merito ad alcuni dei reati di tipo corruttivo, con l’obiettivo di implementare la prevenzione e la repressione della corruzione e dell’illegalità nella Pubblica Amministrazione, ha anche introdotto, con l’art. 2635 c.c., il nuovo reato denominato “*Corruzione tra privati*”.

Si tratta, in particolare, dei reati schematicamente indicati qui di seguito, e che verranno poi descritti più in dettaglio.

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
2635 c.c. comma 3	Corruzione tra privati	da 400 a 600 quote	si: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l’eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
2625 bis c.c. comma 1	Istigazione alla corruzione	da 200 a 400 quote	si, per non più di un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.
--	--	--	--

La norma punisce la condotta degli amministratori, dei direttori generali, del dirigente preposto alla redazione dei documenti contabili societari, dei sindaci e dei liquidatori che, a seguito della dazione o anche solo della promessa di denaro o di altra utilità, per sé o per altri, compiono o omettono atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando un danno alla società. La responsabilità è estesa anche alle medesime condotte quando siano compiute anche da chi, nell'ambito organizzativo della società o dell'ente privato, esercita funzioni direttive diverse da quelle proprie dei soggetti sopra indicati. Si tratta, in quest'ultimo caso, dei soggetti che esercitano le funzioni tipiche degli amministratori o dei direttori generali, ecc. pur senza una formale investitura.

Una delle principali novità introdotte dall'art. 2635 c.c. consiste nel fatto che la stessa pena è prevista non solo per il soggetto "corrotto", ma anche per il c.d. corruttore, ossia colui che dà o promette denaro o altre utilità.

Sotto il profilo della responsabilità amministrativa degli enti, la l. 190/2012 ha aggiunto la lettera *s-bis*) all'art. 25 *ter* del Decreto, che a sua volta richiama il comma 3 dell'art. 2365 c.c. Entrambe le disposizioni – quindi sia l'art. 2365 c.c. che la lettera *s-bis*) dell'art. 25 *bis* del Decreto sono poi state ulteriormente modificate, l'art. 2365 c.c. in modo significativo, dal d.lgs. 15 marzo 2017 n. 38.

Si deve però notare che la disposizione espressamente richiamata dal Decreto fa riferimento alla sanzione prevista per il solo corruttore. Il richiamo alla sola figura del corruttore implica pertanto che la responsabilità amministrativa degli Enti sia prevista solo a carico, e nella sola ipotesi, della società corruttrice. L'ente sarà quindi responsabile, ai sensi del Decreto, nella sola ipotesi in cui i suoi amministratori, direttori generali, dirigente preposto alla redazione dei documenti contabili societari, sindaci, liquidatori, o soggetti sottoposti alla direzione o alla vigilanza di questi, pongano in essere atti corruttivi.

Con l'intervento del d.lgs. 15 marzo 2017, n. 38, la responsabilità dell'Ente è stata estesa anche condotta di chi offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia o ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.

2. AREE A RISCHIO

Al fine della valutazione delle possibili aree di rischio per la commissione del reato in esame, si deve anzitutto tenere presente che l'art. 2635 c.c., nonostante sia intitolato "*Corruzione tra privati*", trova applicazione solamente nei rapporti tra società. La norma infatti punisce le condotte corruttive che

arrechino un danno al patrimonio sociale, e punisce pertanto la corruzione solamente nel caso in cui determini appunto un nocumento al patrimonio sociale, e non invece la corruzione in quanto tale.

Il richiamo poi espresso al solo comma 3 dell'art. 2635 c.c., ossia a quello che si riferisce alla condotta di chi "*dà o promette denaro o altre utilità*", implica che la responsabilità amministrativa sussista solamente a carico della società i cui esponenti diano o promettano denaro o altre utilità ad esponenti di un'altra società al fine di ottenerne un vantaggio a fronte del nocumento al patrimonio della società di cui fanno parte gli esponenti aziendali corrotti. Per semplificare la ricostruzione della fattispecie, è, quindi, la sola condotta attiva dell'impresa corruttrice che viene punita con le sanzioni previste dal Decreto, e non anche quella, passiva, della società corrotta.

Ne consegue che le potenziali aree a rischio, quindi, per la commissione dei reati in questione sono quelle che riguardano i rapporti tra Data Appeal e le società terze con cui questa entra in contatto nello svolgimento della propria attività aziendale, quali - a titolo esemplificativo - i fornitori, i clienti privati (la Pubblica Amministrazione rientra infatti nelle ipotesi corruttive nei confronti di un pubblico ufficiale/incaricato di un pubblico servizio), i consulenti. Nell'ambito di tali rapporti si potrebbe infatti astrattamente ipotizzare, da parte di dipendenti di Data Appeal, la promessa di una qualche utilità in cambio di prestazioni o servizi a condizioni di maggior favore.

