



***CONSORZIO per la  
DEPURAZIONE delle  
ACQUE di SCARICO  
del SAVONESE S.p.A.***

**Modello**  
**di organizzazione e di gestione**  
ex Decreto Legislativo 8 giugno 2001, n° 231

**APPROVATO DAL CONSIGLIO DI GESTIONE  
IN DATA 1° GIUGNO 2016**

Il Presidente del Consiglio di Gestione	<b>Firma</b> 
---	--

## INDICE

Glossario .....	5
1. Il Decreto Legislativo n. 231/2001.....	8
1.1 Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società e associazioni. ....	8
1.2 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente della responsabilità amministrativa. ....	9
2. L'"ambiente di controllo".....	12
2.1 Il contesto aziendale di Consorzio Depurazione del Savonese .....	12
2.2 La struttura organizzativa ed il sistema delle deleghe.....	13
2.3 Il controllo di gestione.....	15
2.4 Il sistema di certificazione ambientale.....	15
2.5 Il sistema informativo.....	16
2.6 Il codice etico.....	16
2.7 Il revisore legale .....	17
2.8 Il Consiglio di Sorveglianza .....	17
2.9 Gli altri elementi dell'ambiente di controllo .....	17
3. Il modello di organizzazione e di gestione di Consorzio Depurazione del Savonese	18
3.1 Gli obiettivi perseguiti dalla società con l'adozione del Modello. ....	18
3.2 La funzione del Modello.....	18
3.3 La struttura del Modello: Parte Generale e Parti Speciali in funzione delle diverse figure di reato. ....	20
3.4 L'adozione del Modello.....	23
3.5 L'identificazione la composizione dell'organismo interno di vigilanza.....	23
3.6 Le funzioni e i poteri dell'organismo interno di vigilanza. ....	24
3.7 I flussi informativi agli organi societari.....	25
3.8 I flussi informativi verso l' <i>Organismo di Vigilanza</i> . ....	26
3.9 La raccolta e conservazione delle informazioni. ....	27
4. La diffusione della conoscenza del Modello. ....	28
4.1 La formazione del personale. ....	28
4.2 L'informativa a Collaboratori esterni e Partner. ....	29
5. Il sistema disciplinare. ....	30
5.1 La funzione del sistema disciplinare.....	30
5.2 Le misure nei confronti dei lavoratori dipendenti. ....	30
5.3 Le misure nei confronti dei dirigenti, del Presidente e dai componenti del CdG e organi di controllo. ....	31
5.4 Le misure nei confronti di Collaboratori esterni e Partner.....	32
6. Le verifiche sull'adeguatezza del Modello. ....	33
PARTE SPECIALE I - Reati nei rapporti con la Pubblica Amministrazione.....	34
1 Destinatari della "Parte Speciale I". ....	35

2.	I reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001).	36
3.	Processi “sensibili” della Consorzio Depurazione del Savonese nei rapporti con la Pubblica Amministrazione.	43
4.	Procedure adottate.	45
4.1	Il sistema procedurale	45
4.2	Principi generali di comportamento.	46
4.3	Procedure specifiche generalmente applicabili.	47
4.4	Elementi fondamentali del processo decisionale.	48
5.	I controlli dell’ODV	49
PARTE SPECIALE II - Reati Societari		50
1.	Destinatari della “Parte Speciale - II”	51
2.	I reati societari (art. 25 <i>ter</i> del D.Lgs. 231/2001)	52
3.	Processi “sensibili” della Consorzio Depurazione del Savonese nell’ambito dei reati societari	58
4.	Procedure adottate	59
4.1	Il sistema procedurale	59
4.2	Principi generali di comportamento	59
4.3.	Procedure specifiche generalmente applicabili	61
5.	I controlli dell’ODV	63
PARTE SPECIALE III - Omicidio colposo e lesioni gravi o gravissime, commessi in violazione delle norme anti-infortunistiche e sulla tutela dell’igiene e della salute sul lavoro		64
1.	Destinatari della “Parte Speciale - III”	65
2.	I reati relativi alla tutela della salute e sicurezza nei luoghi di lavoro (art. 25 <i>septies</i> del D. Lgs. 231/01)	67
	<i>Delitti di omicidio colposo e di lesioni colpose gravi o gravissime, conseguenti a violazione delle norme in tema di salute e sicurezza nei luoghi di lavoro.</i>	69
3.	Processi sensibili e definizione del modello di organizzazione ex art. 30 D.Lgs. 81/08.	72
3.1	Il sistema procedurali	73
3.2	Il Responsabile	74
4.	I controlli dell’ODV	76
PARTE SPECIALE IV - Reati ambientali di cui all’ art. 25 undecies del D.Lgs. 231/01		77
1.	Destinatari della “Parte Speciale IV”	78
2.	I reati ambientali (art. 25 undecies del D.Lgs. 231/01).	79
3.	Processi “sensibili” della Consorzio Depurazione del Savonese nell’ambito dei reati ambientali.	85
3.1	Principi generali di comportamento.	87
4.	Procedure adottate	88
4.1	Il sistema procedurale	88

5. Flussi di comunicazione e sistema disciplinare .....	90
6. I controlli dell'ODV.....	91
PARTE SPECIALE V - REATI INFORMATICI .....	92
1. Destinatari della "Parte Speciale VI" .....	93
2. I reati relativi ai delitti informatici e trattamento illecito di dati introdotti dell'art. 24-bis del decreto legislativo 231/01 e dei delitti in violazione del diritto d'autore introdotti dall' art. 25-nonies del decreto legislativo 231/01 .....	94
3. Processi sensibili della Consorzio Depurazione del Savonese per i delitti informatici	106
3.1 Aree a Rischio .....	106
3.2 Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001 .....	106
4. Procedure adottate.....	107
4.1 Il sistema procedurale.....	107
4.2 Principi generali di comportamento .....	112
4.3 Le procedure specifiche generalmente applicabili .....	114
5. I controlli dell'ODV .....	118

## Glossario

- *“as-is analysis”*: processo di identificazione delle procedure e attività aziendali che possono condurre alla commissione di reati tutelati dal D.Lgs.231/2001;
- *“CCNL”*: Contratto Collettivo Nazionale di Lavoro del Settore Gas e Acqua;
- *“Codice etico”*: codice etico adottato da Consorzio Depurazione del Savonese;
- *“Organismo di Vigilanza”* o *“ODV”*: organismo interno preposto alla vigilanza sul funzionamento e sull’osservanza del Modello e al relativo aggiornamento;
- *“consulenti”*: coloro che agiscono in nome e/o per conto della società sulla base di un mandato o di altro rapporto di collaborazione;
- *“corporate governance”*: le regole di direzione e controllo della società;
- *“D.Lgs.231/2001”*: il decreto legislativo n. 231 dell’8 giugno 2001 e successive modifiche;
- *“gap analysis”*: processo di identificazione delle azioni di miglioramento del sistema di controllo interno preventivo;
- *“consiglio di gestione”* (CdG): organo gestorio nel modello dualistico adottato dall’impresa;
- *“consiglio di sorveglianza”*: organo deputato al controllo sull’amministrazione nel modello dualistico;
- *“operazione sensibile”*: operazione ritenuta a rischio di commissione di reati tutelati dal D.Lgs.231/2001;
- *“processi sensibili”*: procedure e attività aziendali che possono condurre alla commissione di reati tutelati dal D.Lgs.231/2001;
- *“P.A.”*: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio;
- *“partner”*: controparti contrattuali della società, quali ad es. fornitori, clienti, sia persone fisiche sia persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (acquisto e cessione di beni e servizi, associazione temporanea d’impresa - ATI, joint venture, consorzi, etc.), ove destinata a cooperare con l’azienda nell’ambito dei processi sensibili;
- *“reati”*: i reati ai quali si applica la disciplina prevista dal D.Lgs. 231/2001 (anche eventualmente integrato in futuro);

- "*stakeholders*": i soggetti portatori di interessi nei confronti della società.

## **PARTE GENERALE**

- tale reato sia stato commesso intenzionalmente nell'interesse o a vantaggio dell'ente;
- l'autore del reato sia un soggetto in posizione cosiddetta "apicale" (1) o sia un soggetto cosiddetto "sottoposto" (2).

Ne consegue che la condizione che il reato sia commesso nell'interesse o a vantaggio dell'ente consente di escludere la responsabilità della società nei casi in cui il reato sia stato commesso esclusivamente al fine di perseguire un interesse personale, ovvero il soggetto abbia commesso il reato nell'esclusivo interesse proprio o di terzi.

