“Infosyn s.r.l.”

MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (“MOG”)

predisposti ai sensi e per gli effetti di cui al D.lgs. 231/01

Versione 2.0
con il piano anticorruzione e trasparenza

* * *

Bolzano – Bozen
Bressanone – Brixen (BZ)
Merano – Meran (BZ)
Sede operativa: Via Luis Zuegg 40, CAP 39012, Merano (BZ)

REA BZ-168960;
CF e P.IVA 02298140217;
indirizzo pec: pec@pec.infosyn.it
www.infosyn.it – info@infosyn.it

Sommario della "parte generale"

1 La società e il suo oggetto sociale 5
2 Adozione del Modello ai sensi del D. lgs. 231/01 e costanti integrazioni 5
3. Metodologia 8
3.1. Analisi dei rischi: framework di riferimento e sistema di controllo interno 8
4. I reati che possono determinare la responsabilità della società 11
4.1. Reati nei confronti della Pubblica Amministrazione e contro il patrimonio a danno dello Stato o di altro Ente Pubblico: 11
4.2. Reati societari: 12
4.3. Reati in materia di sicurezza sul lavoro: 13
4.4. Reati in materia di riciclaggio del denaro, autoriciclaggio e ricettazione: 14
4.5. Reati informatici: 14
4.6. Reati transnazionali: 14
4.7. Reati in materia di violazione del diritto d'autore: 15
4.8. Reati in materia ambientale: 15
4.9. Caporalato e Impiego di cittadini di Paesi terzi, il cui soggiorno è irregolare 15
4.10. Reati di corruzione tra privati e di induzione indebita a dare o promettere utilità 17
4.11. Delitti contro l'industria e il commercio 17
5. Il sistema sanzionatorio 19
5.1. Le sanzioni disciplinari a carico dei Dipendenti 19
5.2. Le sanzioni a carico dei Dirigenti 19
5.3. Sanzioni nei confronti dei componenti del Consiglio di Amministrazione 20
5.4. Sanzioni nei confronti dei componenti del Collegio sindacale, revisori e OdV 20
5.5. Sanzioni nei confronti di terzi con cui la società instauri rapporti 20
6. Struttura dei presidi di controllo 21
7. L'Organismo di Vigilanza 22
7.1. Scopo ed ambito di applicazione 22
7.2. Nomina e composizione 22
7.3. Requisiti dell'Organismo di Vigilanza 22
7.4. Durata, revoca e recesso dei componenti 23
7.5. Funzioni e poteri 23
8. Verifiche periodiche del Modello 25
9. Formazione e Diffusione del Modello 25
9.1. Formazione del personale apicale 25
9.2. Formazione del personale sottoposto 25
9.3. Informazione a collaboratori esterni e fornitori 25
10. Il Codice Etico 26
11. Valutazione del rischio in itinere, controlli e segnalazioni all'OdV 26
12. Anticorruzione e trasparenza 27
13. Accesso civico semplice, accesso generalizzato e accesso documentale agli atti (L. 241/90) 42

ALLEGATI alla "parte generale"

1. Matrice del rischio e *risk assessment* sui processi e reati presupposto
2. Elenco dei "reati-presupposto" del D.Lgs. 231/01
3. Clausole da inserire nei contratti (per fornitori, consulenti, dipendenti, ecc.)
4. Codice Etico
5. Codice di comportamento dei dipendenti pubblici, ai sensi dell'art. 54 del d.lgs. 30/3/2001, N. 165 e DPR 16/4/2013, n. 62 e disposizioni locali
6. Regolamento dell'OdV (Organo di Vigilanza)
7. Policy e linea guida anticorruzione
8. Tabella degli adempimenti e obblighi di pubblicazione *on line* (sito web istituzionale, sezione amministrazione trasparente) ai sensi del d.33/2013 e ss.mm.ii. (in corso di aggiornamento)
9. Regolamento per l' "accesso generalizzato" sulla base delle Linee Guida FOIA – ANAC 2016 (in elaborazione).
10. Registro delle richieste di accesso civico generalizzato (rinvio a sezione "amministrazione trasparente").

Parte “speciale” – Procedure organizzative

1. Rapporti e adempimenti con la P.A. e relativi adempimenti (autorizzazioni e finanziamenti)
2. Acquisti di consulenze e beni/servizi “non core”
3. Gestione visite ispettive
4. Tenuta contabilità e bilancio/chiusure
5. Rapporti commerciali con controparti del settore pubblico e privato
6. Utilizzo del sistema informatico
7. Regolamento acquisti
8. Regolamento assunzione dipendenti

1 La società e il suo oggetto sociale

InfoSyn s.r.l., con sede legale in Bressanone (BZ) via A. Ammon 24 e sede operativa in Merano (BZ), via Zuegg 40,[1] è stata costituita a fine anno 2001, con oggetto l'acquisto, la vendita, il noleggio, la progettazione, la consulenza, la ricerca, lo sviluppo e l'implementazione, la formazione e l'aggiornamento ed in generale lo svolgimento ed il coordinamento di ogni tipo di servizio nell'elaborazione elettronica dei dati, per imprese private ed enti locali in ordine alla gestione delle attività afferenti ai seguenti settori: energia; ambiente; acqua potabile ed acque reflue; telecomunicazioni; teleriscaldamento e teleraffreddamento; trasporto; strutture del traffico; illuminazione pubblica; impianti sportivi; servizi cimiteriali e farmaceutici.

La società potrà svolgere tutte le altre attività commerciali, industriali, finanziarie, mobiliari ed immobiliari che saranno ritenute dall'organo amministrativo strumentali, accessorie, connesse, necessarie od utili per la realizzazione delle attività che costituiscono l'oggetto sociale, assumere interessenze e partecipazioni in altre società od imprese aventi per oggetto attività analoghe, affini o connesse alle proprie, sia direttamente che indirettamente, sia in Italia che all'estero , nonchè rilasciare garanzie e fidejussioni a favore di terzi, il tutto purchè non nei confronti del pubblico e purchè tali attività non vengano svolte in misura prevalente rispetto a quelle che costituiscono l'oggetto sociale. viene espressamente esclusa ogni attività che rientri nelle prerogative che necessitano l'iscrizione ad albi professionali ed ogni attività finanziaria vietata dalla legge tempo per tempo vigente in materia ed in particolare ai sensi di quanto disposto dall'articolo 113 del d.l. 1 settembre 1993 n.385.la società si inibisce la raccolta del risparmio tra il pubblico e le attività previste dal d.l. 415/96.

Il codice Ateco che indica l'attività svolta è il 58.2.

I soci sono:

1. AZIENDA SERVIZI MUNICIPALIZZATI DI MERANO S.P.A. (48,5%),
2. ASM BRESSANONE S.P.A. (48,5%);
3. UNIONE DELL'ENERGIA ALTO ADIGE SOCIETA' COOPERATIVA (2%);
4. SEAB SERVIZI ENERGIA AMBIENTE BOLZANO S.P.A., IN BREVE "SEAB SPA/AG" (1%).

La società è amministrata da un CdA e da un Direttore, sotto la cui supervisione operano sedici dipendenti e altri collaboratori. Per ulteriori dettagli relativi all'organizzazione, organigramma e riferimenti di contatto si fa rimando al Modello Organizzativo e Gestionale di cui al d.lgs. 231/01, del quale questo Piano triennale anticorruzione costituisce presidio e parte integrante e sostanziale.

Tutto ciò premesso, nel presente documento si illustrano i "Modelli di organizzazione, gestione e controllo" (di seguito i "Modelli") adottati dalla società ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito il "Decreto") e delle sue modificazioni e integrazioni.

Con i presenti Modelli la società ha inteso attuare i principi di corretta gestione affermati dal Decreto citato.

2 Adozione del Modello ai sensi del D. lgs. 231/01 e costanti integrazioni

Il D.Lgs. 231/01 introduce nell'ordinamento italiano la responsabilità "amministrativa" degli enti relativamente alla commissione di alcuni reati, specificamente indicati dal legislatore; permette, quindi, di colpire direttamente l'Ente,

[1] REA BZ-168960; CF e P.IVA 02298140217; indirizzo pec: pec@pec.infosyn.it

con sanzioni pecuniarie, l'interdizione dall'attività, il commissariamento, il divieto a contrarre con la PA. Quest'ultimo, tuttavia, non risponde se dimostra di avere "adottato ed efficacemente attuato" un modello organizzativo idoneo a prevenire la commissione di reati della stessa fattispecie di quello verificatosi.

Con il D. Lgs. 231/01 il legislatore ha adeguato la normativa interna alle convenzioni internazionali OCSE OECD in materia di responsabilità delle persone giuridiche, alle quali l'Italia aveva già aderito da tempo. La normativa in oggetto ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa dell'Ente per reati che sono tassativamente indicati in un elenco (allegato), e commessi a suo vantaggio o semplicemente nel suo interesse (a prescindere da un'effettiva utilità apportata). I soggetti che possono commettere tali reati comportando la responsabilità amministrativa dell'Ente sono:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale;
- persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi;
- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati, se la commissione del reato sia stata resa possibile dall'omissione della vigilanza.

La responsabilità dell'Ente si aggiunge a quella penale della persona fisica che ha commesso il reato.

Ciò premesso, si specifica che il consorzio-azienda ASIA ha adottato nel 2014 i modelli di organizzazione e di gestione ("MOG") della propria attività in base alle norme di cui al Decreto Legislativo n. 231 del 2001, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e determinazioni ANAC.

L'aggiornamento dei MOG, del codice etico, del risk assessment e, in generale, delle procedure e protocolli, avviene regolarmente, ai cambi organizzativi e normativi/giurisprudenziali e in base alle determinazioni ANAC. Si riportano di seguito le ultime modifiche salienti:

Tabella degli aggiornamenti:

Prima adozione	20/11/2015	Risk assessment; MOG, codice etico, procedure.
Revisione integrale	31/01/2017	Revisione MOG; fusione MOG con PTPC; sdoppiamento procedure acquisti/vendite; adozione procedura formazione.
	…/…/……	

Occorre anche tener conto che Infosyn ha anche adottato -negli anni scorsi, a partire dal 2014- un "Piano Triennale per la Prevenzione della Corruzione" (PTPC), ai sensi della L. 190/2012 e determinazioni ANAC (già allegato al precedente MOG, quale presidio e parte integrante e sostanziale del sistema organizzativo dell'Azienda); ciò al fine di rendere maggiormente esimente il sistema dei modelli organizzativi e gestionali predisposti secondo il d.lgs. 231/01. L'azienda ha anche nominato un "responsabile della prevenzione della corruzione" (RPC) e anche un "responsabile della trasparenza e integrità" (RT), ai sensi del d.lgs. 33/2013 e norme locali (l.r. 10/2014), che costituiscono ulteriori presidi antirischio, confluiti a partire da dicembre 2016 nella funzione unica "RPCT" (Responsabile della prevenzione della corruzione e responsabile trasparenza).

Per la costruzione del modello organizzativo e gestionale (MOG), metodologicamente Infosyn si era ispirata inizialmente alle linee guida di Confindustria 2014, a prassi in materia e ad indicazioni della magistratura locale e

nazionale, quali il decalogo del GIP di Milano (Dr. Secchi), ordinanze dei Tribunale e Procure di Trento e Bolzano, nonché alle recenti sentenze della S. C. di Cassazione. Nell'ultima revisione del modello si è tenuto conto di quanto disposto dal d.lgs. 97/2016 e dalle Linee Guida ANAC 2016 in materia di trasparenza, integrità e anticorruzione e accesso civico, nonché dalle norme locali quali la legge regionale TNAA n. 10/2014 e la legge regionale n. 16/2016.

Si è provveduto quindi a far confluire nei MOG 231/01 disposizioni, procedure, obiettivi e strumenti del PTPC, in modo sistemico e tenendo conto delle procedure 231/01 già esistenti (peraltro già tutte impostate in modo da prevenire la corruzione, la concussione e altri reati contro la PA e altre condotte di impresa irresponsabile che configurano, sostanzialmente, una *mala gestio* o *maladministration*.

L'**obiettivo strategico** principale di Infosyn, accessorio all'oggetto sociale e connesso alle tematiche **anticorruttive e di trasparenza-integrità**, ai sensi della l. 190/2012, è proprio quello di evitare corruzione, concussione, altri reati contro la PA, *maladministration* e, in generale, condotte di per sé lecite, ma parte di un più vasto disegno illecito.

Anche in quest'ultima revisione dei MOG, un'analisi completa dei processi e di confronto con i preposti alle varie attività gestionali ha consentito di comprendere al meglio la specificità dell'attività aziendale e, in tal modo, di individuare le ipotesi di reato che possono essere commesse sia da soggetti apicali sia da loro sottoposti. L'individuazione è avvenuta proponendo dapprima una analisi dei processi, con un questionario somministrato alle figure apicali e di loro supporto, volto a evidenziare l'organizzazione aziendale e eventuali passaggi operativi che difettassero dei controlli necessari per escludere la commissione di reati. A seguito dell'esame delle risposte è stata realizzata una tabella, nella quale si è proceduto ad incrociare i processi dell'Ente con i possibili reati commettibili, graduandone la probabilità, l'impatto e, di conseguenza, il rischio residuo. In essa sono state inserite le procedure di riferimento (ossia i singoli "modelli organizzativi"), ossia istruzioni in grado di arginare la commissione di determinati reati. Le risposte alle domande del questionario sono state corroborate da interviste e focus group, poiché metodologicamente ai dati quantitativi occorre sempre affiancare una analisi qualitativa, anch'essa peraltro analizzata con variabili proxy, analisi semantiche, MaxQda. Ciò ha consentito di predisporre le varie procedure regolatrici dei principali processi operativi aziendali e di realizzare una mappatura procedurale precisa e puntuale delle fattispecie di reato astrattamente commettibili colposamente o dolosamente in azienda; in aggiunta sono stati mappati quei comportamenti apparentemente leciti, ma che strumentalmente costituiscono la base di altri più vasti illeciti.

L'efficacia del Modello viene garantita dalla verifica periodica dello stesso e dalle modifiche in caso di significative violazioni delle prescrizioni o in caso di mutamenti organizzativi o di ampliamento/riduzione dei reati riconducibili al Decreto in esame, nonché dalla predisposizione di un sistema sanzionatorio da applicarsi in caso di mancato rispetto delle disposizioni organizzative-procedurali.

A sovraintendere il rispetto delle procedure viene predisposto l'Organismo di Vigilanza ("OdV"), che si dota di un apposito regolamento.