Si tratta, com'è di tutta evidenza, di un rischio immanente nell'attività qualsiasi tipo di società.

In via di principio, sono pertanto da considerarsi a rischio tutte quelle attività aziendali che comportano il relazionarsi, in nome e per conto della Società, e anche in via indiretta o mediata, con società terze nell'ambito di un rapporto di tipo commerciale.

Sono inoltre da considerarsi a rischio tutte quelle attività che, da un lato, potrebbero portare alla creazione dell'utilità che costituisce, in via di estrema semplificazione, il risultato ultimo nonché il fine dell'attività corruttiva. E si tratta quindi di tutte le attività inerenti al c.d. ciclo attivo, quali, a titolo esemplificativo, la definizione del prezzo di offerta di un bene o di un servizio, la definizione delle condizioni e dei termini di pagamento, della scontistica e della definizione di eventuali risoluzioni transattive in caso di contestazioni.

Sotto diverso profilo, sono allo stesso modo da considerarsi a rischio tutte quelle attività attraverso le quali sarebbe possibile costituire la provvista o i fondi necessari per le illecite dazioni o promesse di denaro. Si tratta quindi di tutte le attività relative al c.d. ciclo passivo quali, a titolo esemplificativo, gli acquisti di beni e servizi, l'affidamento di consulenze e altre prestazioni professionali, la gestione del magazzino.

3. I DESTINATARI DELLA PRESENTE PARTE SPECIALE

L'ambito dei potenziali soggetti attivi del reato, ai sensi degli artt. 2635 e 2365 *bis* c.c. è esteso non soltanto agli amministratori, ai direttori generali, e, più in generale, a coloro che sono già stati individuati come i c.d. apicali all'interno della società, ma anche a coloro che svolgono identiche funzioni, pur se in assenza di un'investitura formale, nonché ai soggetti sottoposti alla loro direzione e alla vigilanza.

Va da sé, pertanto, che la presente Parte Speciale è necessariamente indirizzata a tutti i dipendenti della società, nonché a quei terzi che, sottoposti alla vigilanza o alla direzione di un apicale, agiscano nell'interesse e a vantaggio di Data Appeal.

4. REGOLE DI COMPORTAMENTO

Come principio generale, Data Appeal non tollera al proprio interno il ricorso alla tangente o alla corruzione, in qualsiasi forma essa sia attuata, come modalità di svolgimento delle attività aziendali, e ha pertanto già da tempo codificato nel proprio Codice Etico, una serie di principi e di regole generali di comportamento cui i dipendenti delle Società devono rigorosamente attenersi.

La regola generale che guida il comportamento di tutti i Destinatari della presente Parte Speciale, così come sopra individuati, è la seguente

nessuno dei dipendenti o di quanti agiscano in nome e per conto di Data Appeal può offrire, promettere o dare elargizioni in denaro ad alcuno, così come non può richiedere, acconsentire o accettare di ricevere elargizioni in denaro da alcuno

In aggiunta, un piano anticorruptivo interno alla Società per dirsi efficace deve necessariamente passare attraverso i seguenti passaggi/strumenti di verifica:

- Adeguata tenuta dei libri contabili

la prevenzione del rischio di corruzione non può prescindere da un'adeguata ed appropriata conservazione, gestione e registrazione dei libri sociali, conformemente a quanto previsto dal Codice Etico dalle procedure interne adottate dalla Società in ambito contabile e finanziario. È quindi fondamentale che i libri sociali riflettano fedelmente tutte le transazioni poste in essere dalla Società.

- Effettivo controllo interno e monitoraggio

Data Appeal ha già da tempo formalizzato un sistema di controllo interno che prevede che i pagamenti vengano effettuati sempre con il coinvolgimento di almeno due soggetti; che l'accesso ai conti della Società sia consentito solo ai soggetti dei relativi poteri, che periodicamente vengano effettuate verifiche e controlli sui movimenti contabili;

- Diffusione e formazione

Data Appeal cura anche la formazione specifica in materia di anticorruzione ai propri dipendenti, a tutti i livelli. Tali incontri formativi devono essere periodicamente ripetuti nel tempo, non solo per ottemperare alla formazione in caso di nuove assunzioni, ma anche per rinfrescare quella dei dipendenti, in modo che siano sempre presenti ed attuali le necessarie ed adeguate condotte preventive da seguire all'interno della Società.