La norma, prevedendo la responsabilità nel caso di reato commesso da un soggetto in posizione apicale, ha posto l'attenzione sulla situazione di fatto e non sull'aspetto puramente formale, lasciando all'interprete, caso per caso, la verifica della necessaria autonomia decisionale che caratterizza un soggetto in posizione apicale.

## **1.2 L'adozione del "Modello di Organizzazione e di Gestione" quale possibile esimente della responsabilità amministrativa.**

L'art. 6 del D.Lgs 231/2001 qualora l'azienda dimostri di aver adottato con adeguata efficacia un appropriato modello di organizzazione, gestione e controllo ritenuto in grado di prevenire e contrastare la manifestazione degli illeciti penali in precedenza elencati, esonera l'ente, sotto determinate condizioni, dalla responsabilità e dalle relative sanzioni pecuniarie ed interdittive.

Il modello deve consentire di:

- individuare le attività che possono condurre alla commissione dei reati tutelati dalla norma;
- prevedere istruzioni specifiche finalizzate a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- individuare un organismo a cui affidare il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento onde così consentire il costante mantenimento delle caratteristiche di adeguatezza del modello stesso;

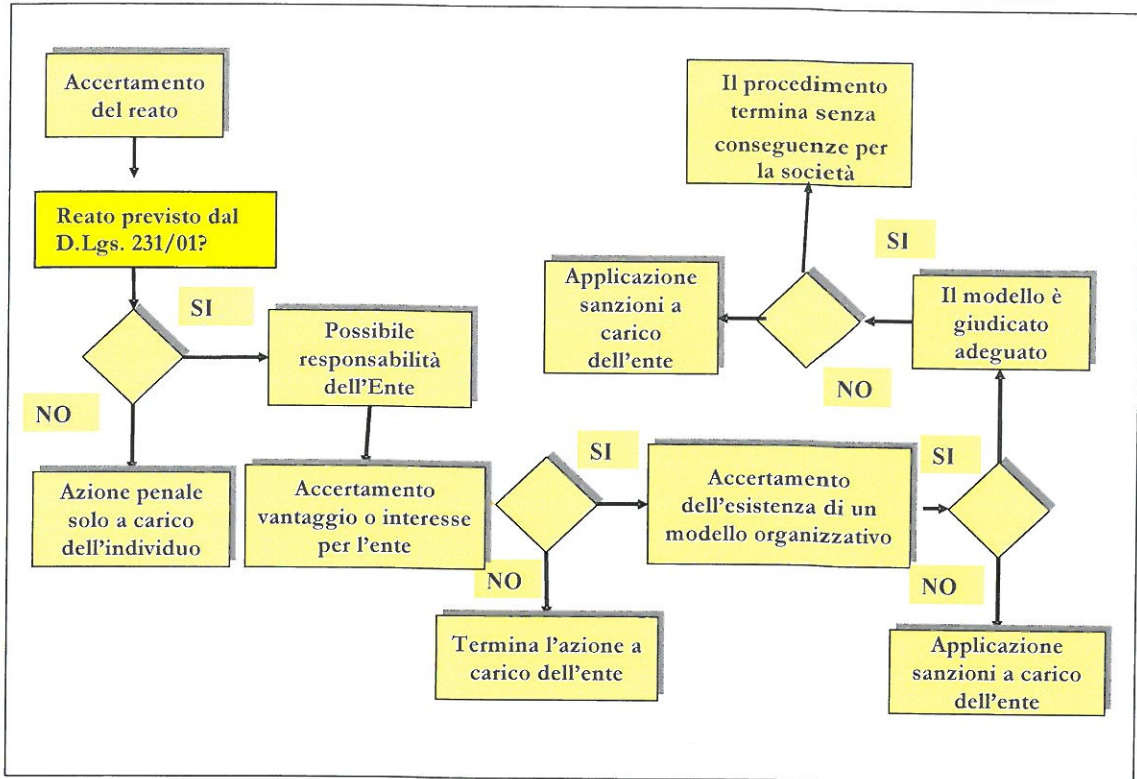
---

<sup>1</sup> I soggetti considerati in posizione apicale sono rappresentati, secondo quanto previsto dall'art. 5 lettera a) del Decreto, da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso".

<sup>2</sup> Per soggetti sottoposti la norma, all'art. 5 lettera b) del Decreto, indica le "persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)".

- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

FIGURA 1: IL MODELLO ORGANIZZATIVO E LA RESPONSABILITÀ AMMINISTRATIVA DELL'ENTE.



Il legislatore, nel disciplinare il modello “di salvaguardia” che consente di escludere le sanzioni conseguenti ad un eventuale reato, fa riferimento, in linea generale, all’insieme di criteri utilizzati per definire i tratti essenziali di un adeguato sistema di “controllo interno” che viene così ad assumere il ruolo centrale nel sistema in grado di prevenire e gestire il “rischi di reato” insite in ogni area funzionale in cui si articola l’azienda. In sostanza, l’azienda deve valutare compiutamente il proprio sistema organizzativo ed il proprio sistema di controllo interno.

L’adozione del modello di organizzazione, gestione e controllo è facoltativa e non obbligatoria. L’eventuale mancata adozione non è soggetta, di conseguenza, ad alcuna sanzione, ma espone l’ente alla responsabilità per gli illeciti realizzati dal Presidente e dai componenti del CdG e dipendenti.

L’adozione del modello diviene essenziale per poter beneficiare di tale sorta di “scudo”.

Tra gli obiettivi generali del sistema di controllo interno vi è, infatti, il rispetto di norme e regolamenti. Per quanto non assoluta, la “ragionevole certezza” che

deve essere garantita dai sistemi di controllo interno si basa su un “disegno architettonico” che si dimostri coerente e solido nel corso del tempo.

“Ragionevole certezza” significa che il giudice, a fatti avvenuti ex post, può essere chiamato a decidere quanto affidabile fosse il sistema in essere e quanto efficace sia stata l’azione di verifica attuata dagli organismi preposti.

L’adozione di metodologie e standard di svolgimento dell’attività può costituire un importante elemento oggettivo su cui basare i giudizi e le valutazioni. La norma si limita, peraltro, ad indicare solo alcune delle caratteristiche essenziali.

A tal fine, la norma (art. 6, comma 3, D.Lgs. 231/2001) indica che “i modelli di organizzazione possono essere adottati (...) sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti”.

La redazione dei modelli organizzativi in conformità alle indicazioni di tali codici conferisce a tale Modello soltanto in astratto le caratteristiche di idoneità, poiché l’ente, affinché tale Modello sia giudicato idoneo, deve essere in grado di dimostrare non soltanto la sua adozione, ma anche l’attuazione e l’idoneità in relazione alle caratteristiche specifiche della società.

L’ente può essere esonerato dalla responsabilità conseguente alla commissione dei reati indicati, secondo quanto richiesto dalla norma, se l’organo dirigente ha, fra l’altro:

- adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l’osservanza del modello e di curarne l’aggiornamento ad un organismo dell’ente dotato di autonomi poteri di iniziativa e controllo.

L’affidamento di detti compiti a tale Organo e, ovviamente, il corretto ed efficace svolgimento degli stessi sono, dunque, presupposti indispensabili per l’esonero dalla responsabilità.

L’efficace attuazione del Modello richiede, oltre all’istituzione di un sistema disciplinare, una sua verifica periodica da parte dell’organo a ciò deputato.

## 2. L'“ambiente di controllo”.

Il sistema di controllo interno, nella prassi internazionale, è definito come:

*“l'insieme dei processi attuati dal Consiglio di gestione, dal management e dal personale di una organizzazione, finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi rientranti nelle seguenti categorie:*

- *efficacia ed efficienza delle attività operative;*
- *attendibilità delle informazioni contabili ed extracontabili, sia per i terzi, sia a fini interni;*
- *conformità alle leggi, ai regolamenti, alle norme e alle politiche interne”.*

Il sistema di controllo interno aziendale può essere analizzato distinguendo tra elementi:

- *di “struttura”, costituiti dal contesto in cui opera il sistema di controllo interno;*
- *di “processo”, ovvero la “componente attuativa” del sistema di controllo interno, costituita dalle attività che devono essere svolte: l'identificazione e valutazione dei rischi, la definizione delle attività di controllo ed il monitoraggio.*

L'ambiente di controllo:

- *rappresenta il principale elemento di struttura poiché costituisce il contesto all'interno del quale il sistema di controllo viene progettato e successivamente monitorato;*
- *deriva dalle scelte compiute dall'alta direzione in merito alla definizione delle variabili organizzative, come la struttura organizzativa, il sistema informativo, i processi di controllo di gestione ed informativi.*

La struttura organizzativa riguarda gli organi tra cui è suddiviso il lavoro, le funzioni a loro assegnate (direttive, esecutive, l'attribuzione di deleghe, le responsabilità), le relazioni tra i diversi organi (la definizione delle gerarchie, la fissazione dei diversi livelli in cui si compone verticalmente la struttura).