3. Metodologia

Il fatto che un esiguo numero di Modelli Organizzativi abbia passato il vaglio della Magistratura ha spinto ASIA, dopo l'applicazione delle Linee Guida di Confindustria, anche verso una loro successiva integrazione, mediante le fonti di seguito riportate. Il presente documento, pertanto, è stato personalizzato il più possibile, ritagliandolo in relazione all'effettiva attività esercitata dall'azienda e, soprattutto, scritto in base alla complessità dei processi aziendali e attività effettivamente esercitate.

L'esigenza di non irrigidire a dismisura l'attività di gestione, nel caso di processi semplici e a basso rischio reato, è stata contemperata con la predisposizione di una adeguata organizzazione e suddivisione delle funzioni. Peraltro la filosofia di INFOSYN si è sempre basata sulla buona organizzazione aziendale; il presente Modello Organizzativo (MOG), quindi, deriva anche dal processo di aggiornamento e di integrazione di attività di *risk assessment* già in essere in azienda, ora meglio integrate con:

- Le determinazioni e altri provvedimenti dell'ANAC, Autorità Nazionale Anti corruzione, quali il PNA 2013 e PNA 2016 e la metodologia di *risk assessment* ivi suggerita;
- Le norme locali della Regione autonoma Trentino Alto Adige in materia di trasparenza, accesso civico, codice dei dipendenti pubblici;
- la documentazione emanata dal GIP di Milano ("decalogo" per ottenere un corretto modello organizzativo ex D.Lgs. 231/01);
- lo Standard ISO 37001:2016 (anti bribery - anticorruzione);
- la giurisprudenza in materia di D.Lgs. 231/01 (sentenze della Corte di Cassazione);
- gli standard UNI ISO 31000 e 31010 (*risk management*);
- lo standard ISO 19600 (compliance);
- la dottrina in materia di D.Lgs. 231/01;
- i modelli organizzativi e le procedure di gruppi e aziende simili o comparabili;
- momenti di formazione specifici sul D.Lgs. 231/01 presso gli Ordini professionali, Tribunali e CSM;
- colloqui con magistrati, CTU, CTP, legali e docenti universitari esperti della materia;
- la realtà aziendale, riconosciuta e codificata attraverso la "mappatura dei rischi" e diversi colloqui con il CdA, altri/e responsabili, i/le dipendenti.

3.1. Analisi dei rischi: framework di riferimento e sistema di controllo interno

L'analisi dei processi aziendali ha consentito di individuare le attività nelle quali può essere presente il rischio di commissione di reati presupposto della responsabilità degli enti ai sensi del d.lgs. n. 231 del 2001 (di seguito, le "Attività Sensibili"). Valutando la graduazione della probabilità e l'impatto di possibili modalità commissive di illeciti riconducibili alle fattispecie di reato-presupposto rilevanti per INFOSYN , è stato calcolato il rischio residuo e, di conseguenza, sono state assunte misure e presidi a difesa dell'azienda, volte a diminuire nel tempo la probabilità di accadimento di un fenomeno illecito e/o il suo impatto.

Si è tenuto conto delle specificità delle attività svolte negli uffici e attività fuori sede, mediante l'uso di software e variabili derivanti dal framework ANAC e dalla prassi 231/01, ossia:

il budget a disposizione e/o il valore delle pratiche gestite; la provenienza dei fondi e i destinatari; il livello di discrezionalità dell'attività / processo; la complessità dell'attività in termini di coinvolgimento di altre società, enti o amministrazioni pubbliche esterne (esclusi i controlli); la determinazione dell'impatto economico dell'attività; la frazionabilità dell'attività / processo; la correttezza dei tempi di esecuzione del lavoro; la segregazione delle funzioni; i precedenti giudiziali, i provvedimenti disciplinari e la rimozione dei responsabili di condotte irresponsabili. La presenza di referenti dell'OdV; l'attività di formazione; l'esistenza e l'uso di codici etici e/o di procedure; piani di retribuzione variabile-MBO con indicatori anti-corruzione; utilizzo di *tool* software per mappare i rischi; *whistleblowing* (meccanismo di denuncia di irregolarità con tutela dell'anonimato); rating etico dei fornitori; controlli, a tre livelli, e loro efficacia; impatto organizzativo, economico e sull'immagine.

Gli standard di riferimento utilizzati sono stati la UNI ISO 31000 (*risk management*), la ISO 31010 (metodologie), la matrice del rischio ANAC–PNA, utili per valutare la probabilità di un reato (o di un evento strumentale al suo compimento) e l'impatto che tale evento avrebbe sull'azienda, in modo da determinare il c.d. "rischio residuo" di commissione di illeciti. La matrice ANAC è stata integrata mediante software con le disposizioni del GIP di Milano e le recenti indicazioni tratte dalle sentenze giurisprudenziali pronunciate in materia di esimenza dei modelli organizzativi. Per ciascuna Attività Sensibile sono state quindi identificate, oltre al referente del singolo processo aziendale ("Key Officer")[2], le modalità operative e gestionali in atto, la segregazione delle funzioni e gli elementi di presidio e controllo in essere. È stata poi effettuata un'analisi comparativa tra il sistema di controllo interno esistente e i principi e i contenuti del Modello organizzativo 231/01 (in particolare i presidi di controllo).

Secondo il documento emanato dal Committee of Sponsoring Organizations (CoSO) sotto il titolo di Internal Control-Integrated Framework (CoSoIC-IF)[3], il sistema di controllo interno può essere definito come un insieme di meccanismi, procedure e strumenti predisposti dalla direzione per assicurare il conseguimento degli obiettivi di efficienza delle operazioni aziendali, affidabilità delle informazioni finanziarie, rispetto delle leggi e dei regolamenti e salvaguardia dei beni aziendali. Le componenti del sistema di controllo interno, sulla base del CoSO Report, Internal Control – Integrated Framework, sono:

Ambiente di controllo:

Riflette gli atteggiamenti e le azioni del "Top Management" con riferimento al controllo interno nell'ambito dell'organizzazione. L'ambiente di controllo include i seguenti elementi:

- integrità e valori etici;
- filosofia e stile gestionale del Management;
- struttura organizzativa;
- attribuzione di autorità e responsabilità;
- politiche e pratiche del personale;
- competenze del personale.

[2] Con il termine "Key officer" si intende il soggetto che, in funzione delle responsabilità ad esso assegnate, è parte del processo riconducibile ad una Attività Sensibile e, in tale qualità, dispone delle migliori informazioni utili ai fini della valutazione del sistema di controllo interno ad esso inerente, con particolare riferimento a: (i)modalità operative di gestione del processo e (ii) norme interne e agli strumenti normativi ed organizzativi che lo governano.

[3] Committee of Sponsoring Organizations of the Treadway Commission (1992), internal control integrated framework, AICPA, www.coso.org, aggiornato nel maggio 2013.

Valutazione dei rischi (Risk Assessment):

Definizione di processi di identificazione e gestione dei rischi più rilevanti che potrebbero compromettere il raggiungimento degli obiettivi aziendali.

Informazione e comunicazione:

Definizione di un sistema informativo (sistema informatico, flusso di reporting, sistema di indicatori per processo/attività) che permetta sia ai vertici della INFOSYN che al personale operativo di effettuare i compiti a loro assegnati.

Attività di controllo:

Definizione di normative aziendali che assicurino una gestione strutturata dei rischi e dei processi aziendali e che consentano il raggiungimento degli obiettivi prefissati.

Monitoraggio:

È il processo che verifica nel tempo la qualità e i risultati dei controlli interni. Le componenti succitate del sistema di controllo interno sono prese a riferimento per l'analisi del rischio di commissione dei reati previsti dal d.lgs. n. 231 del 2001. In particolare l'attività di analisi è focalizzata a (i) individuare le Attività Sensibili in essere nell'azienda nel cui ambito può potenzialmente presentarsi il rischio di commissione dei reati previsti dal d.lgs. n. 231 del 2001 e le cui potenziali modalità di commissione siano state preliminarmente identificate, (ii) rilevare gli standard di controllo idonei a prevenirne la commissione.

Obiettivo dell'attività è assicurare il mantenimento e l'aggiornamento del sistema di identificazione, mappatura e classificazione delle aree di attività aziendali a rischio rilevanti anche ai fini delle attività di vigilanza.

4. I reati che possono determinare la responsabilità della società

Di seguito vengono indicati **per estratto** i reati principali che possono essere commessi dalle posizioni apicali o da quelle sottoposte, nell'interesse o a favore o vantaggio della società, rilevanti ai sensi del D.lgs. 231/01. L'individuazione degli stessi è stata calibrata in base alla valutazione dell'effettivo coinvolgimento dell'attività di INFOSYN in ipotesi che possono creare il presupposto per la commissione dei reati individuati. I reati di seguito indicati sono riferibili alle funzioni aziendali meglio identificate nella "matrice dei processi e reati". Per la trattazione completa dell'analisi di ogni processo aziendale e dei reati astrattamente ivi configurabili e graduazione della probabilità impatto e "rischio residuo" si veda l'allegato 1 (*risk assessment)*.

4.1. Reati nei confronti della Pubblica Amministrazione e contro il patrimonio a danno dello Stato o di altro Ente Pubblico:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-01; P231-02; P231-03; P231-04; P231-05; Codice etico; Codice dei dipendenti pubblici; policy anticorruzione (ex PTPC); regolamento acquisti e appalti; regolamento accesso civico; regolamento assunzione dipendenti.

Malversazione a danno dello Stato o di altro Ente Pubblico (art. 316 bis c.p.): la finalità è quella di reprimere, dopo il conseguimento di prestazioni pubbliche, le frodi allo scopo tipico individuato dal precetto che autorizza l'erogazione: tale scopo risulterebbe vanificato ove il vincolo di destinazione venisse eluso.

Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro Ente Pubblico (art. 316 ter c.p.): è norma sussidiaria rispetto a quella della truffa di cui all'art. 640bis c.p. Il reato si configura con riguardo all'ipotesi di utilizzo di dichiarazioni o documenti falsi o attestanti cose non vere a condizione che tale condotta non sia accompagnata da ulteriori malizie dirette all'induzione in errore del soggetto passivo.

Concussione (art. 317 c.p.): il delitto di concussione è collegato all'obiettiva qualifica di pubblico ufficiale dell'autore del reato o di incaricato di pubblico servizio (Art. 358 Nozione della persona incaricata di un pubblico servizio. Agli effetti della legge penale, sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. (Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale). Il reato si concretizza nell'abuso della propria qualità di incaricato di pubblico servizio, per costringere o indurre qualcuno a dare o promettere indebitamente, anche a terzi, denaro o altra utilità.

Istigazione alla corruzione (art. 322 c.p.): il reato è configurabile quando l'attuazione della promessa di denaro od altre utilità non sia immediata né configurabile come possibile dal soggetto passivo a cui è rivolta. Il reato si concretizza con l'offerta o la promessa di denaro o altra utilità non dovuti a un pubblico ufficiale o incaricato di pubblico servizio per indurre a compiere o omettere o ritardare un atto del suo ufficio o un atto contrario ai suoi doveri.

Truffa a danno dello Stato o di altro ente pubblico (art. 640, I° comma, n° 1 c.p.): ai fini della sussistenza della truffa il raggiro non deve necessariamente consistere in una particolare subdola messa in scena, bastando una qualsiasi simulazione o dissimulazione posta in essere per indurre in errore.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.): l'elemento specializzato rispetto al reato di truffa è costituito dall'oggetto materiale della frode cioè da ogni attribuzione economica agevolata erogata da parte dello Stato, enti pubblici o comunità europee.

Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.): l'elemento differenziatore dagli altri reati è che l'attività fraudolenta dell'agente investe non la persona bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema.

4.2. Reati societari:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-03; P231-04; P231-07; Codice etico.

False comunicazioni sociali (art. 2621 c.c.) e ***false comunicazioni sociali in danno dei soci e o dei creditori*** (art. 2622 c.c.): in primo luogo il legislatore ha previsto che la falsità sia commessa attraverso una delle comunicazione sociali previste dalla legge (bilanci, relazioni ecc.), non essendo sufficiente una qualsiasi comunicazione (es. orale). La falsità consiste nell'esposizione di "fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni", oppure nell'omissione di "informazioni, la cui comunicazione è imposta dalla legge". Al riguardo si precisa che la falsità penalmente rilevante non coincide necessariamente con l'invalidità in senso civilistico di una delle comunicazioni sociali sopra dette. Affinchè la falsificazione assuma una rilevanza penale, infatti, è necessario che essa abbia una idoneità offensiva per il patrimonio di INFOSYN . Il reato si può concretizzare in tutte le comunicazioni rivolte la pubblico e che siano viziate.

Impedito controllo [4] (art. 2625 c.c.): il delitto di cui al secondo comma dell'art. 2625 cc è da considerare un reato che tutela il patrimonio di INFOSYN a differenza dell'illecito amministrativo di cui al primo comma, in cui non è prevista la causazione del danno e oggetto di tutela e le attività di controllo in sé.

Formazione fittizia del capitale (art. 2632 c.c.); Trattasi di reato d'evento, ove l'evento è descritto come il formare od aumentare fittiziamente il capitale sociale ossia della consistenza economica dell'Ente.

Quanto alla condotta (collegata all'evento di cui sopra), essa può consistere in generale: nell'attribuire azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale; nella sottoscrizione reciproca di azioni o quote; nella sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti. In riferimento alla nostra realtà aziendale tale tipo di reato può concretizzarsi in via esemplificativa nella sopravvalutazione rilevante del patrimonio sociale al fine di attribuire requisiti eventualmente richiesti da bandi di gara o per l'assegnazione di sovvenzioni o conclusione di convenzioni.

[4] Si specifica che il d.lgs. 15/2016 - depenalizzazione di alcune fattispecie di reato, ha classificato indirettamente l'ostacolo alle funzioni di controllo come condotta non più presupposto della responsabilità amministrativa degli enti ai sensi del d.lgs.231/01. In dettaglio, il decreto legislativo 15 gennaio 2016 n. 8, in vigore dal 6 febbraio 2016, non tocca l'impedito controllo ex art 2625 c.c., ma depenalizza la fattispecie contravvenzionale prevista dal comma 1 dell'art 29 d.lgs. 39/2010. Peraltro tale fattispecie di impedito controllo del revisore non solo diventa illecito amministrativo ma inoltre l'importo della sanzione risulta ora meno gravoso, potendo giungere alla sanzione pecuniaria di 50.000 euro, a fronte dei previgenti 75.000 di ammenda (o 150.000 euro nell'ipotesi aggravata di cui al comma 3). Va pure rilevato che nell'ipotesi di impedito controllo "interno" (ex art 2625 comma 1 c.c.), la sanzione amministrativa può arrivare ad un massimo di 10mila euro circa. Resta invece fuori dalla depenalizzazione la fattispecie aggravata, prevista nel comma 2, punita con pena detentiva congiunta a quella pecuniaria.