Data Appeal ha inoltre ritenuto opportuno prevedere specifiche regole di comportamento in relazione ad alcune fattispecie in cui più facilmente potrebbero essere poste in essere degli atti corruttivi, cui i Destinatari della presente Parte Speciale devono strettamente attenersi.

(i) Fornitori

I fornitori hanno l'obbligo di rispettare i principi etici e le regole di comportamento adottati da Data Appeal e sintetizzati nella presente Parte Speciale, oltre che nel suo Codice Etico.

I processi di selezione dei fornitori sono fissati da Data Appeal con apposite procedure che prevedono espressamente la ripartizione dei ruoli ed un doppio controllo nella scelta dei fornitori e i criteri oggettivi di valutazione dei fornitori, nel monitoraggio sul rispetto, da parte di questi, degli standard fissati dalla Società, secondo quanto sopra già riportato.

(ii) Consulenti

I consulenti e gli altri collaboratori che hanno in essere con la Società specifici rapporti di collaborazione formalizzati in appositi contratti, con la finalità di promuovere l'Attività, eventualmente anche promuovendo contatti ed incontri con potenziali clienti.

La Società monitora l'attività svolta dai propri consulenti e collaboratori attraverso un sistema di reportistica costante, tale da consentire la tracciabilità e la verifica di tutte le attività svolte sotto il profilo commerciale. In particolare, è richiesto ad ogni consulente e collaboratore commerciale di fornire *feedback* sui contatti potenziali o avviati, sui rispettivi *deal* e progetti, sin dalla prima occasione di contatto, con indicazione della provenienza del *lead* e ogni informazione utile, sia al fine di scongiurare i fenomeni di corruzione qui presi in esame sia in ottica antiriciclaggio, in ossequio alle relative procedure previste. Tale operazione di reportistica avviene attraverso una specifica comunicazione ed è indirizzata alla funzione Commerciale.

Il rispetto di tale obbligo di rendicontazione è previsto nei contratti che la Società stipula con i consulenti e collaboratori commerciali a pena di risoluzione espressa degli stessi da parte di Data Appeal.

Data Appeal provvede comunque alla verifica periodica circa la conservazione, nel tempo, dei necessari requisiti di correttezza e professionalità dei consulenti incaricati. Identiche verifiche vengono compiute in caso di affidamento di incarichi a nuovi consulenti, con cui Data Appeal non abbia in precedenza intrattenuto alcun rapporto

(iii) Organizzazione di eventi di intrattenimento e di *marketing*

È consentita l'organizzazione di eventi di intrattenimento a condizione che siano connessi con la presentazione o con la promozione dei prodotti o dei servizi offerti da Data Appeal.

Allo stesso modo, è consentita la distribuzione di prodotti promozionali o di *marketing* ai clienti della Società, a condizione che i prodotti promozionali consegnati siano di quantità e importo ragionevoli e comunque sempre connessi al *business* aziendale.

(iv) Omaggi

È vietata qualsiasi forma di regalo a controparti commerciali o a loro familiari o a persone che intrattengono con questi stretti rapporti personali, se non si caratterizzano per l'esiguità del valore o non sono volti a promuovere iniziative di carattere culturale o artistico, o ancora se non sono tesi a promuovere l'attività aziendale.

In ogni caso, i regali e gli omaggi sono sempre preventivamente approvati da Data Appeal. I regali offerti - con la sola eccezione di quelli di modico valore - devono essere documentati in modo adeguato per consentire le prescritte e necessarie verifiche.

Parimenti, la Società ha attuato una stretta *policy* volta a regolamentare le spese sostenute in occasione delle trasferte lavorative.

5. SEGNALAZIONI

In aggiunta alle segnalazioni di ogni violazione, accertata o di cui si abbia anche solo il sospetto, che - conformemente a quanto disposto nella Parte Generale del presente Modello - devono essere indirizzate senza indugio all'Organismo di Vigilanza, ogni condotta che non sia conforme alle procedure anticorruzione descritte nella presente Parte Speciale deve essere segnalata anche alla Responsabile HR.

La Società inoltre raccomanda a tutti i propri dipendenti di rivolgersi al Manager Incaricato in ogni caso di dubbio o di incertezza sulla condotta corretta da adottare.