Accanto a tali variabili, definibili “hard”, vi sono poi le situazioni di contesto aziendale che costituiscono variabili “soft”, come lo stile della direzione e la sensibilità al controllo diffusa all'interno dell'impresa.

### 2.1 Il contesto aziendale di Consorzio Depurazione del Savonese

Nella predisposizione del presente Modello si è tenuto conto dell'“ambiente di controllo” della Consorzio Depurazione del Savonese, costituito dall'insieme delle

procedure e dei sistemi di controllo operanti in azienda, ove giudicati idonei a valere anche come misure di prevenzione dei Reati e controllo sui Processi Sensibili.

Nell'indagare l'ambiente di controllo in Consorzio Depurazione del Savonese è stato esaminato il ruolo dei seguenti elementi:

- *il sistema di governance;*
- *la struttura organizzativa ed il sistema delle deleghe e delle procedure;*
- *il controllo di gestione;*
- *la certificazione ambientale;*
- *il sistema informativo;*
- *il codice etico;*
- *la revisione legale;*
- *gli altri elementi dell'ambiente di controllo;*
- *il sistema di anticorruzione e di gestione della trasparenza.*

## **2.2 Il sistema di governance**

Il sistema di governance del Consorzio si basa su un modello dualistico, i cui organi sono, ai sensi dell'art. 11 dello Statuto, i seguenti:

- Assemblea dei soci;
- Consiglio di Gestione;
- Consiglio di sorveglianza;
- Revisore contabile.

I poteri dell'Assemblea sono previsti dall'art. 16, inoltre, come caso specifico, si richiama anche l'art. 23 che, a rafforzamento del sistema di amministrazione e controllo della società, prevede il controllo "analogo" in ottemperanza alla normativa comunitaria che dispone le seguenti prerogative attribuite in capo alla stessa Assemblea dei soci:

- approvazione di particolari atti di gestione (previsti dall'art. 16, comma 1, lettera e) ed f), tra cui il preventivo annuale disciplinato all'art. 20 comma 3 dello Statuto);
- nomina diretta dei componenti del Consiglio di Gestione e del Consiglio di Sorveglianza secondo le modalità previste dallo Statuto (art. 16, comma 1, lettera a);
- ai Comuni soci è riservato il controllo sulle modalità di erogazione dei servizi e la verifica degli standard qualitativi e quantitativi degli stessi nonché dei livelli tariffari praticati.

Il Consiglio di gestione si occupa dell'amministrazione dell'impresa e quindi del compimento delle operazioni necessarie all'attuazione dell'oggetto sociale, come previsto dall'art. 20 dello Statuto (poteri).

Il Consiglio di Sorveglianza svolge funzioni di controllo che possono essere assimilate a quelle esercitate dal Collegio Sindacale e detiene inoltre alcuni poteri che nel sistema tradizionale sono attribuiti all'Assemblea dei Soci, nonché poteri inerenti alla definizione dei piani strategici aziendali, che nello specifico sono disciplinati dall'art. 25 dello Statuto.

Il controllo contabile è attribuito al revisore come previsto dall'art. 29 dello Statuto.

### **2.3 La struttura organizzativa ed il sistema delle deleghe.**

In particolare, in merito alla Governance, per il sistema di amministrazione e controllo è stato adottato il modello dualistico delle società per azioni, gestite da un Consiglio di Gestione, con l'attività di controllo affidata al Consiglio di Sorveglianza, ed il controllo contabile esercitato da un revisore legale iscritto nell'apposito albo.

Inoltre, con riferimento all'analisi della struttura organizzativa sono emersi elementi che rafforzano l'ambiente di controllo quali:

- *la disponibilità dell'organigramma aziendale aggiornato;*
- *la presenza di un sistema di controllo di gestione;*
- *la fissazione di un sistema delle deleghe chiaro ed articolato che mette in evidenza le responsabilità, i poteri autorizzativi e di firma;*
- *la disponibilità di documenti che guidano e vincolano i diversi soggetti nello svolgimento dei processi aziendali: i comunicati e le comunicazioni organizzative e le procedure.*

Le disposizioni di origine interna derivano da:

- *provvedimenti del Consiglio di Gestione;*
- *comunicati e comunicazioni organizzative.*

I "provvedimenti del Consiglio di Gestione" hanno natura di disposizioni che impegnano l'azienda verso parti terze. In particolare, i provvedimenti del C.d.G. riguardano la definizione di rapporti con il personale.

I "comunicati e le comunicazioni organizzative" hanno natura di disposizioni e informazioni al personale aziendale su procedure tecniche, gestionali e organizzative. In caso di coinvolgimento diretto dei Dirigenti, i comunicati e le comunicazioni organizzative sono firmati dal Presidente.

## **2.4 Il controllo di gestione.**

I diversi livelli gerarchici aziendali sono stati responsabilizzati attraverso il sistema di controllo di gestione che si propone di attuare un'attività di monitoraggio delle responsabilità in ordine al conseguimento degli obiettivi singolarmente definiti e finalizzati, nel loro complesso, a garantire il miglioramento dell'efficienza e la valorizzazione dei risultati.

In particolare, compongono elementi del controllo di gestione i seguenti:

- *il sistema di controllo contabile finalizzato all'unbundling (apposito applicativo) conforme alle disposizioni dell'Autorità per l'energia elettrica il gas ed il sistema idrico;*
- *il sistema di controllo degli investimenti (personalizzazione del sistema gestionale);*
- *il sistema di reporting trimestrale rivolto agli azionisti per l'esercizio del "controllo analogo" (residente sul gestionale).*

Tale sistema prevede una metodologia di controllo articolata in aree funzionali e la redazione di un budget in relazione alla tipologia di attività che il Consorzio Depurazione del Savonese svolge.

## **2.5 Il sistema di certificazione ambientale.**

Il Consorzio ha istituito nella propria organizzazione un Sistema di Gestione Ambientale dando pari importanza agli aspetti di sicurezza, qualità ed ambiente, senza peraltro venire meno agli obiettivi di flessibilità e reattività e di massima soddisfazione per il cliente che sono irrinunciabili per l'azienda.

Nell'insieme delle sue attività il Consorzio per la Depurazione delle Acque di Scarico del Savonese si impegna quindi a:

1. Promuovere il rispetto e la tutela di tutte le risorse naturali e del mare in particolare.
2. Svolgere tutte le attività, prevenendo ogni forma di inquinamento e in assoluto rispetto della legislazione ambientale di riferimento, nonché di tutte le altre regolamentazioni ambientali sottoscritte dall'azienda.
3. Stabilire obiettivi e traguardi di miglioramento continuo delle proprie prestazioni ambientali nel rispetto delle esigenze delle parti interessate.
4. Migliorare la formazione e la cultura ambientale di tutto il personale.
5. Intraprendere le disposizioni necessarie per far sì che la protezione ambientale costituisca parte integrante della nostra cultura comune.
6. Promuovere la protezione ambientale tramite formazione, comunicazione e condizioni di lavoro che corrispondano agli obiettivi dell'azienda in termini di ambiente.

7. Informare adeguatamente i Comuni e tutte le altre parti interessate circa la politica, gli obiettivi e traguardi di miglioramento, nonché le prestazioni ambientali dell'azienda.

8. Svolgere la depurazione e le attività complementari in conformità alla protezione ambientale, promuovendo un'efficace politica della prevenzione e della protezione che si traducano in un incremento della produttività ed in un risparmio dei costi.

9. Intraprendere tutte le attività necessarie per il mantenimento della qualità e della continuità della depurazione, con particolare attenzione al periodo interessato dalla balneazione.

10. Realizzare la depurazione dei reflui o rifiuti liquidi dell'ambito territoriale che l'impianto è in grado di servire, salvaguardando la compatibilità con la qualità della portata in uscita.

11. Impegnarsi nella gestione o nel miglioramento di ulteriori opere connesse al sistema principale, che richiedono lo stesso tipo di tecniche, impianti e risorse impiegati nell'attività.

## **2.6 Il sistema informativo.**

Tra i diversi elementi che costituiscono l'ambiente di controllo il sistema informativo costituisce un elemento che incide sul sistema di controllo interno.

Il sistema informativo utilizzato dall'impresa è un sistema informativo "legacy" che consente di gestire i processi registrando le operazioni in tempo reale e di automatizzare una serie di operazioni nell'ambiente informatico.