È opportuno ribadire che tali condotte non costituiscono reato in se stesse, ma assurgono a fattispecie penalmente rilevanti solamente se provocano, con collegamento causale, eziologicamente pregnante, un aumento fittizio del capitale sociale.

Illecita influenza sull'assemblea (art. 2636 c.c.); La condotta richiesta dall'art. 2636 c.c., al fine di configurare il delitto in oggetto, consiste nel porre in essere atti simulati o fraudolenti. Il porre in essere la condotta evidenziata, tuttavia non basta per configurare il delitto in esame: il reato in oggetto è, infatti, reato d'evento; ciò significa che la condotta posta in essere (che è, all'evidenza, condotta vincolata), per configurare reato deve necessariamente esser collegata eziologicamente all'evento descritto dalla norma, ossia deve determinare la maggioranza in assemblea.

Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.): Trattasi, all'evidenza, di un classico reato d'evento ove è necessario, affinché la fattispecie possa dirsi configurata, che la condotta posta in essere dall'agente determini, con collegamento eziologico, l'effetto che la norma intende impedire (nel caso di specie: ostacolare le funzioni delle autorità pubbliche di vigilanza).

Il reato è "a forma libera": l'evento richiesto può, infatti, esser cagionato "in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità".

La norma, inoltre, non prevede la perseguibilità a querela del delitto in oggetto, sicché quest'ultimo **è procedibile d'ufficio**.

Corruzione tra privati (art. 2635 c.c. III° comma)***:*** è il reato compiuto da amministratori, direttori generali, dirigenti preposti alla redazione di documenti contabili societari, sindaci e liquidatori che omettono di compiere atti di loro dovere a seguito del ricevimento di un'utilità. La responsabilità amministrativa è limitata all'ente cui sia riconducibile il soggetto apicale o dipendente che ha posto in essere la condotta di corruzione e non riguarda invece la società/ente cui appartiene il soggetto corrotto. Tale costruzione della fattispecie è coerente con i criteri di imputazione della responsabilità ex. D.Lgs. 231/2001 secondo cui l'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio. La corruzione tra privati, al contrario, prevede per definizione normativa che la società/ente in cui opera il soggetto corrotto subisca un "nocumento" derivante dagli atti compiuti od omessi in violazione degli obblighi inerenti il proprio ufficio o di fedeltà.

Per tale tipo di reato ci si riferisce alle procedure che trattano di corruzione e concussione, in quanto già le procedure per i reati societari sono finalizzate ad evitare il verificarsi di tale reato presupposto. Inoltre i vertici di INFOSYN hanno deciso di adottare, oltre al codice dei dipendenti pubblici suggerito dalla Provincia Autonoma e DPR 62/2013, un proprio codice etico, di uguale forza cogente in cui sono definiti i valori ed i principi di condotta rilevanti ai fini del buon funzionamento, dell'affidabilità, del rispetto delle leggi e regolamenti nonché della reputazione e immagine della medesima. Esso contiene l'insieme dei diritti, dei doveri e delle responsabilità della società nei confronti delle parti interessate interne ed esterne (dipendenti, fornitori, ospiti e familiari, Pubblica Amministrazione, collettività).

4.3. Reati in materia di sicurezza sul lavoro:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: DVR; Codice etico; Clausole 231/01 nei contratti a rischio HSE.

Omicidio colposo (art. 589 c.p.): la colpa può identificarsi con l'imprudenza e negligenza. Ai fini della sussistenza del rapporto di causalità è sufficiente che l'agente abbia posto in essere una condizione qualsiasi dell'evento lesivo.

Lesioni colpose gravi e gravissime (art. 590, III^ comma, c.p.): affinché non possa essere esclusa la colpa nella condotta dell'agente, l'evento ancorché non previsto, né prevedibile, non può essere ascritto al caso fortuito in quanto ricollegabile pur sempre ad un comportamento colposo. L'elemento psicologico rilevante non è condizionato dall'opinione soggettivo dell'individuo cui l'evento dannoso è contestato né ha rilevanza la prevedibilità dell'evento. Elemento costitutivo è solo la condotta dell'agente contraria alla normale prudenza, alle leggi o regolamenti o consistente nella negligenza e imperizia.

4.4. Reati in materia di riciclaggio del denaro, autoriciclaggio e ricettazione:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-04; P231-05; P231-07; Codice etico.

Ricettazione (art. 648 c.pc.): è un illecito contro il patrimonio e ne deriva che la sua oggettività giuridica si sostanzia nell'interesse di garantire il diritto del privato. Si concretizza nell'acquistare, ricevere od occultare (o intromettersi in tali operazioni) denaro o cose provenienti da un qualsiasi delitto.

Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.): presupposto è la provenienza da delitto dei denaro o beni o altra utilità. La finalità perseguita deve essere quella di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità che detta finalità è perseguita mediante l'impiego delle risorse in attività economiche e finanziarie.

Autoriciclaggio: (art.3 L. 186/2014).

4.5. Reati informatici:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-06; Codice etico.

Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.): il sistema informatico va inteso come un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione anche parziale di tecnologie informatiche che sono caratterizzate per mezzo di un'attività di codificazione e decodificazione dalla registrazione o memorizzazione per mezzo di impulsi elettronici, su supporti adeguati, di dati e dalla elaborazione automatica di tali dati in modo da generare informazioni. Il reato si concretizza nell'accesso abusivo o nel permanere nel sistema contro la volontà di chi ha diritto di escludere.

Detenzione e diffusione abusiva di codici di accesso a sistemi telematici e informatici (art. 615 quater c.p.): il reato si concretizza quando il soggetto abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri sistemi idonei all'accesso ad un sistema informatico o telematico.

4.6. Reati transnazionali:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-05; Codice etico.

La legge 16 marzo 2006 n. 146, con la quale è stata ratificata e data esecuzione alla Convenzione ed ai Protocolli aggiuntivi delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 Novembre 2000 ed il 31 maggio 2001, ha ulteriormente ampliato il catalogo di reati rilevanti ai fini della responsabilità amministrativa degli enti ex. D.lgs. 231/2001.

La Convenzione è nata dalla necessità di elaborare uno strumento internazionale idoneo a contrastare la criminalità

organizzata che, negli ultimi decenni, con la progressiva apertura delle frontiere e delle economie nazionali, ha preso sempre più ad operare a livello transnazionale.

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.): Tale ipotesi di reato è prevista nel caso di uso di violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, per indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

Favoreggiamento personale (art. 378 c.p.): La norma prevede la punizione per chiunque, dopo che fu commesso un delitto per il quale la legge stabilisce la pena dell'ergastolo o la reclusione, e fuori dei casi di concorso nel medesimo, aiuta taluno a eludere le investigazioni dell'Autorità, o a sottrarsi alle ricerche di questa.

4.7. Reati in materia di violazione del diritto d'autore:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: Codice etico; Codice dei dipendenti pubblici; regolamento acquisti e appalti.

Duplicazione di programmi (171 bis l. n. 633 del 1941): La Suprema Corte ribadisce che, a seguito alle modifiche introdotte alla L. 633/1941 dalla L. 248/2000, non è più richiesto – dall'art. 171 bis – che vi sia un "fine di lucro", essendo sufficiente la presenza di un "fine di profitto".

4.8. Reati in materia ambientale:

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: Codice etico.

Bonifica dei siti (art. 257, comma 1, D. Lgs 152/06).

Superamento valori limite e di qualità dell'aria (art. 279, comma 5, D. Lgs.152/06)

Caratteristiche di pericolo dei rifiuti (Regolamento europeo 1357/2014 e Legge 68/2015)

In generale i reati considerati dal Decreto Legislativo 231/2001 sono dolosi, ossia posti in essere volontariamente dal soggetto con quello scopo specifico e il Modello Organizzativo ha una funzione esimente della responsabilità dell'Ente se le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il suddetto modello. I reati considerati in questa Parte Speciale (ambiente) sono invece di **natura colposa,** ossia conseguenza di negligenza, imprudenza o imperizia da parte del soggetto; pertanto la funzione di esimente del Modello Organizzativo è rappresentata dall'introduzione di previsioni volte a far si che i destinatari pongano in essere una condotta (non accompagnata dalla volontà di determinare un danno all'ambiente) rispettosa delle procedure ambientali, congiuntamente agli adempimenti e agli obblighi di vigilanza previsti dal Modello Organizzativo.

4.9. Caporalato e Impiego di cittadini di Paesi terzi, il cui soggiorno è irregolare

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-07; P231-08; Codice etico.

Con la legge n. 199/2016 è stato aggiunto all'art. 25quinquies del d.lgs. 231/01 (Delitti contro la personalità individuale) il "reato presupposto" dell'art. 603-bis del codice penale, relativo all'intermediazione illecita e sfruttamento del lavoro (c.d. "caporalato"). In breve, salvo che il fatto costituisca più grave reato e oltre alle sanzioni in "quote", tipiche del d.lgs.231/01, è punito con la reclusione da uno a sei anni e con la multa da 500 a 1.000 euro per ciascun lavoratore reclutato, chiunque:

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

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

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

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

- 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;
- la reiterata violazione della normativa relativa all´orario di lavoro, ai periodi di riposo, al riposo settimanale, all´aspettativa obbligatoria, alle ferie;
- la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
- la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

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

- il fatto che il numero di lavoratori reclutati sia superiore a tre;
- il fatto che uno o più dei soggetti reclutati siano minori in età non lavorativa;
- l´aver commesso il fatto esponendo i lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

Nel presente modello sono stati quindi posti i presidi volti ad evitare che il datore di lavoro si approfitti dello stato di bisogno di lavoratori/trici, sottopagandoli/e dopo averli/e sottoposti/e a condizioni di lavoro particolarmente faticose. Il primo indice dello sfruttamento è dato dal corrispondere una retribuzione palesemente difforme da quella prevista dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale o comunque sproporzionata rispetto alla qualità e alla quantità del lavoro prestato. Si è ritenuto che una sproporzione retributiva in termini percentuali ammonti almeno del 30%. Altri indici di inadeguata qualità del luogo di lavoro sono costituiti dal mancato rispetto di orario di lavoro, congedi o ferie e precarie/insalubri condizioni di salute e sicurezza nei luoghi di lavoro.

Inoltre, a partire dall'agosto 2012 è stato integrato l'art. 25 del D.lgs 231/01, con la pubblicazione in data 25 luglio 2012 in G.U. del D.lgs **109**/2012 del 16 luglio 2012, il quale, in attuazione della direttiva 2009/52/CE volta a rafforzare la cooperazione tra Stati membri nella lotta contro l'immigrazione illegale, **introduce norme relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare**. Il provvedimento legislativo prevede ipotesi aggravanti in caso di impiego lavorativo di cittadini stranieri, il cui soggiorno sia irregolare. Pur presentandosi un basso rischio per la società, sempre attenta a rispettare le norme in materia giuslavoristica, un aspetto in astratto da non sottovalutare riguarda le disposizioni sanzionatorie richiamate all'art. 2 del D.lgs 109/2012, che prevede che al decreto legislativo 8 giugno 2001, n. 231, dopo l'articolo "25-undecies" e' inserito il seguente: "25-duodecies. (Impiego di cittadini di paesi terzi il cui soggiorno è irregolare).

1. In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del decreto legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro.".

Le attività e processi aziendali da monitorare con attenzione sono:

- selezione del personale;
- definizione delle politiche retributive (compresa l'attribuzione di benefit);
- individuazione e gestione di corsi di formazione.

4.10. Reati di corruzione tra privati e di induzione indebita a dare o promettere utilità

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: P231-01; P231-02; P231-03; P231-04; P231-05; P231-07; P231-08; Codice etico; Codice dei dipendenti pubblici; policy anticorruzione (ex PTPC); regolamento acquisti e appalti.

La punibilità per il **reato di corruzione tra privati** (art. 2635 c.c.) è riconosciuta solo per l'ente/società "corruttrice" ossia l'ente/società ove operi il soggetto apicale o sottoposto a direzione e vigilanza dello stesso che abbia dato o promesso denaro o altra utilità ad un amministratore, direttore generale, dirigente preposto, liquidatore o persona sottoposta a direzione e vigilanza di uno degli stessi di una società terza al fine di ottenere un vantaggio per la conduzione del proprio business. Nel caso di specie si può ipotizzare che possa verificarsi la condotta contestata anche al solo fine di rendere la società più competitiva rispetto ai *comparables* del settore.

L'**induzione indebita a dare o promettere utilità** consegue alla rivisitazione del reato di concussione (art. 317 c.p.) per induzione. Risponde per tale reato l'ente/società privata cui appartiene il soggetto apicale o sottoposto che, assecondando il comportamento induttivo del funzionario pubblico, perfeziona la dazione dell'indebito.

4.11. Delitti contro l'industria e il commercio

Procedure, allegate, per la prevenzione dei reati presupposto di questo paragrafo: Codice etico; Codice dei dipendenti pubblici; regolamento acquisti e appalti.

La punibilità per la condotta di **turbata libertà dell'industria o del commercio (art. 513 c.p.)** riguarda chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l´esercizio di un´industria o di un commercio, punibile a querela della persona offesa.

La punibilità per la condotta di **illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.)** riguarda chi, nell´esercizio di un´attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia. La pena è aumentata se gli atti di concorrenza riguardano un´attività finanziata in tutto o in parte dallo Stato o da altri enti pubblici.

La punibilità per la condotta di **frode nell'esercizio del commercio (art. 515 c.p.)** riguarda chi, nell´esercizio di un´attività commerciale, consegna all´acquirente una cosa mobile per un´altra, ovvero una cosa mobile che, per origine, provenienza, qualità o quantità, è diversa da quella dichiarata o pattuita.

Si tratta di **reati di pericolo**, nel senso che non occorre che l'impedimento o turbamento dell'industria o del commercio si verifichino effettivamente, ma è sufficiente l'uso delle violenza sulle cose o di mezzi fraudolenti a ciò finalizzati. Nel caso di specie, si può ipotizzare che possano verificarsi queste citate condotte al fine di rendere la società più competitiva, o per consolidare la propria attività in via sempre più esclusiva o prevalente, avvalendosi di intimidazioni o di atti di coartazione, che inibiscono la normale attività imprenditoriale (vessazioni, boicottaggi, storno di dipendenti, rifiuto a contrattare).

* * *

Una volta individuati i possibili illeciti commettibili astrattamente (meglio identificati nell'allegato relativo ai reati/processi aziendali/cause scatenanti), sono state predisposte apposite "procedure", allegate, al fine di organizzare una segregazione delle funzioni, per diminuirne l'accentramento delle decisioni e per migliorare i controlli e i livelli autorizzativi e, quindi, per diminuire fortemente la realizzabilità di condotte contrarie alla legge.