PARTE SPECIALE “P”

Reati con finalità di razzismo e xenofobia

6. LA TIPOLOGIA DEGLI ILLECITI RILEVANTI (ART. 25 TERDECIES)

La Legge Europea 2017 (la legge 20 novembre 2017, n. 167) ha imposto l'introduzione di una nuova fattispecie di Reato Presupposto, inserita all'art. 25 *terdecies* del Decreto e finalizzata a sanzionare penalmente condotte di istigazione e incitamento all'odio a sfondo razziale, etnico o religioso.

Si tratta in particolare, della seguente fattispecie di reato, schematicamente riassunta qui di seguito:

Articolo	Fattispecie	Sanzione pecuniaria	Sanzione interdittiva
Art. 3 comma 3 e comma 3 <i>bis</i> l. 654/1975 (come sostituito dall'art. 604 <i>bis</i> c.p.)	Incitamento, istigazione, propaganda alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, oltre che condotte basate sulla negazione, sulla minimizzazione in modo grave o sull'apologia.	da 200 a 800 quote	sì, per una durata non inferiore a un anno: 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, salvo che per ottenere le prestazioni di pubblico servizio; esclusione di agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi.

Se l'ente o una sua unità organizzativa è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti” in questione, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività.

Per agevolare la lettura e la consultazione del Modello, e vista la sua finalità, si riporta qui di seguito una sintetica descrizione degli illeciti per cui è prevista la responsabilità amministrativa.

La norma mira quindi a sanzionare ogni organizzazione, associazione, movimento avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, fondandosi in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

In realtà la condotta che rileva, ai fini della responsabilità amministrativa dell'Ente, e che costituisce quindi Reato Presupposto è la propaganda di idee fondate sull'odio razziale o etnico, l'istigazione alla discriminazione, la violenza per motivi razziali, etnici, nazionali o religiosi, la partecipazione o l'assistenza ad organizzazioni o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, quando le condotte (i.e. propaganda, istigazione ed incitamento), quando siano commessi in modo che ne derivi concreto pericolo di diffusione e si fondino sulla negazione, minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

7. LA VALUTAZIONE DELLE AREE DI RISCHIO

La scelta del legislatore di introdurre tra i Reati Presupposto quello, qui esaminato, che punisce condotte integranti violenza razziale, istigazione alla violenza o all'apologia di crimini di genocidio suscita non poche perplessità, soprattutto perché appare davvero difficile ipotizzare che esista un Ente in cui tali condotte possano accompagnarsi ad un concreto interesse o vantaggio, presupposto che, insieme alla condotta vietata, costituisce condizione della responsabilità amministrativa dell'Ente.

Ciononostante, trovandosi ad adottare il Modello e ad implementare tutte le conseguenti regole di condotta, Data Appeal ha deciso di dedicare una parte speciale anche ai reati c.d. di razzismo e xenofobia qui in esame, a conferma dell'impegno e del progetto che stanno alla base dell'adozione del Modello stesso.

Si ritiene tuttavia che, data l'Attività svolta da Data Appeal, che non ha nulla a che vedere con la diffusione e la creazione di opinioni, il rischio di commissione di uno dei reati qui in esame, che devono sempre accompagnarsi, perché sussista una responsabilità ai sensi del Decreto, ad un concreto interesse o vantaggio dell'Ente, sia a dir poco remoto.

8. PRINCIPI GENERALI DI COMPORTAMENTO

Data Appeal si è da sempre ispirata, in qualsiasi tipo di rapporto abbia instaurato nello svolgimento della propria attività di impresa, al rispetto della persona e dei suoi diritti fondamentali e rifugge da qualsiasi forma di discriminazione, di qualsivoglia forma e genere. Gli stessi principi sono stati sintetizzati nel Codice Etico della Società.

Data Appeal infatti opera secondo i principi del rispetto reciproco, della collaborazione, dell'inclusione e condanna qualsiasi atteggiamento di istigazione e incitamento all'odio basato su motivi razziali nonché i fenomeni di negazionismo dei crimini contro l'umanità.

In particolare, la Società si impegna ad operare e a far rispettare ai propri dipendenti e consulenti i seguenti principi di comportamento:

- astenersi da comportamenti tali da integrare le fattispecie di reato sopra descritte;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

- è fatto assoluto divieto di utilizzare i canali di comunicazione e i dispositivi della Società al fine di diffondere messaggi, condividere idee e promuovere forme di associazionismo tali da poter integrare le fattispecie di reato sopra descritte;
- utilizzare, nella diffusione di messaggi, scritti, orali o sotto qualsiasi formato, espressioni quanto più neutre possibili, senza alcun riferimento nei confronti di orientamenti o appartenenze etiche, religiose, ideologiche, al fine di creare un giudizio di valore.