L'area sistemi informativi si è dotata di specifiche procedure per gestire i rischi derivanti dalla commissione di reati informatici, che sono identificati nella Parte Speciale a cui si rinvia.

## **2.7 Il codice etico.**

Lo stile di direzione o stile di leadership rappresenta il modo in cui, ai diversi livelli della struttura gerarchica, i capi si relazionano nei confronti dei subordinati. Si tratta di una sorta di "codice di conduzione" che, per quanto possibile, dovrebbe trascendere le caratteristiche personali, in modo da costituire un vera e propria variabile organizzativa di supporto al corretto funzionamento dell'organizzazione.

L'efficacia del sistema di controllo interno dipende dall'integrità e dai valori etici delle persone che operano nell'organizzazione e certamente di coloro che amministrano ed effettuano il monitoraggio dei controlli.

Conseguentemente in questo contesto assume particolare importanza l'adozione, da parte della Consorzio Depurazione del Savonese, del codice etico,

approvato dal Consiglio di gestione e reso pubblico su internet, che costituisce un elemento essenziale al fine della definizione di un adeguato modello di controllo ex D.Lgs. 231/2001.

## **2.8 Il revisore legale**

Il revisore legale è nominato dagli azionisti riuniti in Assemblea ordinaria.

## **2.9 Il Consiglio di Sorveglianza**

La società ha adottato il modello dualistico nel quale il controllo amministrativo è esercitato dal Consiglio di Sorveglianza.

## **2.10 Gli altri elementi dell'ambiente di controllo**

La Consorzio Depurazione del Savonese ha identificato al proprio interno alcune figure chiave nell'ambito del rispetto delle leggi e dei regolamenti precedenti al D.Lgs, 231/01 che rafforzano l'ambiente di controllo alla base del modello organizzativo.

Nello specifico, la società ha identificato le figure richieste per il rispetto della normativa sulla sicurezza sul lavoro; per quanto riguarda i meccanismi operativi si rinvia alla parte speciale di riferimento.

Inoltre, la società in quanto ente pubblico si è dotata di procedure relative all'anticorruzione e trasparenza che sono pubblicate sul sito e rafforzano il sistema di controllo interno.

## **2.11 Il sistema di anticorruzione e di gestione della trasparenza**

Stante la tipicità della società consortile partecipata esclusivamente da Enti pubblici il sistema di anticorruzione e gestione della trasparenza (coerente con le disposizioni normative e dell'ANAC in materia) rafforza il sistema di controllo della società.

Nello specifico si rinvia al sito aziendale per le disposizione adottate relativamente al sistema di anticorruzione e di gestione trasparente.:

[http://www.depuratore.sv.it/html/amministrazione\\_trasparente.html](http://www.depuratore.sv.it/html/amministrazione_trasparente.html)

### **3. Il modello di organizzazione e di gestione di Consorzio Depurazione del Savonese**

#### **3.1 Gli obiettivi perseguiti dalla società con l'adozione del Modello.**

La società Consorzio Depurazione del Savonese, nell'ambito della propria *corporate governance*, ha ritenuto di ottemperare alle prescrizioni contenute nel D.Lgs. 231/2001, finalizzate a prevenire la commissione di particolari tipologie di reati.

L'attuazione del "Modello di organizzazione e gestione" risponde alla convinzione dell'azienda che ogni elemento utile al fine di ricercare condizioni di correttezza e trasparenza nella gestione delle attività aziendali è meritevole di attenzione sia per l'immagine della società sia per la piena tutela degli interessi degli stakeholders aziendali (individui, istituzioni e consumatori).

In questo senso l'attuazione della norma può essere considerata la continuazione delle politiche aziendali che hanno portato all'introduzione del codice etico.

La scelta di adozione del Modello si ritiene che possa costituire, così come il codice etico ed altri elementi della *governance societaria*, un importante strumento di sensibilizzazione nei confronti di tutti i soggetti che operano per conto del Consorzio Depurazione del Savonese affinché, nell'espletamento delle loro attività, siano indotti a comportamenti ispirati dall'etica della responsabilità e conseguentemente corretti ed in linea con le diverse disposizioni di legge anche oltre ai reati previsti dal Decreto legislativo in oggetto.

Il Modello di seguito esposto detta delle regole e prevede procedure che devono essere rispettate al fine di costituire l'esimente per la società ai fini della responsabilità di cui al D.Lgs. 231/2001 ed intende costituire, più in generale, un miglioramento delle regole di *governance* societaria.

#### **3.2 La funzione del Modello.**

Scopo del Modello è la predisposizione di un sistema strutturato ed organico di procedure e regole, comprendenti attività di controllo (preventive ed ex post), volto a ridurre in maniera consistente il rischio di commissione dei reati contemplati nel Decreto.

In particolare, mediante la individuazione dei "processi sensibili" costituiti dalle attività maggiormente a "rischio di reato" e la loro conseguente proceduralizzazione, il modello si propone le finalità di:

- *determinare, in tutti coloro che operano in nome e per conto della società, una piena consapevolezza di poter incorrere, in caso di violazione delle disposizioni contenute in tale documento, in un illecito passibile di sanzioni, sul piano penale e amministrativo;*
- *rendere tali soggetti consapevoli che tali comportamenti illeciti potrebbero comportare sanzioni penali ed amministrative anche nei confronti dell'azienda;*
- *sottolineare come i comportamenti illeciti siano fortemente condannati e contrari agli interessi di Consorzio Depurazione del Savonese, anche quando apparentemente essa potrebbe trarne un vantaggio, poiché sono comportamenti contrari ai principi etico-sociali della società oltre che alle disposizioni di legge;*
- *consentire a Consorzio Depurazione del Savonese, grazie ad un monitoraggio costante dei processi sensibili e quindi dei rischi di commissione di reato, di reagire tempestivamente al fine di prevenire e contrastare la commissione dei Reati stessi.*

La società Consorzio Depurazione del Savonese, in relazione al particolare oggetto di attività, che riguarda il servizio idrico integrato (acquedotto, fognatura e depurazione), è sottoposta a numerosi controlli di conformità, oltre naturalmente agli eventuali controlli da parte dell'Amministrazione finanziaria e degli Enti Previdenziali.

L'adozione del Codice Etico e del presente Modello sottolineano la ferma volontà della società Consorzio Depurazione del Savonese di condannare tutti i comportamenti contrari alla legge ed ai regolamenti.

I principi cardine a cui il Modello si ispira, oltre a quanto sopra indicato, sono:

- a) le linee guida di Confindustria;
- b) i requisiti indicati dal D.Lgs. 231/2001, in particolare per quanto riguarda:
  - *l'attribuzione ad un organismo di vigilanza (Organismo di Vigilanza – ODV, analizzato al successivo paragrafo 4) interno in stretto contatto con il vertice aziendale di Consorzio Depurazione del Savonese ritenuto in grado di garantire un risultato soddisfacente del compito di promuovere l'attuazione efficace e corretta del Modello anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del D.Lgs. 231/2001;*
  - *la messa a disposizione a favore dell'ODV di risorse adeguate affinché sia supportato nei compiti affidatigli per raggiungere i risultati ragionevolmente ottenibili;*

- *l'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo ex post);*
  - *l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;*
- c) i principi generali di un adeguato sistema di controllo interno ed in particolare:
- *ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua;*
  - *nessuno deve poter gestire in autonomia un intero processo, ovvero deve essere rispettato il principio della separazione delle funzioni;*
  - *i poteri autorizzativi devono essere assegnati coerentemente con le responsabilità assegnate;*
  - *il sistema di controllo deve documentare l'effettuazione dei controlli, compresa la supervisione.*

### **3.3 La struttura del Modello: Parte Generale e Parti Speciali in funzione delle diverse figure di reato.**

La predisposizione del presente Modello ha richiesto una serie di attività volte alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D. Lgs. 231/2001.

La società Consorzio Depurazione del Savonese ha ritenuto di procedere con la predisposizione del Modello nella convinzione che tale sistema rappresenti anche uno strumento di miglioramento della *corporate governance* societaria, oltre che un'occasione per sensibilizzare il personale aziendale rispetto ai temi del controllo dei processi aziendali, al fine di prevenire i Reati.

Di seguito sono riportate, in estrema sintesi, le fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, ovvero i "processi sensibili" sulle cui basi si è poi potuto redigere il presente Modello.