5. Il sistema sanzionatorio

Il presente MOG prevede specifiche sanzioni disciplinari nei confronti degli amministratori, direttori generali e eventuali *compliance officers* che, per negligenza ovvero imperizia, non abbiano saputo individuare e, conseguentemente, eliminare, violazioni del modello e, nei casi più gravi, perpetrazione di reati.

L'irrogazione delle sanzioni disciplinari previste avverrà in seguito ad un autonomo procedimento che sarà instaurato dopo opportune valutazioni in rapporto alla gravità dell'infrazione e prescindendo dall'eventuale instaurazione del procedimento penale per i fatti costituenti i reati previsti dalle norme in oggetto.

5.1. Le sanzioni disciplinari a carico dei Dipendenti

Sono quelle previste dal CCNL applicabile, nel rispetto delle procedure previste dalle norme in materia ed in specie L. 300/70. In particolare i provvedimenti previsti sono:

a. Biasimo inflitto verbalmente (la violazione di lieve entità delle procedure interne previste dal Modello o adozione di un comportamento, in attività in aeree a rischio, non conformi al Modello stesso) ;
b. Biasimo inflitto per iscritto (in caso di reiterata violazione di lieve entità delle procedure interne previste dal Modello e di molteplici comportamenti non conformi);
c. Multa sino a tre ore di normale retribuzione;
d. Sospensione sino a tre giorni dal lavoro e dalla retribuzione (violazione di grave entità nelle procedure di un comportamento non conforme nonché il compimento di atti contrari all'interesse della società);
e. Licenziamento disciplinare senza preavviso (comportamento non conforme alle prescrizioni del Modello comportanti la concreta applicazione a carico dell'Ente delle misure previste dal D. Lgs. 231/01 con conseguente venir meno della fiducia e impossibilità al prosieguo anche provvisorio del rapporto di lavoro).

Normalmente il biasimo verbale e scritto saranno inflitti nei casi di prima mancanza; la multa nei casi di recidiva, la sospensione nei casi di recidiva per mancanza già punita con la multa nei sei mesi precedenti. Il biasimo, la multa e la sospensione e il licenziamento verranno irrogate nei casi previsti dal CCLN e/o per infrazioni lesive dei principi esposti nel Modello.

È altresì applicabile la sospensione cautelare del dipendente in caso di mancanze che prevedano il licenziamento senza preavviso. La durata non potrà essere superiore ai sei giorni lavorativi. Il datore di lavoro comunicherà per iscritto agli interessati i fatti rilevanti ai fini del provvedimento e ne esaminerà le eventuali deduzioni contrarie.

Le sanzioni verranno irrogate dal Consiglio di Amministrazione.

5.2. Le sanzioni a carico dei Dirigenti

Esse saranno comminate nel rispetto delle disposizioni normative applicabili. In ogni caso le violazioni dovranno essere puntualmente contestate per iscritto dal Consiglio di Amministrazione, con l'osservanza delle procedure normativamente previste, assicurando -in ogni caso- il diritto alla difesa della persona sottoposta a procedimento disciplinare, che potrà essere sentita ovvero potrà presentare difese scritte.

Il provvedimento disciplinare irrogato dovrà essere motivato e comunicato per iscritto al domicilio del/della dirigente.

I provvedimenti disciplinari disposti dal Consiglio di Amministrazione nell'adottare il Modello sono:

1. richiamo scritto alla corretta osservanza ed applicazione del Modello, quale specifico obbligo contrattuale;

2. sospensione immediata dall'incarico in attesa dell'istruttoria per l'accertamento del livello di gravità dell'inosservanza;
   a. qualora l'istruttoria accerti un grado di inosservanza tale da non incidere sul rapporto fiduciario, sarà comminato il richiamo scritto;
   b. ove nel corso dell'istruttoria siano rilevate una gravità dell'infrazione ed una intenzionalità tali da incidere sull'interesse dell'Ente nell'applicazione del Modello e, quindi, sul rapporto fiduciario, costituendo un grave inadempimento ai doveri del dirigente considerato lesivo dei principi contenuti nel Modello stesso, verrà dato corso al procedimento per il recesso dal contratto ai sensi dell'art. 2118 c.c. e dell'art. 2119 c.c. sussistendone i presupposti.

5.3. Sanzioni nei confronti dei componenti del Consiglio di Amministrazione

Salvo quanto previsto sotto il profilo contrattuale, le sanzioni irrogabili ai componenti del Consiglio di Amministrazione che violino le disposizioni del Codice etico e del Modello di organizzazione e di gestione, potranno essere costituite da una multa da un minimo di euro 5.000,00 (cinquemila/00) ad un massimo di euro 50.000,00 (cinquantamila/00); dalla sospensione immediata dall'incarico, fatti salvi l'eventuale revoca per giusta causa e il diritto della società alla richiesta di eventuali danni diretti e indiretti e ad ogni altra azione prevista dal codice civile.
Il procedimento di accertamento della violazione e di irrogazione della sanzione avverrà ad opera del Collegio Sindacale, revisore o OdV.

5.4. Sanzioni nei confronti dei componenti del Collegio sindacale, revisori e OdV

Salvo quanto previsto sotto il profilo contrattuale, le sanzioni irrogabili ai componenti del Collegio sindacale, revisori e OdV che violino le disposizioni del Codice etico e del Modello di organizzazione e di gestione, potranno essere costituite da una multa da un minimo di euro cento ad un massimo di euro mille o dalla sospensione temporanea e immediata dall'incarico, fatti salvi l'eventuale revoca per giusta causa e il diritto dell'Ente alla richiesta di eventuali danni diretti e indiretti e ad ogni altra azione prevista dal codice civile.
Il procedimento di accertamento della violazione e di irrogazione della sanzione avverrà ad opera del Direttore.

5.5. Sanzioni nei confronti di terzi con cui la società instauri rapporti

L'inosservanza delle disposizioni indicate nel Modello di organizzazione e di gestione nonché la violazione dei principi stabiliti nel Codice etico, dei quali deve essere data comunicazione in occasione di ogni convenzione o contratto con soggetti terzi, comporteranno, qualora non sia possibile l'eliminazione delle conseguenze della violazione nel termine perentorio comunicato dalla società, l'immediata risoluzione del contratto ai sensi dell'art. 1456 c.c. Fermo il diritto al risarcimento di tutti i danni diretti e indiretti subiti dalla società.
A tale scopo INFOSYN avrà cura di **inserire in ogni contratto o convenzione una clausola relativa all'obbligo di osservanza dei comportamenti previsti dal Codice Etico e dal Modello di organizzazione e di gestione ed alle conseguenze della loro eventuale inosservanza**.
INFOSYN avrà cura di comunicare nelle forme più idonee il sistema sanzionatorio ai destinatari, evidenziando le possibili conseguenze della violazione del Codice Etico e del Modello.

INFOSYN dovrà comunicare a tutti i soggetti terzi con i quali vengano instaurati rapporti di qualsiasi tipo il sistema sanzionatorio in oggetto. Ai soggetti con i quali sono già in corso rapporti verrà comunicato nei giorni successivi all'adozione del presente modello.

6. Struttura dei presidi di controllo

I presidi finalizzati alla prevenzione del rischio di commissione dei reati previsti dal d.lgs. n. 231 del 2001 affiancano l'osservanza del Codice Etico, principio generale non derogabile del Modello 231/01, e sono strutturati su due livelli di controllo:

1) **standard generali** di trasparenza delle attività, che devono essere sempre presenti in tutte le Attività Sensibili prese in considerazione dal Modello 231/01;

2) **standard di controllo specifici**, che prevedono disposizioni particolari volte a disciplinare gli aspetti peculiari delle Attività Sensibili e che devono essere contenuti negli strumenti normativi aziendali di riferimento. Tali strumenti riportano l'indicazione, tra le normative di riferimento, del Modello 231/01.

Standard generali di trasparenza

Gli "standard generali" di trasparenza delle Attività Sensibili ai sensi del Modello 231/01 sono:

a. **Segregazione delle attività**: **deve esistere segregazione delle attività tra chi esegue, chi controlla e chi autorizza**. Deve essere consentita quantomeno una "dissenting opinion" nel senso che un processo non può essere svolto interamente da una persona senza confrontarsi con altre, specie se questa persona agisce a livello apicale. È attribuita allo standard la seguente qualificazione: il principio della segregazione deve sussistere considerando l'Attività Sensibile nel contesto dello specifico processo di appartenenza; la segregazione sussiste in presenza di sistemi codificati, complessi e strutturati ove le singole fasi siano coerentemente individuate e disciplinate nella gestione, con conseguente limitazione di discrezionalità applicativa, nonché tracciate nelle decisioni assunte.
b. **Norme**: devono esistere disposizioni aziendali idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile;
c. **Poteri di firma e poteri autorizzativi**: devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni idonee anche a garantire che l'attribuzione dei predetti poteri avvenga in coerenza con le responsabilità organizzative assegnate;
d. **Tracciabilità**: i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati devono assicurare l'individuazione e la ricostruzione delle fonti degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della società e le modalità di gestione delle risorse finanziarie.

Gli standard generali di trasparenza sono recepiti dalle funzioni competenti nell'ambito negli strumenti normativi interni riferibili alle Attività Sensibili. Tali strumenti normativi sono comunicati e diffusi dalle funzioni competenti in osservanza delle leggi e dei contratti applicabili e vincolano il management e i dipendenti alla loro osservanza.

Attività Sensibili e standard di controllo specifici

IL CdA può approvare anche il documento "Attività Sensibili e standard di controllo specifici del Modello 231/01", che riguarda le modalità necessarie ad eseguire successivi aggiornamenti dei MOG e prevede disposizioni particolari volte a disciplinare gli aspetti peculiari delle Attività Sensibili e dei relativi presidi di controllo adottati da INFOSYN .

Tale documento:

(i) è custodito presso l'Organismo di Vigilanza,

(ii) è comunicato dall'Organismo di Vigilanza al Direttore nonché alla funzione Amministrazione e al CdA.

Gli standard di controllo specifici sono recepiti dalle funzioni competenti negli strumenti normativi interni riferibili alle Attività Sensibili. Attività Sensibili e standard di controllo specifici sono comunicati alla funzione *Internal Audit* per lo svolgimento delle attività di controllo di competenza.

L'Organismo di Vigilanza ne promuove inoltre la conoscenza e diffusione alle strutture ed organismi interessati, anche a mezzo di strumenti normativi interni.

Gli strumenti che compongono il sistema normativo aziendale sono comunicati e diffusi dalle funzioni aziendali competenti, in osservanza delle leggi e dei contratti applicabili e vincolano il management e i dipendenti alla loro osservanza.

7. L'Organismo di Vigilanza

7.1. Scopo ed ambito di applicazione

È istituito un Organo con funzioni di vigilanza e controllo (di seguito Organismo o OdV) per garantire il funzionamento, l'efficacia, l'adeguatezza e l'osservanza del modello di organizzazione, gestione e controllo (di seguito il Modello) adottato dalla società, allo scopo di prevenire i reati dai quali possa derivare la responsabilità amministrativa della stessa, in applicazione delle disposizioni di cui al D.Lgs. n. 231/2001, recante "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della L. n. 300/2000*" (di seguito "Decreto").

Nell'esercizio delle sue funzioni, l'Organismo deve improntarsi a principi di autonomia ed indipendenza.

A garanzia del principio di terzietà, l'Organismo è collocato in posizione gerarchica di vertice, riportando e rispondendo direttamente ed esclusivamente all'Amministratore unicoad.

7.2. Nomina e composizione

L'Organismo è monocratico o collegiale. Il Presidente del CdA nomina, ai sensi dell'art. 6 del Decreto, l'Organismo con delibera o provvedimento motivato, scelto esclusivamente fra soggetti in possesso dei necessari requisiti di autonomia, indipendenza, onorabilità, professionalità, competenza e continuità d'azione richiesti dal D. Lgs. 231/01.

L'Organismo di Vigilanza è scelto tra soggetti esterni, qualificati ed esperti. In particolare, l'OdV, tramite i suoi componenti, deve garantire competenze del settore in cui opera la società e le sue eventuali società controllate in ambito in ambito legale, contabile, di analisi delle procedure e dei processi organizzativi aziendali. Inoltre, i componenti devono garantire adeguata professionalità nelle anzidette materie ed essere in possesso dei requisiti di onorabilità.

L'Organismo svolge le sue funzioni curando e favorendo una razionale ed efficiente cooperazione con gli organi e le funzioni di controllo già esistenti.

7.3. Requisiti dell'Organismo di Vigilanza

Il Modello adottato intende attuare rigorosamente le prescrizioni del Decreto in relazione ai requisiti che l'Organismo di Vigilanza deve possedere e mantenere nel tempo. In particolare:

a) l'autonomia e l'indipendenza sono garantiti con l'inserimento in una posizione referente al CdA per fatti censurabili che dovessero coinvolgere gli amministratori; il requisito dell'autonomia è garantito inoltre dalla

non attribuzione all'Organismo di compiti operativi rilevanti ai fini 231/01 (che ne minerebbero l'obiettività di giudizio nel momento delle verifiche) e dall'assegnazione di un budget di spesa per l'esatto adempimento delle funzioni dell'organismo;

b) la professionalità è garantita dall'esperienza dell'Organismo che è dotato delle competenze specialistiche proprie di chi svolge attività consulenziali o ispettive e necessarie per l'espletamento delle proprie funzioni. In particolare l'Organismo è dotato di:
   - competenze legali: adeguata padronanza nella interpretazione delle norme di legge con specifica preparazione nell'analisi delle fattispecie di reato individuabili nell'ambito dell'operatività aziendale e nella identificazione di possibili comportamenti sanzionabili;
   - competenze nella organizzazione: adeguata preparazione in materia di analisi dei processi organizzativi aziendali e nella predisposizione di procedure adeguate alle dimensioni aziendali, nonché dei principi generali sulla legislazione in materia di "*compliance*" e dei controlli correlati;
   - competenze "ispettive": esperienza in materia di controlli interni maturati in ambito aziendale;
   - competenze di "revisione" e in tecniche di campionamento statistico (stratificazione, elaborazione, ecc.).

c) la continuità d'azione è garantita dalla calendarizzazione delle attività dell'Organismo di Vigilanza, dalla periodicità dei propri interventi ispettivi, dalla regolarità delle comunicazioni verso i vertici aziendali.

7.4. Durata, revoca e recesso dei componenti

Il componente dell'Organismo resta in carica per tre anni ed è sempre rieleggibile.

Il CdA può revocare in ogni momento l'Organismo, per giustificato motivo.

Costituiscono cause di ineleggibilità e/o decadenza dalla carica di Organismo:

a) le circostanze di cui all'art. 2382 del Codice Civile;

b) la sentenza di condanna, anche non definitiva, o di patteggiamento per aver commesso uno dei reati previsti dal Decreto;

c) una sentenza di condanna ai sensi del Decreto, di primo grado, ovvero un procedimento penale concluso tramite c.d. "patteggiamento", ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

d) la sentenza di condanna anche non definitiva a pena o di patteggiamento che comporta l'interdizione, anche temporanea, dai pubblici uffici, oppure l'interdizione, anche temporanea, dagli uffici direttivi delle persone giuridiche e delle imprese;

Nei casi sopra descritti, il CdA provvederà contestualmente alla revoca e, senza ritardo, a nominare il nuovo Organismo, in sostituzione di quello cui sia stato revocato il mandato.

La rinuncia da parte componenti del componente dell'Organismo può essere esercitata in qualsiasi momento (mediante preavviso di almeno 1 mese), previa motivata comunicazione al CdA per iscritto.

7.5. Funzioni e poteri

L'Organismo è chiamato a svolgere le seguenti attività:

- verifica della diffusione in azienda della conoscenza e della comprensione del Modello;
- vigilanza sull'osservanza del Modello all'interno della società;
- vigilanza sulla validità ed adeguatezza del Modello, con particolare riferimento ai comportamenti

riscontrati nel contesto aziendale;

- verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal D.Lgs. n. 231/2001;
- proposta di aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni ed adeguamenti dello stesso, in relazione alle mutate condizioni aziendali e/o legislative;
- comunicazione e relazione periodica al CdA in ordine alle attività svolte, alle segnalazioni ricevute, agli interventi correttivi e migliorativi del Modello suggeriti e al loro stato di realizzazione.

Nell'ambito delle attività di cui al precedente comma, l'Organismo provvederà ai seguenti adempimenti:

- verificare nel contesto aziendale la conoscenza e la comprensione dei principi delineati nel Modello;
- proporre un piano annuale di formazione, volto a favorire la conoscenza dei principi del Modello e del Codice Etico, differenziato secondo il ruolo e la responsabilità dei destinatari;
- raccogliere, elaborare, conservare e aggiornare ogni informazione rilevante ai fini della verifica dell'osservanza del Modello;
- verificare e controllare periodicamente le aree/operazioni a rischio individuate nel Modello;
- verificare e controllare la regolare tenuta ed efficacia di tutta la documentazione inerente le attività/operazioni individuate nel Modello;
- istituire specifici canali informativi "dedicati", diretti a facilitare il flusso di segnalazioni ed informazioni verso l'Organismo;
- segnalare tempestivamente al CdA qualsiasi violazione del Modello che sia ritenuta fondata dall'Organismo stesso, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o che abbia accertato lui stesso;
- valutare periodicamente l'adeguatezza del Modello rispetto alle disposizioni ed ai principi regolatori del D.Lgs. n. 231/2001 e relativo aggiornamento;
- trasmettere tempestivamente al CdA ogni informazione rilevante al fine del corretto svolgimento delle funzioni proprie dell'Organismo, nonché al fine del corretto adempimento delle disposizioni di cui al D. Lgs. 8 giugno 2001, n. 231;
- trasmettere, con periodicità semestrale, una relazione al CdA in merito all'attività complessivamente svolta, ai necessari e/o opportuni interventi correttivi e migliorativi del Modello e al loro stato di realizzazione.

Ai fini dello svolgimento degli adempimenti elencati al comma precedente, all'Organismo sono attribuiti i poteri qui di seguito indicati:

- accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D.Lgs. n. 231/2001;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
- disporre che i Responsabili di funzione forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;
- segnalare comportamenti in violazione al Modello ed al Codice Etico per i provvedimenti disciplinari che la

società riterrà di adottare.

8. Verifiche periodiche del Modello

Il presente modello sarà soggetto a due tipologie di verifiche:

1. un'attività di monitoraggio periodico sull'effettiva applicazione dei modelli, protocolli e procedure, anche tramite verifiche a campione;
2. analisi, in occasione delle segnalazioni ricevute, degli eventi considerati rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alle problematiche della responsabilità penale dell'Ente anche tramite verifiche a campione.

9. Formazione e Diffusione del Modello

Ai fini dell'attuazione dei Modelli occorre provvedere alla formazione del personale, a cura del Responsabile della Gestione Risorse Umane in stretta cooperazione con l'OdV. La formazione viene differenziata in base al soggetto destinatario, essendo rivolta ai dipendenti nella loro generalità, ai dipendenti che operino in specifiche aree di rischio, all'organo di vigilanza ed ai preposti al controllo interno. Il contenuto dei corsi di formazione deve riguardare la disciplina normativa, la prassi, la giurisprudenza, le procedure della società e eventualmente l'analisi di casi comparabili. È obbligatoria la frequenza e la partecipazione ai corsi, i quali devono prevedere: test di ingresso (eventuale); spiegazione frontale o mediante slide / corso on ine su intranet/e-learning; test di comprensione finale; firme di partecipazione. I programmi di formazione vanno controllati dall'OdV prima della somministrazione, anche in riferimento alla qualità.

9.1. Formazione del personale apicale

La formazione del personale apicale e del personale fornito di poteri di rappresentanza dovrà avvenire a cura del Responsabile della Gestione Risorse Umane estendendo anche ai nuovi assunti un seminario di aggiornamento annuale e l'accesso ad un sito intranet dedicato all'argomento.

L'ufficio Gestione Risorse Umane in collaborazione con l'OdV provvederà a curare la diffusione del Modello e del Codice Etico.

9.2. Formazione del personale sottoposto

La formazione di soggetti diversi da quelli rientranti nel precedente paragrafo dovrà avvenire sulla base di una nota informativa interna, in un'informativa nella lettera di assunzione, l'accesso a intranet e email di aggiornamento.

9.3. Informazione a collaboratori esterni e fornitori

A tutti i soggetti che collaborano con la società dovranno essere fornite apposite informative sulle procedure adottate e dovrà essere curato in collaborazione con l'OdV la diffusione del Codice Etico.

Ogni comportamento posto in essere in contrasto con le linee di condotta indicate nel presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal D. Lgs. 231/01 potrà determinare, grazie ad **apposite clausole che verranno inserite dall'Ufficio Acquisti**, la risoluzione del rapporto contrattuale.

10. Il Codice Etico

Il Codice Etico si applica a tutte le attività della società. L'osservanza dei principi e delle disposizioni del Codice etico sono vincolanti per tutti i soggetti che operano per il conseguimento degli obiettivi della società, siano essi soggetti in posizione apicale, quali gli amministratori, sia dirigenti, soggetti con funzioni di direzione o rappresentanza, dipendenti e tutti coloro che operano con INFOSYN sulla base di un rapporto contrattuale, anche temporaneo. I dipendenti e i collaboratori non subordinati e tutti coloro che intrattengono rapporti contrattuali con INFOSYN sono tenuti ad adeguare i propri comportamenti alle disposizioni del Codice etico. Il Codice Etico viene messo a disposizione dei fornitori (eventualmente anche con strumenti informatici o tramite sito web) invitandoli a rispettarne i principi ed i criteri di condotta, nell'ambito dei rapporti che essi hanno con la stessa società. La Direzione o il Presidente si impegnano a divulgare il Codice Etico presso i destinatari, mediante apposite attività di comunicazione. In nessun caso il perseguimento di un interesse o di un vantaggio per la società può giustificare un comportamento non corretto. Ogni comportamento contrario allo spirito del Codice Etico sarà sanzionato in modo proporzionato alla gravità delle eventuali infrazioni commesse, in conformità con quanto previsto dal sistema disciplinare definito dal Modello Organizzativo, di cui il presente Codice Etico è presidio e parte integrante e sostanziale.

11. Valutazione del rischio in itinere, controlli e segnalazioni all'OdV

Il Modello organizzativo prevede sistematiche procedure di ricerca e di identificazione dei rischi da attivare quando sussistano circostanze particolari, quali ad esempio l'emersione di precedenti violazioni; un elevato turn-over del personale; notizie su quotidiani locali, nazionali o internazionali relativi a violazioni anche presunte da parte dell'ente o suoi apicali o suoi dipendenti/collaboratori-trici. A tal proposito occorre utilizzare la matrice del rischio suggerita da ANAC – Autorità Anti-Corruzione, compilando le fattispecie previste e graduandole in base alla gravità degli eventi e possibilità di commissione dei reati (cfr. la normativa ANAC e le scale Likert relative alle possibili risposte e graduazione del rischio, basate sullo standard ISO 31000).

Il Modello prevede che l'OdV possa effettuare controlli di routine e controlli a sorpresa, oltre agli audit periodici, nei confronti delle attività aziendali sensibili.

Vige l'obbligo per i/le dipendenti, i/le direttori/trici, gli amministratori/trici, Presidente, Consiglieri/e di riferire all'organismo di vigilanza ogni notizia rilevante relativa alla vita dell'ente, connessa a violazioni (anche ipotizzate) del modello o alla consumazione di reati. In particolare coloro che vengano a conoscenza di comportamenti illeciti devono riferire all'organo di vigilanza mediante la casella di posta elettronica dedicata all'OdV.

Al fine di rendere massimamente efficace il sistema delle segnalazioni, è stata predisposta la procedura *whistleblowing*, relativa alla segnalazione delle anomalie con protezione dell'anonimato della persona che esegue la segnalazione. Essa costituisce un "modello organizzativo" a sé stante ed è da utilizzarsi mediante l'uso della apposita modulistica.

12. Anticorruzione e trasparenza

Il Modello organizzativo e gestionale (MOG) di INFOSYN costituisce istruzione organizzativa e presidio antireato, soprattutto in materia di prevenzione della corruzione e di *maladministration*. Gli allegati relativi a policy anticorruzione e procedure organizzative 231/01 sono, nella pratica, gli strumenti quotidianamente attuati e controllati per garantire una attività lavorativa trasparente e al mero al servizio della cittadinanza e utenza.

D'altronde la prevenzione della corruzione è stata impostata in modo che non costituisca una attività da svolgersi *una tantum*, ma un processo ciclico, in cui le strategie e gli strumenti aziendali vengono via via affinati, modificati o sostituiti in relazione ai feedback ottenuti nella loro applicazione.

In particolare il presente MOG, che recepisce quanto previsto già nel PTPC di INFOSYN 2016-2018, ingloba tutte le misure previste dalla normativa in tema di prevenzione della corruzione, nella sua più ampia accezione, nonché quelle ulteriormente stabilite nei MOG 231/01 approvato nel 2016 da Infosyn, mediante delibera del CdA cui si fa rimando.

Per lo svolgimento delle attività Infosyn ha deliberato, da parte del CdA, **obiettivi strategici in materia di trasparenza** e **anticorruzione**, ai sensi dell'art. 1, co. 8, l. 190/2012 e delle Linee Guida ANAC 2016 del 29 dicembre 2016 rubricate "Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016".

In dettaglio, gli **obiettivi** sono:

- Evitare non solo corruzione, concussione, altri reati contro la PA e corruzione tra privati, ma anche *mala gestio* o *maladministration*.
- Prevenire condotte di per sé lecite, ma parte di un più vasto disegno illecito (assunzione dipendenti, sponsorizzazioni, consulenze quali contropartite di più vasti disegni corruttivi);
- Rendicontare trasparentemente la propria attività alla cittadinanza e altri stakeholder;
- Promozione di maggiori livelli di trasparenza (art. 10, c. 3, d.lgs. 33/2013);
- Collegare l'accesso obbligatorio con l'accesso generalizzato;
- ridurre il rischio *maladministration* nei processi aziendali valutati con livello "medio/alto" o "critico" mediante definizione dei criteri da seguire per la rotazione del personale;
- perseguire una attiva partecipazione degli stakeholder interni ed esterni nella elaborazione e nell'attuazione delle misure di prevenzione della corruzione, anche attraverso comunicati mirati, in una logica di sensibilizzazione dei cittadini alla cultura della legalità;
- Mantenere una formazione anticorruzione aggiornata sia ad apicali sia a persone sottoposte.
- Prevedere un costante coordinamento tra gli obiettivi strategici in materia di trasparenza contenuti nel MOG unito al PTPCT e gli obiettivi degli altri documenti di natura programmatica e strategico-gestionale.

Le **soluzioni organizzative** idonee ad assicurare l'adempimento degli obblighi di pubblicazione di dati e informazioni previsti dalla normativa vigente sono:

- Predisposizione di relazione periodica per l'organo di indirizzo, da parte della RPCT, per comprendere eventuali disfunzioni riscontrate inerenti l'attuazione delle misure di prevenzione e di trasparenza;

- Unificazione della figura del RPC con l' RT e affidamento dell'incarico a una dei 5 consiglieri di amministrazione (indipendente e senza deleghe) rispetto alla previgente situazione che prevedeva l'incarico all'unico dirigente che, nel contempo, è anche Direttore Generale.
- Creazione di un database dei documenti non obbligatoriamente pubblicabili ma più frequentemente richiesti dall'utenza mediante nuovo accesso civico;
- Pubblicazione di F.A.Q. in materia di accesso civico;
- Organizzazione di attività di risposta all'accesso in modo da minimizzare l'impatto economico finanziario;
- Organizzazione di attività di risposta all'accesso in modo da minimizzare i tempi di lavorazione e risposta;
- Attivazione di strumenti di partecipazione per l'aggiornamento del *risk assessment* e delle misure anticorruzione (stakeholder engagement, ai sensi della norma AA1000SES e standard ISO 26000);
- Attivazione di **procedure** per la costante mappatura dei processi, per la loro valutazione (*risk assessment*) e per l'individuazione delle misure idonee al loro successivo trattamento e attuazione (*audit* e *gap analysis* e *action plan*);
- Monitoraggio dell'applicabilità del deliberato Codice di Comportamento per il personale della società ;
- Definizione di criteri generali per il conferimento di incarichi, nonché i criteri per l'autorizzazione degli incarichi extra-istituzionali, in adesione a quanto verrà stabilito dai Regolamenti di cui all'articolo 53, comma 3 bis, del d.lgs. n. 165/2001;
- Avvio di forme di monitoraggio, anche informatiche, sull'implementazione del P.T.P.C;
- Previsione di monitoraggio del canale whistleblowing (come da istruzioni ANAC) anche in relazione a eventuali misure discriminatorie dirette o indirette nei confronti della RPCT;
- Previsione di una struttura organizzativa di supporto alla RPCT adeguata (per qualità del personale e per mezzi tecnici) ai fini di garantirle lo svolgimento adeguato del proprio compito (nello specifico si tratta di tre figure composte da: Direttore; assistente amministrativa: OdV dei MOG 231/01);
- Diffusione di comunicato interno in cui si invitano tutti i soggetti responsabili di processi o di procedure a fornire massima collaborazione alla RPCT. Eventuali atti ufficiali di organizzazione interna o nomine/modifica mansionari, ai fini di garantire responsabilità in materia di invio periodico di flussi informativi alla RPCT.