#### 1) *Identificazione dei Processi Sensibili: "as-is analysis".*

Il lavoro di analisi del contesto aziendale, rappresentato dall'"ambiente di controllo" descritto nel capitolo 2 del presente Modello, è stato attuato attraverso il previo esame della documentazione aziendale (organigrammi, attività della società, processi principali, sistema delle deleghe, comunicati e comunicazioni organizzative, disposizioni organizzative, procedure aziendali etc..) e una serie di interviste con i soggetti "chiave" risultanti dall'organigramma aziendale e dal sistema delle deleghe (in particolare, il Presidente, i dirigenti ed i dipendenti aziendali nelle aree ritenute esposte a maggior rischio di commissione di reato) al fine di individuare i "processi

sensibili” e gli elementi del sistema di controllo interno preventivo (procedure esistenti, verificabilità, documentabilità, congruenza e coerenza delle operazioni, separazione delle responsabilità, documentabilità dei controlli, etc.).

Questa fase preliminare si è proposta l’obiettivo di identificare i processi aziendali esposti maggiormente ai rischi di reato e di verificare la tipologie e l’efficacia dei controlli esistenti al fine di garantire l’obiettivo di conformità alla legge. In tale fase sono state coinvolti i soggetti apicali della società in una metodologia articolata nei seguenti passi:

- identificazione dei reati previsti dal D.lgs. 231/01 e loro esame in merito all’applicabilità all’interno dei processi aziendali e del livello di rischio (alto, medio, basso) da parte dei soggetti apicali;
- nel caso di rischio/reato giudicato applicabile identificazione dei processi sensibili coinvolti sui quali si è proceduto con la gap analysis;
- documentazione delle attività svolta attraverso redazione di carte di lavoro.

Il risultato delle attività sopra riportate ha consentito di indentificare i “processi sensibili” del Consorzio Depurazione del Savonese che sono stati documentati dalle procedure aziendali e descritti nella “Parte Speciale I”, “Parte Speciale II”, “Parte Speciale III”, “Parte Speciale IV”, “Parte Speciale V” del presente modello.

## 2) Effettuazione delle analisi volte al miglioramento del sistema di controllo preventivo: “gap analysis”.

In base alle risultanze delle analisi effettuate e delle previsioni e finalità del D. Lgs. 231/2001, si sono individuati gli interventi volti a rafforzare l’attuale Sistema di Controllo Interno con particolare riferimento ai reati tutelati dalla norma, al fine di adottare un modello aziendale di organizzazione, gestione e monitoraggio ai sensi del D.Lgs. 231/2001.

A seguito della mappatura dei processi sensibili si è proceduto abbinando ad essi le relative procedure aziendali per descrivere ed identificare il sistema di controllo necessario a mitigare il rischio di commissione dei reati; Nello specifico si è operato come descritto di seguito:

- *formalizzazione delle procedure non ancora disponibili in azienda;*
- *collegamento tra processi sensibili ex D.Lgs. 231/01 e sottosistemi procedurali già attivi (es. sistema di certificazione ambientale, umbandling tariffario, ecc.).*

In tale modo si è prodotto un quadro di collegamento tra il Modello e le procedure aziendali che sono state messe a disposizione dell’Organismo di Vigilanza e che dovranno essere soggette a periodiche verifiche di conformità e di efficacia in relazione all’evoluzione normativa del D.Lgs. 231/01.

### 3) Predisposizione del Modello.

Per quanto riguarda la struttura, il presente Modello è costituito da una "Parte Generale" e da diverse "Parti Speciali" predisposte per le differenti categorie di reato contemplate nel D.Lgs. 231/2001.

La "Parte Speciale I", denominata "Reati nei rapporti con la Pubblica Amministrazione", riguarda le tipologie specifiche di Reati previste ai sensi degli artt. 24, 25 e 25 *quater* del D.Lgs. 231/2001.

La "Parte Speciale II", denominata "Reati Societari", si applica per le tipologie specifiche di Reati previste ai sensi dell'art. 25 *ter* del D.Lgs. 231/2001.

La "Parte Speciale III", denominata "omicidio colposo e lesioni gravi o gravissime, commessi in violazione delle norme antifortunistiche e sulla tutela dell'igiene e della salute sul lavoro", si applica per le specifiche di Reati previsti ai sensi dell'art. 25 *septies* del D.Lgs. 231/2001.

La "Parte Speciale IV", denominata "reati ambientali", si applica per le specifiche di Reati previsti ai sensi dell'art. 25 *undecies* del D.Lgs. 231/2001.

La "Parte Speciale V", denominata "reati informatici", si applica per le specifiche di reati previsti ai sensi degli art 24-bis e 25 *nonies*.

Con riferimento ai reati di seguito riportati, non si è ritenuto di procedere con la definizione di parti speciali specifiche:

- *corruzione tra privati: la legge anticorruzione (legge 190/2012) ha portato consistenti cambiamenti in termini di rischi reato, con la introduzione della corruzione tra privati e la necessità di apposita valutazione di rischi e strumenti idonei circa l'attuazione dei piani di prevenzione della corruzione. A tal proposito si è tenuto conto del reato introducendo il Codice Etico ribadendo i principi di correttezza e trasparenza da tenere da parte del personale aziendale nei confronti dei soggetti terzi ed in particolare verso i clienti ed i fornitori;*
- *impiego di cittadini di paesi terzi il cui soggiorno è irregolare: la società risulta responsabile quand'anche entrasse nel proprio sito/cantiere/area di lavoro una ditta esterna con lavoratori irregolari. A tal proposito si è proceduto ad adeguare i contratti con i terzi prevedendo clausole di salvaguardia aziendale al fine di evitare l'utilizzo di cittadini il cui soggiorno è irregolare;*
- *ricettazione, riciclaggio: la società Consorzio Depurazione del Savonese non dispone di sportelli aperti al pubblico per l'incasso della bollettazione.*
- = *omessa comunicazione conflitto di interessi: il reato di omessa comunicazione del conflitto di interessi è stato inserito dall'art. 31 L. n. 262/2005 nella categoria dei reati societari che costituiscono il*

*presupposto della responsabilità amministrativa degli enti, così come previsto dall'art. 25-ter, commi 1, lett. r) e 2, del D. Lgs. n. 231/2001. L'ipotesi di maggior rilievo sembra essere quella in cui la condotta omissiva dell'amministratore abbia causato danni non alla società di appartenenza, bensì ai terzi che sono venuti in contatto ed hanno concluso con la società medesima rapporti giuridici di qualsiasi genere;*

= *autoriciclaggio*: introdotto dall'art. 25 octies.

### **3.4 L'adozione del Modello.**

Il Modello, costituito dalla "Parte generale", dalla "Parte speciale I", "Parte speciale II", "Parte speciale III", "Parte speciale IV", "Parte speciale V", è adottato dal Consiglio di gestione di Consorzio Depurazione del Savonese S.p.A con apposita delibera.

Considerato che il presente Modello costituisce "atto di emanazione dell'organo dirigente", ai sensi dell'art. 6 co. 1 lett. a) del D.Lgs. 231/2001, la competenza in merito alle eventuali successive modifiche e integrazioni del Modello stesso sono di prerogativa del Consiglio di gestione del Consorzio Depurazione del Savonese.

Il Consiglio di gestione ha la facoltà di apportare al testo modifiche ed integrazioni di carattere formale.

Nella predetta delibera, tutti i membri del Consiglio di gestione dichiarano di impegnarsi al rispetto del presente Modello.

Allo stesso modo il Consiglio di Sorveglianza e l'organo di controllo contabile del Consorzio Depurazione del Savonese, presa visione del presente Modello, si impegnano al rispetto del Modello medesimo.

Il Consiglio di gestione delibera in merito alle modifiche proposte dai consiglieri e dal Consiglio di Sorveglianza.

Considerata l'importanza di dare adeguata informazione ai Soci, è opportuno che l'adozione del modello venga comunicato formalmente ai Soci stessi.

Considerata l'importanza di dare adeguata informazione ai Soci, il modello è formalmente trasmesso ai Soci stessi e pubblicato nell'apposita sezione del sito internet della società per renderlo disponibile al pubblico e alle terze parti.

### **3.5 L'identificazione la composizione dell'organismo interno di vigilanza.**

La norma (art. 6., lett. b) del D. Lgs.231/2001) richiede, quale condizione per ottenere l'esimente dalla responsabilità amministrativa, che il compito di vigilare sul funzionamento e l'osservanza delle indicazioni del Modello nonché di curarne

l'aggiornamento, sia affidato ad un organismo interno alla società dotato di autonomi poteri di iniziativa e di controllo.

L'autonomia richiesta dalla norma presuppone che l'ODV (*Organismo di Vigilanza*) risponda, nello svolgimento di questa sua funzione, al Consiglio di gestione.

L'Organismo di Vigilanza è composto da tre membri nominati dal Consiglio di Gestione che identifica tra gli stessi il Presidente.