***

La presente sezione sulla trasparenza viene essere impostata come atto organizzativo fondamentale dei flussi informativi necessari per garantire, all'interno di INFOSYN , l'individuazione/l'elaborazione, la trasmissione e la pubblicazione dei dati da porre nella sezione "amministrazione trasparente" del sito internet istituzionale.

Nella presente sezione segue l'indicazione dei nominativi delle persone responsabili della trasmissione dei dati (art. 10, co. 1, d.lgs. 33/2013), intesi quali uffici tenuti alla individuazione e/o alla elaborazione dei dati, e di quelli cui spetta la pubblicazione.

Si specifica che il dettaglio dei singoli obblighi di pubblicazione è contenuto nella più vasta tabella allegata al presente MOG.

Persone responsabili dei flussi informativi ai fini della pubblicazione on line dei dati nella sezione "società trasparente" posizionata nel sito web istituzionale (peraltro opzionale in TNAA ex art. 1, c. 1, L.R. n. 16/2016, ma pubblicato per maggiore trasparenza ai sensi del nuovo art. 7 bis c. 3, inserito nel d.lgs. 33/2013 dal d.lgs. 97/2016):

- Responsabile primaria della trasparenza e anticorruzione: M. Vidoni (Direttore e RPCT).
- Responsabile operativa: F. Beghini (Responsabile legale) elaboratore del dato e addetto alla trasmissione dell'informazione alla ditta software che si occupa materialmente di eseguire la pubblicazione on *line*.
- Soggetto preposto all'iscrizione e all'aggiornamento dei dati (**RASA**) nell'Anagrafe unica delle stazioni appaltanti (AUSA): M. **Vidoni** (Dirigente, Direttore).
- Responsabili secondari dei flussi informativi verso il Direttore, in ambito **amministrativo/contrattuale**: F. Beghini e M. Leccese (per la pubblicazione)
- Responsabili secondari dei flussi informativi verso il Direttore, in ambito **contabile/fiscale**: S. Bottura e M. Leccese (per la pubblicazione)
- Responsabili secondari dei flussi informativi verso il Direttore, in ambito **gare e appalti**: C. Gemelli, F. Beghini e M. Leccese (per la pubblicazione)
- Responsabili secondari dei flussi informativi verso il Direttore, in ambito **concorsi e assunzione di personale**: M. Granieri, F. Beghini e M. Leccese (per la pubblicazione)

***

I **termini** entro i quali si prevede l'effettiva pubblicazione di ciascun dato sono contenuti nella tabella allegata.

***

Modalità stabilite per la **vigilanza** ed il **monitoraggio** sull'attuazione degli obblighi:

la vigilanza sulle pubblicazioni *on line* viene eseguita dalla figura **RPCT** (responsabile prevenzione corruzione e trasparenza), coadiuvata ove ritenga dall'**OdV** dei MOG 231/01 (Organo di Vigilanza). Queste figure svolgono *audit* periodici, nell'ambito del più vasto piano di audit delle procedure e delle parti speciale dei modelli organizzativi e gestionali redatti ai sensi e per gli affetti di cui al d.lgs. 231/01.

Le risultanze degli audit vengono comunicate al Direttore e, in seconda fase, al CdA.

Il Direttore, laddove competente, prende i provvedimenti operativi al fine di migliorare eventuali processi operativi e/o eliminare irregolarità o aggiornare parti che lo necessitano.

Laddove il Direttore non abbia competenza, il CdA provvede a deliberare miglioramenti dei processi operativi e/o eliminare irregolarità o aggiornare sezioni e documenti e personale che lo necessitano.

Le risultanze degli audit dell'OdV vengono inserite nella relazione annuale dell'OdV, inviata al CdA.

Ad una funzione interna in INFOSYN è stato attribuito il compito di monitorare costantemente la legislazione nazionale e locale e di riferire al Direttore e all'OdV, in modo da restare sempre al passo con le norme nazionali, locali e determinazioni ANAC.

Il Direttore e l'OdV periodicamente si formano in materia di anticorruzione e trasparenza, anche mediante lettura della documentazione o partecipazione agli eventi di categoria.

Il RPCT si occupa di svolgere la regia complessiva della predisposizione del PTPCT inglobato nel MOG, in costante coordinamento con le strutture dell'amministrazione. In particolare, la RPCT si occupa di mantenere sistematiche procedure di ricerca e di identificazione dei rischi da attivare quando sussistano circostanze particolari, quali ad esempio l'emersione di precedenti violazioni; un elevato turn-over del personale; notizie su quotidiani locali,

nazionali o internazionali relativi a violazioni anche presunte da parte dell'ente o suoi apicali o suoi dipendenti/collaboratori-trici. A tal proposito occorre utilizzare la matrice del rischio suggerita da ANAC – Autorità Anti-Corruzione, compilando le fattispecie previste e graduandole in base alla gravità degli eventi e possibilità di commissione dei reati (cfr. la normativa ANAC e le scale Likert relative alle possibili risposte e graduazione del rischio, basate sullo standard ISO 31000).

A fini di garantire forme di consultazione per la predisposizione del proprio modello anticorruzione, onde poter giungere a una massima diffusione del lavoro e ad un corrispettivo coinvolgimento delle comunità di stakeholder nelle strategie di prevenzione di *mala gestio,* in ottemperanza alle disposizioni del Piano Nazionale Anticorruzione la figura Responsabile della prevenzione della corruzione (RPCT) concorderà specifici incontri con gli addetti alle aree amministrative, con il Revisore legale e con altri responsabili di processi aziendali.

RPCT avvierà inoltre la raccolta, via web, dei contributi dei componenti della comunità locale, oltre che monitorare il canale *whistleblowing* e organizzare la giornata della trasparenza, ove convocare i soci e gli stakeholder della comunità locale e invitare come relatori alcuni docenti universitari, giudici, esperti legali o comunque esperti della materia "anticorruzione".

Ciò appare fondamentale anche ai fini dell'analisi del contesto esterno e interno. "L'analisi del contesto" è fondamentale per ottenere una serie di informazioni necessarie a comprendere come il rischio corruttivo possa verificarsi all'interno dell'amministrazione - azienda per via delle specificità dell'ambiente in cui essa opera; ciò in termini di strutture territoriali e di dinamiche sociali, economiche e culturali, o per via delle caratteristiche organizzative interne. Specie laddove, come nel nostro caso, si faccia riferimento al concetto di corruzione in senso ampio, sulla base di quanto riportato nell'aggiornamento 2015 al PNA: non ci si riferisce solo allo specifico reato di corruzione o complesso dei reati contro la pubblica amministrazione, ma anche al più vasto concetto di "maladministration". Essa è da intendersi come "mala gestio", intesa come l'assunzione di decisioni (di assetto di interessi a conclusione di procedimenti, di determinazioni di fasi interne a singoli procedimenti, di gestione di risorse pubbliche) devianti dalla cura dell'interesse generale a causa del condizionamento improprio da parte di interessi particolari. Occorre, cioè, avere riguardo ad atti e comportamenti che, anche se non consistenti in specifici reati, contrastano con la necessaria cura dell'interesse pubblico e pregiudicano l'affidamento dei cittadini nell'imparzialità delle amministrazioni e dei soggetti che svolgono attività di pubblico interesse.

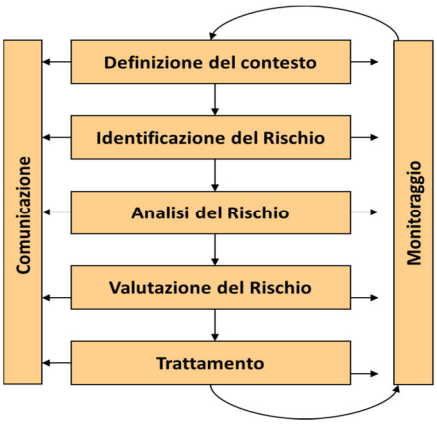
Circa l'analisi del **contesto esterno** ad INFOSYN , con il periodico *risk assessment* si è scelto come obiettivo quello di evidenziare talune caratteristiche dell'ambiente nel quale INFOSYN opera, con riferimento in particolare a fattispecie di reato connesse astrattamente all'oggetto sociale della società. Sono stati considerati, quindi, fattori legati al territorio di riferimento, relazioni e possibili influenze esistenti con i portatori di interessi esterni; sentenze dei Tribunali civili, penali e amministrativi; dati contenuti nelle relazioni periodiche sullo stato dell'ordine e della sicurezza pubblica, presentate al Parlamento dal Ministero dell'Interno e pubblicate sul sito della Camera dei Deputati (Ordine e sicurezza pubblica e D.I.A. relativi alla provincia di Trento e Bolzano); patteggiamenti, anche in ottica di responsabilità amministrativa degli enti.

Tale quadro di riferimento consente di meglio comprendere le dinamiche territoriali e le principali influenze e pressioni a cui INFOSYN è potenzialmente sottoposta, al fine di indirizzare con maggiore efficacia e precisione la strategia di gestione del rischio.

Dal punto di vista metodologico il *risk assessment* si è basato sui principi contenuti nello standard internazionale (suggerito anche da ANAC) denominato ISO 31000, con l'utilizzo specifico di criteri di valutazione meglio esplicati nella ISO 31010.

È stato anche considerato lo standard ISO 37001, specifico in materia di corruzione nelle pubbliche amministrazioni e società/enti partecipati, sebbene tale riferimento ha costituito soltanto una guida di principio, essendo tale standard in fase di circolazione in modalità di *draft,* con approvazione finale prevista per la primavera 2016.

Sostanzialmente sono stati applicati i passaggi indicati nelle figure seguenti:



In dettaglio, circa l'analisi del **contesto interno** ad INFOSYN , con il *risk assessment* sono state mappate le deleghe, le responsabilità, il livello di complessità della società; gli organi di indirizzo, la struttura organizzativa, i ruoli operativi per prassi; le politiche, gli obiettivi e le strategie attuali e future; le risorse, le conoscenze, i sistemi informativi e le tecnologie utilizzate; la qualità e la quantità del personale; la cultura organizzativa, con particolare riferimento alla cultura dell'etica d'impresa in chiave di "corporate social responsibility" e di condotte di impresa responsabili (cfr. L.G.Ocse e PCN italiano presso il Mise); i sistemi e i flussi informativi, i processi decisionali (sia formali sia informali); le relazioni interne e con il contesto esterno.

Il PNA suggerisce di focalizzare questo tipo di analisi su alcune "aree di rischio obbligatorie", tenuto conto di dieci domande che misurano la probabilità di reato e l'impatto, giungendo così -tramite moltiplicazione di questi due fattori-, al c.d. "rischio residuo".

In INFOSYN si è scelto dapprima di ampliare le aree di valutazione del rischio e, successivamente, di inserire altre variabili e domande, al fine di meglio comprendere la probabilità di reato lorda, i presidi e le difese esistenti, la probabilità di reato netta, l'impatto lordo, le procedure o sistemi di abbattimento dell'impatto negativo, l'impatto netto e, di conseguenza, il rischio residuo. Ciò è avvenuto conformemente allo standard ISO 31010, mediante somministrazione di una intervista semi-strutturata e di alcuni questionari, ciascuno contenente 29 domande (comprensive delle 10 domande suggerite da ANAC). essi sono stati somministrati ai responsabili dei processi e poi ripetuti per ogni attività identificabile come "procedimento amministrativo" o "processo aziendale" o "fase endoprocessuale" (laddove rilevante). Mediante scale Likert si è giunti alla rappresentazione del rischio.

Le **aree specifiche** monitorate, oltre alle quattro generali suggerite da ANAC (A,B,C,D), si riferiscono ai controlli, alla gestione delle entrate, alle spese e patrimonio; alle verifiche, ispezioni e sanzioni; agli incarichi e nomine; agli affari legali e contenzioso.

Le **variabili utilizzate**, in relazione ad ogni singolo processo e procedimento mappato, hanno avuto ad oggetto le seguenti informazioni:

A. Calcolo della probabilità di reato:
   - Discrezionalità del processo
   - Rilevanza esterna
   - Complessità
   - Valore economico
   - Frazionabilità
   - Tempi di istruttoria
   - Provvedimenti disciplinari passati
   - Indagini magistratura in corso

B. Calcolo dell'impatto
   - Impatto organizzativo persone coinvolte

- Impatto economico
- Impatto sull'immagine
- Impatto sulla reputazione

C. Fattori che abbassano la probabilità e/o l'impatto
- Controlli e loro efficacia (vari livelli)
- Esistenza di precedenti
- Rimozione dei responsabili di illeciti
- Presenza di procedure
- Presenza di codici etici o altri presidi assimilabili
- Segregazione delle funzioni (doppie firme, dissenting opinion, ecc.)
- Referenti periferici RPCT
- Software automazione trasparenza
- Formazione
- Sistema MBO con kpi di "maladministration"
- *Whistleblowing*.

Nel corso dell'intervista è stato inoltre richiesto di indicare se vi fossero anche altre attività, processi, pareri, atti o procedimenti non precedentemente mappati. Una volta individuati tali ulteriori processi e attività, si è proceduto a riproporre le predette domande anche in relazione ad essi.

È stata analizzata pertanto ogni attività, processo e procedimento di ciascuna area di rischio suggerita da ANAC nel PNA:

"A": Acquisizione del personale e progressione carriera;

"B": Affidamento di lavori, servizi e forniture;

"C": Provvedimenti ampliativi della sfera giuridica dei destinatari **privi** di effetto economico diretto ed immediato per il destinatario;

"D": Provvedimenti ampliativi della sfera giuridica dei destinatari **con** effetto economico diretto ed immediato per il destinatario,

e nelle aree aggiuntive:

"E": controlli, verifiche, ispezioni e sanzioni;

"F": altre attività tipiche di cui all'oggetto sociale;

"G": pareri e attività propedeutica ad autorizzazioni/innovazioni;

"H": incarichi e nomine;

"I": affari legali e contenzioso.

A fronte dei calcoli effettuati, ad ogni procedimento e processo oggetto dei predetti quesiti è stato attribuito un punteggio ottenuto dal prodotto tra la media ponderata della probabilità (probabilità, presidi e controlli) e la media dell'impatto, graduando così il rischio finale di ogni processo e procedimento nell'ambito di un range che varia da 0 a 25, così suddiviso:

- da 0 a 6,25, indice di procedimento o processo a rischio **basso**;
- da 6,26 a 12,50 indice di procedimento o processo a rischio **medio**;
- da 12,51 a 18,75 indice di procedimento o processo a rischio **elevato**;
- da 18,76 a 25 indice di procedimento o processo a rischio **critico**.