I componenti devono possedere i requisiti di competenza professionale in discipline attinenti le funzioni inerenti l'incarico.

L'Organismo di Vigilanza si avvale di una funzione di staff opportunamente identificate per lo svolgimento delle verifiche di cui al presente modello.

### **3.6 Le funzioni e i poteri dell'organismo interno di vigilanza.**

All'*Organismo di Vigilanza* è affidato il compito di vigilare:

- 1) sull'osservanza delle prescrizioni del Modello da parte del Presidente dai componenti del CdG, dei dirigenti e dei dipendenti, dei consulenti, dei partner e delle società del Gruppo;*
- 2) sull'efficacia e adeguatezza del Modello, in relazione alla struttura aziendale, atto a salvaguardare la società dalla commissione dei Reati;*
- 3) sull'opportunità di aggiornamento del Modello, qualora si riscontrino esigenze di adeguamento dello stesso in relazione al mutamento della norma e delle condizioni aziendali.*

A tal fine, all'ODV sono altresì affidati i compiti di:

- attivare l'iter/attività di controllo indiretto previste dal Modello considerando che, in ogni caso, una responsabilità primaria del controllo rimane in capo al management che opera nell'ambito dei processi sensibili;*
- condurre ricognizioni sull'attività aziendale al fine di aggiornare la mappatura dei "processi sensibili", in particolare in caso di attivazione di nuove attività di business e quindi nuovi processi aziendali; per processi sensibili si intendono gli iter operativi propri della società; a titolo di esempio gli iter operativi inerenti: il ciclo attivo, il ciclo passivo, il ciclo finanziario;*
- effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere da Consorzio Depurazione del Savonese, soprattutto nell'ambito dei "processi sensibili";*
- essere informato dal management aziendale su situazioni che potrebbero comportare l'adozione di eventuali sanzioni disciplinari, ferma restando la*

*competenza di quest'ultimo per l'irrogazione della sanzione e il relativo procedimento disciplinare;*

- *fornire e richiedere alla Direzione Aziendale una struttura informativa contenente tutte le informazioni relative al D.Lgs. 231/2001 ed al Modello;*
- *dare impulso alle iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine del funzionamento del Modello, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;*
- *raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere ad esso trasmesse o tenute a sua disposizione;*
- *coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività aziendali in relazione alle procedure stabilite nel Modello. A tal fine, l'ODV ha libero accesso a tutta la documentazione aziendale che ritiene rilevante e deve essere costantemente informato dal management e dagli altri referenti/responsabili delle aree interessate sugli aspetti dell'attività aziendale che possono esporre Consorzio Depurazione del Savonese al rischio di commissione di uno dei Reati;*
- *verificare costantemente l'adeguatezza del Modello alle prescrizioni normative e, in collaborazione con le funzioni aziendali (anche attraverso apposite riunioni), valutare l'adeguatezza e le esigenze di aggiornamento del Modello;*
- *condurre le eventuali indagini interne volte ad accertare presunte violazioni delle prescrizioni del presente Modello.*

*Etica di comportamento dell'ODV: durante la propria attività l'ODV dovrà mantenere la massima discrezione e riservatezza, avendo come unici referenti gli organi sociali.*

### **3.7 I flussi informativi agli organi societari.**

L'ODV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

L'ODV ha due linee di reporting:

- *la prima, su base continuativa, nei confronti del Presidente e del Consiglio di Gestione;*
- *la seconda, almeno ogni 180 giorni, nei confronti del Consiglio di gestione e del Consiglio di Sorveglianza.*

L'ODV trasmette annualmente al Consiglio di gestione e al Consiglio di sorveglianza il piano di attività per l'anno successivo e il rapporto consuntivo sull'attività esercitata nell'anno trascorso, motivando gli scostamenti dal piano di attività preventiva.

L'ODV presenta annualmente al Consiglio di gestione il piano di attività per l'anno successivo, che potrà essere oggetto di apposita delibera.

L'ODV presenta annualmente al Consiglio di gestione il rapporto consuntivo sull'attività esercitata nell'anno trascorso, motivando gli scostamenti dal piano di attività preventiva.

Il reporting ha ad oggetto l'attività svolta dall'ufficio dell'ODV e le eventuali criticità emerse sia in termini di comportamenti o eventi interni a Consorzio Depurazione del Savonese, sia in termini di efficacia del Modello.

L'ODV propone al Consiglio di gestione, sulla base delle criticità riscontrate, le azioni correttive ritenute adeguate al fine di migliorare l'efficacia del Modello.

Gli incontri con gli organi cui l'ODV riferisce devono essere verbalizzati e copia dei verbali deve essere custodita dall'ODV e dagli organismi di volta in volta coinvolti.

Il Presidente del Consiglio di gestione ha la facoltà di convocare in qualsiasi momento l'ODV il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

### **3.8 I flussi informativi verso l'Organismo di Vigilanza.**

L'ODV deve essere informato, mediante apposite segnalazioni da parte del Presidente e dai componenti del CdG e del Consiglio di Sorveglianza, dei dirigenti e dei dipendenti, dei consulenti, dei partner in merito ad eventi che potrebbero ingenerare responsabilità di Consorzio Depurazione del Savonese ai sensi del D.Lgs. 231/2001.

Di seguito, sono esposte alcune prescrizioni di carattere generale:

- *devono essere raccolte eventuali segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei reati previsti dal Decreto Legislativo in oggetto o comunque a condotte non in linea con le regole di comportamento di cui al presente Modello;*
- *se un dipendente desidera segnalare una violazione (o presunta violazione) del Modello, lo stesso deve contattare il suo diretto superiore. Qualora la segnalazione non dia esito, ovvero qualora la segnalazione riguardi il diretto superiore, il dipendente ne riferisce all'ODV. I consulenti e i partner delle società, per quanto riguarda la loro attività svolta nei confronti di*

*Consorzio Depurazione del Savonese, effettuano la segnalazione direttamente all'ODV o ai Dirigenti se non coinvolti questi ultimi;*

- *l'ODV valuta le segnalazioni ricevute; e informa la competente funzione aziendale che assumerà i provvedimenti disciplinari idonei;*
- *coloro che effettuano segnalazioni in buona fede saranno garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso sarà assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate erroneamente e/o in malafede.*

Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere obbligatoriamente ed immediatamente trasmesse all'ODV le informazioni concernenti:

- *i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati tutelati dal D.Lgs. 231/2001;*
- *le richieste di assistenza legale inoltrate dai dirigenti e dipendenti in caso di avvio di procedimento giudiziario per i reati tutelati dal D.Lgs. 231/2001;*
- *i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/2001;*
- *le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero ai provvedimenti di archiviazione di tali procedimenti comprendenti le relative motivazioni.*

### **3.9 La raccolta e conservazione delle informazioni.**

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'ODV in un apposito data base riservato (informatico o cartaceo) per un periodo 10 anni.

L'accesso al *data base* è consentito esclusivamente al Presidente del Consiglio di gestione o a soggetto da lui autorizzato.

Compito primario dell'ODV di Consorzio Depurazione del Savonese è l'esercizio dei controlli sulle attività della società relativamente ai "processi sensibili" secondo le procedure di seguito descritte, avvalendosi, della struttura di staff e del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

## 4. La diffusione della conoscenza del Modello.

### 4.1 La formazione del personale.

Ai fini dell'efficacia del presente Modello, è obiettivo del Consorzio Depurazione del Savonese garantire una corretta conoscenza, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei "processi sensibili".

La formazione del personale ai fini dell'attuazione del modello è gestita dal Comitato di Direzione in stretta cooperazione con l'ODV.

#### 1) La comunicazione iniziale.

L'adozione del presente Modello è comunicata a tutte le parti presenti in azienda al momento dell'adozione stessa e pubblicata sul sito della società in apposita sezione.

#### 2) La formazione.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società.

In particolare, Consorzio Depurazione del Savonese ha previsto livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione.

Personale Direttivo e con funzioni di rappresentanza:

- *seminario iniziale;*
- *seminario di aggiornamento annuale;*
- *e-mail di aggiornamento in occasione di modifiche del modello mediante utilizzo della piattaforma informativa;*
- *informativa nella lettera di assunzione per i neoassunti;*
- *informativa al personale che rientra dopo lunghi periodi di assenza.*

Altro personale dipendente e collaboratori:

- *corsi di formazione o comunicazioni ufficiali;*
- *Informativa nella lettera di assunzione per i neoassunti;*
- *e-mail di aggiornamento in occasione di modifiche del modello mediante utilizzo della piattaforma informativa;*
- *informativa al personale che rientra dopo lunghi periodi di assenza.*

#### **4.2 L' informativa a Collaboratori esterni e Partner.**

I consulenti e i partner sono informati del contenuto del Modello e dell'esigenza del Consorzio Depurazione del Savonese che il loro comportamento sia conforme ai disposti del D.Lgs. 231/2001, utilizzando l'area dedicata sul sito internet della società, dando comunicazione della presa visione alla Società.