Sono stati ritenuti a rischio medio i settori con almeno un (1) procedimento o processo a rischio medio, senza processi né procedimenti a rischio elevato né critico;

Sono stati ritenuti a rischio elevato i settori con almeno un (1) procedimento o processo a rischio elevato, senza processi né procedimenti a rischio critico;

Sono stati ritenuti a rischio critico i settori con almeno un (1) procedimento o processo a rischio critico oppure quelli connessi a budget superiori a un miliardo di euro.

Si specifica, infine, che la valutazione così ottenuta non costituisce un giudizio sull'operato del personale o del Direttore o CdA. Una valutazione di processo "critico" o a rischio corruzione "elevato" deriva generalmente dalla mancanza di adeguati presidi o di protezioni e indica il pericolo che la persona addetta alle funzioni analizzate subisca attacchi corruttivi dall'esterno, in assenza di adeguati presidi.

Nell'analisi di dettaglio, settori apparentemente ad elevato rischio corruzione potranno risultare valutati a rischio minore, laddove dotati di difese e presìdi o se sono state adottate tutte le misure che erano possibili, in base a prassi e casi comparabili o sentenze che suggeriscono vie per evitare comportamenti illeciti. Del pari, settori apparentemente a basso rischio potranno risultare a rischio maggiore del previsto qualora il/la Dirigente o addetto/a non abbia attuato le misure, difese e presidi volti ad evitare che un evento illecito venga compiuto.

Dall'analisi del contesto e della situazione generale di INFOSYN è stato riscontrato un livello di applicazione dei presìdi buono. Le criticità sono eccezionali sebbene permangono alcuni processi a rischio elevato. Per diminuire il rischio sono tuttavia sufficienti accorgimenti semplici, poco onerosi, interni, celeri, che possono abbassare di molto i livelli di rischiosità.

Dall'analisi condotta, alla quale hanno partecipato apicali e altri soggetti coinvolti nei processi aziendali, sono emersi dati significativi in relazione ai livelli di rischio connessi ad ogni singola area/processo di INFOSYN .

SETTORE o MACRO ATTIVITA'	Processo (attività, azione, atti pareri, "procedimento amministrativo", processo, attività endoprocessuale)	Area a rischio corruzione (PNA)	Rischio reato, condotta irresponsabile o di "maladministration"	Valore finale del "rischio residuo" (range: 1-25)
SERVIZI e "vendite"	attività di sportello per i servizi di fatturazione (per conto delle aziende elettriche)	D	falso o Abuso nella discrezionalità della scelta	12,00
	lettura contatori	D	falso materiale	18,54
	contabilizzazione	C	falso o errore	12,00
	dichiarazioni periodiche	C	corruzione, concussione, falso	12,96
	incassi e solleciti di pagamento	D	corruzione, concussione, falso	16,85
	stampa e spedizione bollette	C	falso o errore	12,00
	telegestione dei contatori	D	corruzione, concussione, falso	16,85
	Fatturazione	D	corruzione, concussione, falso	12,32
	perequazione	C	Inosservanza delle regole procedurali	12,00
	UTF	C	Inosservanza delle regole procedurali	12,00
	Unbundling	C	Inosservanza delle regole procedurali	12,64

SETTORE o MACRO ATTIVITA'	Processo (attività, azione, atti pareri, "procedimento amministrativo", processo, attività endoprocessuale)	Area a rischio corruzione (PNA)	Rischio reato, condotta irresponsabile o di "maladministration"	Valore finale del "rischio residuo" (range: 1-25)
	noleggio apparecchiature informatiche (stampanti, computer, telefonia, ecc)	D	concussione, corruzione	12,00
	messa a disposizione software (fatturazione, contabilità, ecc.)	D	promessa indebita	12,00
	consulenza varie (ad esempio, SAP per clienti esterni, contabilità, ecc.)	D	corruzione	12,00
	gestione contabilità	D	falso materiale	12,00
	riparazioni hardware - assistenza software	D	corruzione, falso	11,68
	digitalizzazione reti (gis)	D	falso, errore	12,00
	gestione impianti di produzione	D	concussione	12,32
	portali web	D	falso, concussione	12,00
	attività di sportello CAR SHARING	C	concussione, corruzione	12,15
	Attività diretta di sportello e di fatturazione e incasso per il Comune di Fortezza	D	Mancata segnalazione debitori prima di procedura esecutiva; riconoscimento requisiti inesistenti per agevolare taluni soggetti	16,30
RAPPORTI con la PA	Colloqui con clienti "PA"	D	corruzione, concussione	20,69
	Saltuaria richiesta di autorizzazioni	D	corruzione, concussione	17,28
	Invio documentazione periodica a PA locali o nazionali, per la propria azienda	D	falso materiale, errore	11,52
	Invio documentazione periodica a PA locali o nazionali, per conto di clienti (cfr. anche sezione "SERVIZI" di vendita)	D	falso materiale, associazione a delinquere, corruzione	12,48
Management	Gestione modello organizzativo 231/01	E	abuso d'ufficio, errore, falso	13,33
	Gestione piano triennale anticorruzione	E	corruzione	13,33
	Gestione piano triennale trasparenza	E	corruzione	13,33

SETTORE o MACRO ATTIVITA'	Processo (attività, azione, atti pareri, "procedimento amministrativo", processo, attività endoprocessuale)	Area a rischio corruzione (PNA)	Rischio reato, condotta irresponsabile o di "maladministration"	Valore finale del "rischio residuo" (range: 1-25)
	Organizzazione giornata annuale trasparenza	E	corruzione	13,33
Gestione visite ispettive	**Gestione Visite Ispettive (Arpal, Noe, Ag Entrate, Provincia tramite Arpal, INAIL, ASL, Forestale, ecc.)**	F	corruzione	20,06
Rapporti con i SOCI	**Gestione rapporti con Soci** (NO Sindaci, NO Revisori)	D	corruzione, concussione	13,51
CONTABILITA'	**Tenuta contabilità, bilancio e chiusura**	E	falso, errore, elusione regole TUIR, IVA, Irap, II.II, e procedure MOG	12,96
GEST. SMALTIMENTO RIFIUTI	**Smaltimento rifiuti degli uffici (toner, convenzione; neon NO)**	D	corruzione, falso	12,64
PERSONALE DIPENDENTE	**Selezione e gestione del personale**	A	corruzione	8,24
	Reclutamento del personale	A	corruzione	8,07
	Progressioni di carriera	A	corruzione	7,89
	Conferimento di incarichi di collaborazione	A	corruzione	8,07
Affidamento di lavori, servizi e forniture:	**Acquisto generico di materiale**	B	corruzione	11,68
SPONSORIZZIONI	*Gestione attività di sponsorizzazione, omaggi, liberalità*	B	corruzione	13,60
CONSULENZE	**Gestione consulenze e prestazioni professionali**	B	corruzione	13,60
Altri acquisti	Altri acquisti di materiale	B	corruzione	11,68
FINANZA E CASSA	**Gestione flussi monetari, finanziari e cassa**	E	elusione regole, autoriciclaggio	12,96

SETTORE o MACRO ATTIVITA'	Processo (attività, azione, atti pareri, "procedimento amministrativo", processo, attività endoprocessuale)	Area a rischio corruzione (PNA)	Rischio reato, condotta irresponsabile o di "maladministration"	Valore finale del "rischio residuo" (range: 1-25)
	Rimborsi spese (anticipate da dipendenti)	D	riciclaggio	12,64
Sicurezza - SSL HSE	**Organiz. luoghi di lavoro e gestione attività lavorative (acquisto dpi e corsi)**	B	infortuni che generano lesioni gravi penali	18,13
	RSPP - salute e sicurezza sul lavoro (RSPP esterno senza, DVR, protocollo sanitario)	C	corruzione e infortuni che generano lesioni gravi penali	12,00
ICT	**Informatica e privacy (sistemi interni)**	D	corruzione, falso, violazione diritto d'autore e/o privacy	18,56
	"E" = altre attività di servizio e gestionali senza rilevanza pubblica			
	"F" = attività gestionali connesse ai controlli			

A fronte dell'analisi effettuata sono state individuate alcune misure idonee a diminuire l'esposizione al rischio di *maladministration*, sia fra quelle prescritte come obbligatorie dal P.N.A, sia ulteriori misure che l'Amministrazione sta già effettuando o che intende attuare nel triennio in esame.

Si specifica che il rischio analizzato, in generale, si è notevolmente ridotto rispetto al monitoraggio del precedente PTPC, poiché sono stati inseriti diversi presidi, codice etico, modello organizzativo 231/01 e nuovi controlli.

La mappatura dei processi allegata al presente Piano Triennale sarà comunque integrata e/o dettagliata, in occasione della variazione dei processi o funzioni aziendali e secondo le indicazioni di ANAC.

MISURE OBBLIGATORIE		
n.	**Ambito**	**Misura**
1	Trasparenza	Osservanza degli obblighi di trasparenza ai sensi del D.Lgs. 33/2013 e della legge 190/2012, di altre normative provinciali e del vigente programma triennale per la trasparenza e l'integrità.
2	Codice di comportamento	Adozione e osservanza del codice di comportamento del personale (divulgazione e formazione ai dipendenti; adeguamento degli atti di incarico e dei contratti alle previsioni del codice; monitoraggio sull'attuazione del codice; vigilanza sul rispetto del codice da parte dei direttori e dei dirigenti).
3	Rotazione del personale	Rotazione periodica del personale dirigenziale e del personale con funzioni di responsabilità di procedimento direttamente coinvolto nelle attività a rischio critico di corruzione. In caso di esigenze organizzative correlate a specifiche professionalità, tale misura può essere integrata o sostituita da un'attenta e scrupolosa rotazione dei procedimenti affidati al personale appartenente ad una stessa struttura o area di competenza. La rotazione non deve comunque tradursi nella sottrazione di competenze professionali specialistiche ad uffici cui sono affidate attività ad elevato contenuto tecnico. Altra misura efficace, in combinazione o alternativa alla rotazione, potrebbe essere quella della distinzione delle competenze (cd. "segregazione delle funzioni") che attribuisce a soggetti diversi i compiti di: • svolgere istruttorie e accertamenti; • adottare decisioni; • attuare le decisioni prese; • effettuare verifiche.
4	Obbligo di astensione	Obbligo di astensione in caso di conflitto di interesse (attuazione di adeguate iniziative di informazione; verifica da parte del dirigente dell'osservanza dell'obbligo nei confronti del personale assegnato).
5	Inconferibilità e incompatibilità per incarichi dirigenziali	Verifica e monitoraggio di situazioni di inconferibilità di incarichi dirigenziali e verifica e monitoraggio del rispetto dell'obbligo di comunicazione di situazioni potenziali di incompatibilità. Adozione di modalità per effettuare i controlli su situazioni di incompatibilità ed eventuali adempimenti conseguenti.
7	Svolgimento di attività successive alla cessazione del rapporto di lavoro (pantouflage; revolving doors)	Verifica e monitoraggio dell'applicazione delle disposizioni previste dall'art. 53 comma 16-ter, del D. Lgs. n. 165/2001
8	Formazione di commissioni, assegnazione agli uffici, conferimento di incarichi dirigenziali in caso di condanna penale per delitti contro la P:A: contro la p.a.	Verifica e monitoraggio dell'applicazione delle disposizioni previste dall'art. 35-bis del D.Lgs. 165/2001
9	Tutela del dipendente che segnala un illecito	Garantire la tutela del dipendente che effettua segnalazioni di illecito (whistleblower).

MISURE OBBLIGATORIE		
n.	**Ambito**	**Misura**
10	Formazione del personale e dei soggetti coinvolti	Individuazione dei dipendenti operanti in aree a elevato/critico rischio di corruzione; programmazione e realizzazione di percorsi formativi generali e differenziati per destinatari
11	Protocolli di legalità o patti di integrità	Predisposizione e adozione di protocolli di legalità o patti di integrità per l'affidamento di commesse (inserimento in avvisi, bandi di gara e lettere di invito della clausola di salvaguardia relativa al rispetto del protocollo di legalità o del patto di integrità)
12	Monitoraggio del rispetto dei termini per la conclusione dei procedimenti	Realizzazione di un sistema di monitoraggio efficiente del rispetto dei termini, previsti dalla legge o dai regolamenti, per la conclusione dei procedimenti.
13	Monitoraggio sullo stato di attuazione del Piano	Controllo sull'implementazione delle misure previste nel Piano da parte dei soggetti coinvolti.

Misure di prevenzione facoltative ulteriori

Il P.N.A. stabilisce che le misure obbligatorie per trattare il rischio siano accompagnate eventualmente da misure ulteriori, ritenute parimenti necessarie o utili.

Nel caso di specie, a seguito del completamento della mappatura del rischio è emersa una carenza in materia di controlli sui fornitori in merito alla presenza del loro rispettivo MOG 231/01 o di altri indici di legalità (o vero e proprio **rating di legalità)**; del pari, è emersa la mancanza di un sistema di calcolo delle performance (MBO o *balanced scorecard*) che per i dirigenti includa anche indicatori connessi al miglioramento della rischiosità dei processi in ottica di diminuzione del rischio di *maladministration*.

Per questo motivo è stato ritenuto utile inserire nella programmazione alcune misure ulteriori, volte a migliorare l'organizzazione. In particolare, si è valutato di inserire:

- Richiesta ai fornitori del loro MOG 231/01 o rating di legalità, specie per quanto attiene a fornitori di servizi a rischio salute o sicurezza nel luogo di lavoro.
- Collegamento dell'anticorruzione al sistema delle performance dei dirigenti.
- Monitoraggio del contenzioso.
- Migliore esaustività dei criteri di scelta degli affidatari;
- Intensificazione delle verifiche sulle dichiarazioni sostitutive ai sensi del DPR n. 445/2000, anche attraverso eventuali stipule di convenzioni per l'accesso alle banche dati.

Procedura di segnalazione e meccanismi di tutela con protezione dell'anonimato (c.d. *Whistleblowing*)

INFOSYN ritiene che, per poter dare efficace e concreta attuazione alle disposizioni del legislatore e alla *ratio* sottesa alla normativa anti-corruzione, sia necessaria l'istituzione di una procedura che consenta -attraverso una regolamentazione specifica- la gestione del processo di ricezione, analisi e trattamento delle segnalazioni inviate o trasmesse, anche in forma confidenziale o anonima.