## **5. Il sistema disciplinare.**

### **5.1 La funzione del sistema disciplinare.**

La definizione di un adeguato sistema sanzionatorio costituisce, ai sensi dell'art. 6 secondo comma lettera e) del D.Lgs. 231/2001, un requisito essenziale del Modello ai fini dell'esimente rispetto alla responsabilità della società.

La definizione di un sistema di sanzioni commisurate alla violazione e dotate di deterrenza applicabili in caso di violazione delle regole di cui al presente Modello, rende efficiente l'azione di vigilanza dell'ODV ed ha lo scopo di garantire l'effettività del Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito della conclusione del procedimento penale avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare integri una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

### **5.2 Le misure nei confronti dei lavoratori dipendenti.**

La violazione da parte dei dipendenti delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori - nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali normative speciali applicabili - sono quelli previsti dall'apparato sanzionatorio di cui al vigente CCNL, e precisamente:

- *richiamo verbale;*
- *rimprovero scritto;*
- *multa, non superiore a quanto previsto dal vigente CCNL;*
- *sospensione dal lavoro e dalla retribuzione di ammontare non superiore a quanto previsto dal vigente CCNL;*
- *licenziamento con preavviso;*
- *licenziamento senza preavviso.*

Il rispetto delle prescrizioni del presente Modello rientra quindi nel generale obbligo del lavoratore di rispettare le disposizioni aziendali e di agire in conformità agli interessi aziendali.

I comportamenti sanzionabili che costituiscono violazione del presente Modello sono i seguenti (a titolo esemplificativo e non esaustivo):

- *violazione, da parte del dipendente, di procedure interne previste dal presente Modello (ad esempio la non osservanza delle procedure*

*prescritte, l'omissione di comunicazioni all'ODV in merito a informazioni prescritte, omissione di controlli, etc.) o adozione, nell'espletamento di attività connesse ai "processi sensibili", di comportamenti non conformi alle prescrizioni del Modello;*

- *violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento di attività connesse ai "processi sensibili", di comportamenti non conformi alle prescrizioni del Modello stesso che esponano la società ad una situazione oggettiva di rischio di commissione di uno dei Reati;*
- *adozione, nell'espletamento di attività connesse ai "processi sensibili", di comportamenti non conformi alle prescrizioni del presente Modello e diretti in modo univoco al compimento di uno o più Reati;*
- *adozione, nell'espletamento di attività connesse ai "processi sensibili", di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tali da determinare la concreta applicazione a carico della società di sanzioni previste dal D.Lgs. 231/2001.*

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate, nella logica dell'equilibrio tra comportamento e conseguenza disciplinare, in relazione:

- *al livello di responsabilità ed autonomia del Dipendente;*
- *all'eventuale esistenza di precedenti disciplinari a carico dello stesso;*
- *all'intenzionalità del suo comportamento nonché alla gravità del medesimo, intesa come il livello di rischio a cui la società può ragionevolmente ritenersi esposta a seguito della condotta censurata;*
- *alle altre particolari circostanze in cui si è manifestato il comportamento in violazione del presente modello.*

Al fine di disciplinare le modalità di applicazione delle sanzioni di cui al presente capitolo la Società si è dotata di un sistema disciplinare allegato al Codice Etico.

Il sistema disciplinare è soggetto a costante verifica e valutazione da parte dell'ODV e dalla Direzione, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari delineate su eventuale segnalazione dell'ODV.

### **5.3 Le misure nei confronti dei dirigenti, del Presidente e dei componenti dei CdG e organi di controllo.**

La violazione, da parte dei dirigenti, delle procedure previste dal presente Modello o l'adozione, nell'espletamento delle attività nell'ambito dei "processi

sensibili”, di comportamenti non conformi alle prescrizioni del Modello, determinerà l’applicazione delle misure idonee in conformità alle prescrizioni indicate nel Contratto Collettivo Nazionale di Lavoro della categoria.

In caso di violazione del presente Modello da parte del Presidente e dei componenti del CdG, l’ODV informa il Consiglio di gestione ed il Consiglio di Sorveglianza, i quali provvederanno ad assumere le iniziative ritenute idonee secondo le indicazioni della vigente normativa.

In caso di violazione del presente Modello da parte dell’Organo di Controllo Contabile, l’ODV informa il Presidente del Consiglio di gestione ed il Presidente del Consiglio di Sorveglianza che provvederanno ad assumere le iniziative ritenute idonee, tra le quali, la convocazione dell’assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

#### **5.4 Le misure nei confronti di Collaboratori esterni e Partner.**

La violazione del presente Modello da parte di collaboratori esterni e partner comporterà , in relazione a quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di partnership, la risoluzione del rapporto contrattuale.

Resta salva l’eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla società, come nel caso di applicazione da parte del giudice delle misure previste dal D.Lgs. 231/2001.

## **6. Le verifiche sull'adeguatezza del Modello.**

L'ODV svolge un'attività di vigilanza sull'efficacia del Modello, inoltre periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei Reati, eventualmente coadiuvandosi con soggetti terzi.

La verifica consiste in un'attività di analisi dei rischi reato ex D.Lgs. 231/2001 secondo quanto previsto nel presente Modello Organizzativo.

Con riferimento alle segnalazioni ricevute nel corso dell'anno, alle azioni intraprese dall'ODV e dagli altri soggetti interessati, sugli eventi considerati rischiosi verrà predisposto un report annuale indirizzato al Consiglio di gestione, come riportato al precedente punto 5.3.

**PARTE SPECIALE I - Reati nei rapporti con la Pubblica  
Amministrazione**

## **1 Destinatari della “Parte Speciale I”.**

La *Parte Speciale* concerne i comportamenti posti in essere dal Presidente e dai componenti del CdG, dirigenti e dipendenti di Consorzio Depurazione del Savonese, nonché dai suoi consulenti e partner come risultano definiti nella Parte Generale.

Finalità della *Parte Speciale* è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dal D.Lgs. 231/2001 al fine di prevenire il verificarsi dei Reati oggetto di tutela.

Nello specifico, la presente *Parte Speciale* ha lo scopo di:

- a) fornire le “*regole di comportamento*” e le *procedure* che il Presidente e dai componenti del CdG, i dirigenti ed i dipendenti, nonché i consulenti e partner di Consorzio Depurazione del Savonese sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all’ODV, e ai responsabili delle altre funzioni aziendali che cooperano con il medesimo, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

## 2. I reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001).

La "Parte Speciale I" riguarda i reati realizzabili nell'ambito dei rapporti tra la società e la Pubblica Amministrazione (da intendersi atti commessi in danno allo Stato, ad altri Enti Pubblici e alla Comunità Europea attuati da soggetti privati o da pubblici ufficiali o da soggetti incaricati di un pubblico servizio) tralasciando i reati riguardanti la falsità in monete, carte di pubblico credito e in valori in bollo previsti all'art. 25 bis.

La qualifica di pubblico ufficiale va riconosciuta ai soggetti, pubblici dipendenti o privati, che:

- possono o debbono, nell'ambito di una potestà regolata dal diritto pubblico, formare e manifestare la volontà della Pubblica Amministrazione ovvero esercitare poteri autorizzativi o certificativi;
- sono incaricati di un pubblico servizio anche se agiscono nell'ambito di una attività disciplinata nelle forme della pubblica funzione anche in mancanza dei poteri tipici di quest'ultima.

Di seguito vengono descritte, in sintesi, le singole fattispecie di reato previste nel D.Lgs. 231/2001 agli artt. 24 e 25 contenuti nel Capo I sezione III.

In particolare i reati che rilevano ai fini delle sanzioni di cui trattasi sono riconducibili:

- a) ipotesi di corruzione e concussione;
- b) ipotesi di malversazione e di indebita percezione di erogazioni;
- c) ipotesi di truffa.

### **a) Ipotesi di concussione e corruzione.**

Il codice penale, al titolo II, capo I (Delitti dei pubblici ufficiali contro la pubblica amministrazione) prevede tra il resto le ipotesi di corruzione, malversazione, indebita percezione di erogazioni. Il D.Lgs.231/2001 relativamente alla incidenza della gravità sanziona in modo graduale le ipotesi di corruzione.