Il contrasto alla corruzione in termini preventivi può essere infatti affrontato sotto diversi aspetti. Tra questi le segnalazioni assumono grande rilevanza. Esse non solo consentono un'efficace repressione, ma manifestano soprattutto un coinvolgimento eticamente corretto e un'impostazione culturale che costituisce essa stessa il primo deterrente al fenomeno corruttivo. Si pone particolare attenzione al c.d. **whistleblowing**, che è definito come "la denuncia da parte di membri (passati o attuali) di un'organizzazione di pratiche illegali, immorali o illegittime sotto il controllo dei loro datori di lavoro, individui o organizzazioni che hanno la facoltà di agire in merito". Esso costituisce

un sistema di segnalazione già presente nel mondo anglosassone e introdotto, senza non poche critiche, nell'ordinamento giuridico nazionale.

Ispirandosi alle disposizioni ANAC del 2015 e, ancor prima, all'articolo 33 della Convenzione di Merida contro la corruzione e in attuazione dell'articolo 9 della Convenzione Civile sulla corruzione, la legge n. 190/2012 ha infatti introdotto nel D.lgs. n. 165/2001 l'articolo 54 bis, di cui si riporta il testo per opportuna diffusione:

1. *Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per 1. lo stesso titolo ai sensi dell'articolo 2043 del codice civile, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia.*
2. *Nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato.*
3. *L'adozione di misure discriminatorie è segnalata al dipartimento della funzione pubblica, per i provvedimenti di competenza, dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere.*
4. *La denuncia è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7.08.1990, n.241, e successive modificazioni.*

Peraltro si segnala che INFOSYN, già prima delle disposizioni ANAC del 2015 (specifiche in materia di *whistleblowing)* ha adottato una procedura e una modulistica per poter consentire l'esercizio di tale diritto, oltre ad aver somministrato ai dipendenti una formazione specifica in materia.

Nella procedura sono identificati:

- le tipologie di segnalazioni ricevibili;
- canali di comunicazione utilizzabili per la trasmissione della segnalazione, anche da parte dei superiori gerarchici a cui il dipendente si è rivolto in prima istanza;
- meccanismi di tutela dell'anonimato per il segnalatore;
- le attività istruttorie (verifica preliminare, accertamento, audit, monitoraggio azioni correttive);
- archiviazione e conservazione della documentazione, tracciabilità;
- modalità di trattamento dei dati personali ai fini del D.lgs n. 196/2003;
- l'organo con responsabilità e potere di ricevere ed esaminare le denunce e/o indagini improprie.

INFOSYN coglie l'occasione dell'adozione del presente Piano per ricordare ai dipendenti e amministratori il diritto/dovere di denunciare o riferire, in buona fede e sulla base di ragionevoli motivazioni, azioni e/o omissioni illecite o irregolarità di cui si è a conoscenza nelle attività della pubblica amministrazione.

Trasparenza

La trasparenza, intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, costituisce un fondamentale mezzo di prevenzione della corruzione; il suo perseguimento impone infatti forme diffuse di controllo sul raggiungimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, limitando quindi il rischio che si realizzi una corruzione sistemica. Nel D.lgs. n. 33/2013 e ss.mm.ii. il legislatore ha introdotto l'obbligo per ogni pubblica amministrazione di dotarsi di un Programma Triennale per la trasparenza e l'integrità, integrato nel piano anticorruzione e nel MOG 231/01, nel quale definire le misure, i modi e le iniziative volti all'attuazione degli obblighi di pubblicazione previsti dalla normativa vigente.

La legge regionale Trentino Alto Adige n. 10/2014, modificata dalla legge regionale 16/2016 che ha recepito il d. 97/2016, peraltro, determinano specificità e semplificazioni amministrative locali, sebbene resta sottesa la *ratio* del programma sulla trasparenza.

Il responsabile per la trasparenza (e anticorruzione) svolge stabilmente un'attività di controllo sull'adempimento degli obblighi di pubblicazione da parte dell'amministrazione, da caricare *on line* sul sito internet istituzionale, assicurandone la completezza, la chiarezza e l'aggiornamento, nonché segnalando all'organo di indirizzo politico, all'OdV 231/01, all'Autorità nazionale anticorruzione i casi di mancato o ritardato adempimento degli obblighi di pubblicazione.

La scelta di unificare in un unico soggetto le competenze delle figure di responsabile trasparenza e anticorruzione deriva nelle recenti disposizioni normative e interpretative di ANAC.

Si segnala, infine, che INFOSYN sta procedendo, nelle more dell'elaborazione delle modifiche documentali derivanti dalla norma nazionale e regionale, alla riorganizzazione del proprio sito internet istituzionale (sezione "amministrazione trasparente").

Nelle pagine precedenti sono state indicate le figure responsabili dei flussi informativi in ambito trasparenza.

Di seguito viene riportato un piano di audit e programmatico in ambito anti-maladministration e trasparenza.

2017

16.01.2016	Pubblicazione della relazione annuale anticorruzione del RPCT
31.01.2017	Adozione da parte del consiglio di amministrazione del MOG integrato col previgente Piano Triennale di prevenzione della corruzione e Piano triennale trasparenza e Integrità e pubblicazione.
12.01.2017	I dirigenti/responsabili dei processi comunicano al responsabile della prevenzione i procedimenti amministrativi conclusi dopo i termini previsti dalla legge o da disposizioni regolamentari specifiche. Gli stessi devono altresì segnalare situazioni di conflitto e/o ricorsi giurisdizionali relativi all'adempimento degli obblighi di trasparenza e al rispetto del principio di imparzialità.
31.03.2017	I dirigenti/responsabili dei processi trasmettono al responsabile della prevenzione e trasparenza (RPCT) un elenco contenente i nominativi di soggetti con i quali sono stati stipulati contratti o che sono stati interessati da procedimenti di autorizzazione, concessione o erogazione di vantaggi economici di qualunque genere, con la specifica indicazione di eventuali rapporti di parentela, coniugio o affinità sussistente tra i medesimi e i titolari /soci (Sindaci e/o altri consiglieri comunali dei comuni consorziati), gli amministratori, e i dipendenti dei medesimi.
31.03.2017	RPCT individua amministratori/dipendenti/dirigenti che devono seguire specifici **corsi di formazione**.
15.12.2017	Il responsabile della prevenzione della corruzione promuove l'avvio delle procedure di eventuale rotazione del personale
31.12.2017	Il responsabile della prevenzione della corruzione predispone una relazione annuale contenente i risultati dell'attività svolta, da pubblicare nella sezione del **sito web** della società dedicata alla Prevenzione della Corruzione.

2018

31.01.2018	Controllo del risk assessment per la prevenzione della corruzione, per l'adozione di eventuali nuovi modelli da parte del consiglio di amministrazione.
31.01.2018	I dirigenti comunicano al responsabile della prevenzione i procedimenti amministrativi conclusi dopo i termini previsti dalla legge o da disposizioni regolamentari specifiche. Gli stessi devono altresì segnalare situazioni di conflitto e/o ricorsi giurisdizionali relativi all'adempimento degli obblighi di trasparenza e al rispetto del principio di imparzialità.
31.01.2018	Approvazione da parte del consiglio di amministrazione del MOG integrato con le misure di prevenzione della corruzione e trasparenza e sua pubblicazione *on line*.
31.03.2018	Il responsabile della prevenzione della corruzione, individua i dipendenti che dovranno seguire specifici **corsi di formazione**.
31.03.2018	I dirigenti/**responsabili dei processi** trasmettono al responsabile della prevenzione un elenco contenente i nominativi di soggetti con i quali sono stati stipulati **contratti** o che sono stati interessati da procedimenti di autorizzazione, concessione o erogazione di vantaggi economici di qualunque genere, con la specifica indicazione di eventuali rapporti di parentela, coniugio o affinità sussistente tra i medesimi e i titolari /soci (Sindaci e/o altri consiglieri comunali dei comuni consorziati), gli amministratori, e i dipendenti dei medesimi.
30.09.2018	RPCT pubblica, nella sezione del sito internet dedicata alla prevenzione della corruzione, i risultati delle operazioni di consultazioni via web per la predisposizione delle misure anticorruzione.
15.12.2018	Conclusione operazioni di rimappatura dei processi.
15.12.2018	Conclusione operazioni di consultazione per eventuale rotazione del personale
31.12.2018	PRPCT predispone una relazione contenente i risultati dell'attività svolta, da pubblicare nella sezione del **sito web** della società dedicata alla Prevenzione della Corruzione.

2019

31.01.2019	Controllo del risk assessment per la prevenzione della corruzione, per l'adozione di eventuali nuovi modelli da parte del consiglio di amministrazione.
31.01.2019	I dirigenti comunicano al responsabile della prevenzione i procedimenti amministrativi conclusi dopo i termini previsti dalla legge o da disposizioni regolamentari specifiche. Gli stessi devono altresì segnalare situazioni di conflitto e/o ricorsi giurisdizionali relativi all'adempimento degli obblighi di trasparenza e al rispetto del principio di imparzialità.
31.01.2019	Approvazione da parte del consiglio di amministrazione del MOG integrato con le misure di prevenzione della corruzione e trasparenza e sua pubblicazione *on line*.
31.03.2018	Il responsabile della prevenzione della corruzione, individua i dipendenti che dovranno seguire specifici **corsi di formazione**.
31.03.2018	I dirigenti/**responsabili dei processi** trasmettono al responsabile della prevenzione un elenco contenente i nominativi di soggetti con i quali sono stati stipulati **contratti** o che sono stati interessati da procedimenti di autorizzazione, concessione o erogazione di vantaggi economici di qualunque genere, con la specifica indicazione di eventuali rapporti di parentela, coniugio o affinità sussistente tra i medesimi e i titolari /soci (Sindaci e/o altri consiglieri comunali dei comuni consorziati), gli amministratori, e i dipendenti dei medesimi.
30.09.2018	RPCT pubblica, nella sezione del sito internet dedicata alla prevenzione della corruzione, i risultati delle operazioni di consultazioni via web per la predisposizione delle misure anticorruzione.
15.12.2018	Conclusione operazioni di rimappatura dei processi.
15.12.2018	Conclusione operazioni di consultazione per eventuale rotazione del personale
31.12.2018	RPCT predispone una relazione contenente i risultati dell'attività svolta, da pubblicare nella sezione del **sito web** della società dedicata alla Prevenzione della Corruzione.

13. Accesso civico semplice, accesso generalizzato e accesso documentale agli atti (L. 241/90)

INFOSYN recepisce le Linee Guida ANAC 2016 in materia di accesso civico semplice e generalizzato.

Accesso civico semplice ex art. 5 c.1. del d. 33/2013 modificato dal d.97/2016: Cfr. Linee guida trasparenza, relative agli obblighi di pubblicazione di cui al D. 33/2013 (modificato da L.R. 10/2014, D.lgs. 97/2016, L.R. 16/2016).

Accesso generalizzato ex art. 5 c.2 del d. 33/2013 modificato dal d.97/2016: Cfr. Linee guida **FOIA**, relative a accessibilità a documenti non obbligatoriamente da pubblicare ai sensi del d. 33/2013, ma che devono essere disponibili su richiesta di utenti, nei limiti della legge oppure documenti ulteriori per i quali è decorso il temine quinquennale di conservazione e pubblicazione obbligatoria *on line*.

Accesso documentale agli atti (L. 241/1990): Linee guida INFOSYN già da tempo presenti (Cfr. regolamento).

***

L'art. 5 del d.lgs. 33/2013, modificato dall'art. 6 del d.lgs. 97/2016 e norme locali L.R. 16/2016 e circolare del 9 gennaio 2017, riconosce a chiunque:

a) il diritto di richiedere alle Amministrazioni documenti, informazioni o dati per i quali è prevista la pubblicazione obbligatoria, nei casi in cui gli stessi non siano stati pubblicati nella sezione "Amministrazione trasparente" del sito web istituzionale (accesso civico "semplice");

b) il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del d.lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis (accesso civico "generalizzato"). Per quest'ultimo tipo di accesso si rinvia alle apposite Linee guida in cui sono date indicazioni anche in ordine alla auspicata pubblicazione del c.d. registro degli accessi (Delibera ANAC n. 1309/2016, § 9).

Per quanto riguarda gli obblighi di pubblicazione normativamente previsti, il legislatore ha confermato l'istituto dell'accesso civico volto ad ottenere la corretta pubblicazione dei dati rilevanti ex lege, da pubblicare all'interno della sezione "Amministrazione trasparente".

Nel nostro Ente INFOSYN la procedura prevede che:

- l'istanza va presentata alla persona Responsabile per la prevenzione della corruzione e la trasparenza (RPCT).
- La RPCT è tenuta a concludere il procedimento di accesso civico con provvedimento espresso e motivato nel termine di trenta giorni.
- Sussistendone i presupposti, RPCT avrà cura di pubblicare sul sito i dati, le informazioni o i documenti richiesti e a comunicare al richiedente l'avvenuta pubblicazione dello stesso, indicandogli il relativo collegamento ipertestuale. Nonostante la norma non menzioni più il possibile ricorso al titolare del potere sostitutivo, da una lettura sistematica delle norme, l'Autorità ritiene possa applicarsi l'istituto generale previsto dall'art. 2, co. 9-bis, della l. 241/90.
- In caso di ritardo o mancata risposta o diniego da parte del RPCT il richiedente può ricorrere al titolare del potere sostitutivo che conclude il procedimento di accesso civico come sopra specificato, entro i termini di cui all'art. 2, co. 9-ter della l. 241/1990.

- A fronte dell'inerzia da parte del RPCT o del titolare del potere sostitutivo, il richiedente, ai fini della tutela del proprio diritto, può proporre ricorso al Tribunale amministrativo regionale ai sensi dell'art. 116 del decreto legislativo 2 luglio 2010, n. 104.

INFOSYN ha pubblicato, nella sezione "Amministrazione trasparente", nella sottosezione denominata "Altri contenuti"/"Accesso civico" gli indirizzi di posta elettronica cui inoltrare le richieste di accesso civico e di attivazione del potere sostitutivo.

***

Si specifica che alla data odierna (23 gennaio 2016) società partecipate anche indirettamente quali INFOSYN e altre piccole società partecipate dalla PA sono in attesa di ulteriori linee guida, come indicato da ANAC stessa, con atto di indirizzo e linea guida modificativa della determinazione ANAC n. 8/2015.

INFOSYN peraltro segue la Circolare della regione Autonoma Trentino Alto Adige del 9 gennaio 2017 "Modifica alla legge regionale n. 10/2014 in materia di diritto di accesso civico, pubblicità, trasparenza e diffusione di informazioni" che riporta il recepimento del d.97/2016 e della legge regionale 16/2016.

INFOSYN provvederà quanto prima a conformarsi alle Linee Guida ANAC appena disponibili.