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

Tale ipotesi di reato, come modificata dalla L. 190/12, si configura nel caso in cui un pubblico ufficiale riceva indebitamente per sé o per un terzo, per l'esercizio delle sue funzioni o dei suoi poteri, denaro o altra utilità o ne accetti la promessa .

La norma oggetto di disamina configura un vero e proprio “asservimento” del soggetto pubblico ai desideri del soggetto privato, stante la non necessità di dimostrare un legame tra il compenso ed uno specifico atto dell’ufficio.

Tale ipotesi di reato di “corruzione” (che configura una violazione del principio di correttezza ed imparzialità cui deve comunque conformarsi l’attività della Pubblica Amministrazione) si differenzia dalla “concussione”, in quanto tra corrotto e corruttore esiste un accordo libero e nella volontà delle parti, mentre nella concussione (così come nell’induzione indebita a dare o promettere utilità) sussiste una condotta di prevaricazione abusiva del funzionario pubblico, idonea, a seconda dei contenuti che assume, a costringere o a indurre il privato comunque in posizione di soggezione, alla dazione o alla promessa indebita.

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

Il reato si configura allorché il pubblico ufficiale, che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

✓ *Circostanze aggravanti (Art. 319 bis)*

La pena è aumentata se il fatto di cui all’art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l’amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi.

✓ *Corruzione in atti giudiziari (art. 319-ter)*

Il reato (che costituisce una fattispecie autonoma) assume la sua connotazione nel caso in cui i fatti di corruzione indicati negli articoli precedenti vengano posti in essere al fine di favorire o danneggiare una parte in un processo civile, penale o amministrativo (ad esempio corrompendo un magistrato, ma anche un cancelliere od altro funzionario). Le pene sono aumentate qualora dal fatto derivi l’ingiusta condanna di taluno alla reclusione.

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

Le disposizioni degli artt. 318 e 319 si applicano anche all’incaricato di un pubblico servizio.

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

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

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

La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri.

La pena di cui al comma secondo si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319.

✓ *Peculato, concussione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (Art. 322-bis c.p.).*

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

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

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

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

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

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

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte

del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale (4).

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

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

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali ovvero al fine di ottenere o di mantenere un'attività economica o finanziaria.

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

✓ *Concussione (art. 317 c.p.)*

La fattispecie in esame, come modificata dalla Legge 190/2012, sanziona il pubblico ufficiale, che abusando della sua qualità o dei suoi poteri, costringe taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Si intende per "abuso", la strumentalizzazione da parte del pubblico ufficiale di una qualità effettivamente sussistente (abuso della qualità), o delle attribuzioni ad essa inerenti (abuso dei poteri) per il perseguimento di un fine illecito.

L'abuso costituisce elemento caratterizzante del reato di concussione, unitamente alla "costrizione", e cioè la "eterodeterminazione" dell'altrui volontà, l'obbligare taluno a compiere un'azione che altrimenti non sarebbe stata compiuta o ad astenersi dal compiere un'azione che sarebbe altrimenti stata compiuta.

La costrizione si esplica mediante violenza o, più spesso, mediante minaccia.

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

La fattispecie in esame, introdotta dalla L. 190/12, che si differenzia innanzitutto da quella di concussione per l'inclusione dell'incaricato di pubblico servizio tra i soggetti attivi.

Sotto il profilo della condotta, poi, le fattispecie presentano una formulazione analoga salvo per il fatto che nel caso in esame, in luogo della costrizione, viene sanzionata l' "induzione" (precedentemente compresa nella concussione) e cioè una forma *di pressione morale, con più tenue valore*

*condizionante la libertà di autodeterminazione del destinatario* il quale, a differenza della concussione, non è considerato vittima ma concorrente del soggetto pubblico e viene, perciò, penalmente sanzionato.

**b) Ipotesi di malversazione e di indebita percezione di erogazioni.**

Il codice penale prevede agli artt. 316 bis e seguenti i reati di “malversazione a danno dello Stato” e “l’indebita percezione di erogazioni a danno dello Stato”.

✓ *Malversazione a danno dello Stato o dell’Unione Europea (art. 316-bis c.p.)*

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti, sovvenzioni o contributi da parte dello Stato italiano, da Ente Pubblico o dell’Unione Europea destinati alla realizzazione di opere o allo svolgimento di attività, non si proceda all’utilizzo o alla destinazione delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell’aver distratto, anche parzialmente, le attribuzioni di denaro, senza che rilevi che l’attività programmata si sia comunque svolta).

Rileva che i predetti finanziamenti, sovvenzioni o contributi siano qualificati come “attribuzioni di denaro a fondo perduto o caratterizzate da una onerosità ridotta rispetto a quella derivante dalla applicazione delle ordinarie condizioni di mercato”.

Tenuto conto che il momento in cui viene considerato consumato il reato trova coincidenza con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati. Inoltre, occorre evidenziare che rientra altresì nella ipotesi di reato di truffa anche la fattispecie della mancata evidenziazione di informazioni che, se in possesso del soggetto erogante, implicherebbero un esito negativo alla conclusione dell’iter previsto dal bando.

✓ *Indebita percezione di erogazioni in danno dello Stato o dell’Unione Europea (art. 316-ter c.p.)*

Tale ipotesi di reato ha luogo qualora - mediante l’utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l’omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri Enti Pubblici o dalla Comunità Europea.

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

Infine, va ancora sottolineato che tale ipotesi di reato assume natura residuale rispetto alla fattispecie della truffa ai danni dello Stato, poiché si configura solamente nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

### **c) Le ipotesi di truffa.**

✓ *Truffa in danno dello Stato, di altro Ente Pubblico o dell'Unione Europea (art. 640, comma 2 n. 1, c.p.)*

Tale ipotesi di reato si configura nel caso in cui, per realizzare per sé o per altri un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e conseguentemente da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).

Il comportamento attraverso il quale si realizza il reato di truffa consiste in qualsivoglia attività che possa trarre in errore l'ente che deve effettuare l'atto di disposizione patrimoniale.

A titolo esemplificativo tale reato può realizzarsi qualora, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non corrispondenti al vero (come, ad esempio, utilizzando documentazione artefatta che rappresenti anche la realtà in modo distorto) al fine di ottenere l'aggiudicazione della gara stessa. Rileva altresì il reato di truffa qualora si tacciano informazioni che, se conosciute dall'Ente, quest'ultimo avrebbe sicuramente posto parere negativo alla sua volontà negoziale.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire in modo indebito erogazioni pubbliche. L'elemento qualificante rispetto al reato appena esaminato (art. 640 c.p.) è costituito dall'oggetto materiale della frode in quanto "per erogazione pubblica" va intesa "ogni attribuzione economica agevolata erogata da parte dello Stato, di Enti Pubblici o dalle Comunità europee".

Tale fattispecie può realizzarsi qualora si pongano in essere artifici o raggiri idonei ad indurre in errore il soggetto erogante, come, a titolo esemplificativo, nel caso di trasmissione di dati non corrispondenti al vero oppure predisponendo una documentazione falsa, sempre con l'intento di ottenere l'erogazione di finanziamenti, contributi, mutui agevolati per individuati impieghi o di altre erogazioni concessi dallo Stato o da altri Enti Pubblici o dalla Comunità Europea.

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

Tale ipotesi di reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti o intervenendo senza alcun diritto sui dati le informazioni o i programmi, si ottenga un ingiusto profitto arrecando così un danno a terzi.

### 3. Processi “sensibili” della Consorzio Depurazione del Savonese nei rapporti con la Pubblica Amministrazione.

I reati in precedenza illustrati riguardano i rapporti intercorrenti con la Pubblica Amministrazione.

Al fine di identificare i processi sensibili sono stati coinvolti i soggetti apicali della società con una metodologia composta dalle seguenti attività:

- identificazione reati previsti dal D.lgs. 231/01;
- valutazione del rischio riferito ad ogni reato all'interno dei processi aziendali determinandone l'applicabilità o meno per la società;
- identificazione dei processi sensibili sui quali si è valutata la gap analysis;
- documentazione delle attività svolta attraverso redazione di carte di lavoro.

Le attività della Consorzio Depurazione del Savonese che sono state ritenute esposte maggiormente a rischio, ovvero i “processi sensibili”, sono riconducibili alle seguenti fattispecie:

- ✓ *partecipazione a procedure di gara o di negoziazione diretta indette da Enti Pubblici per l'assegnazione di commesse (di appalto di fornitura o di servizi);*
- ✓ *partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e la relativa gestione;*
- ✓ *gestione dei rapporti con gli Enti Pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio, necessarie al processo di espansione o integrazione delle attività aziendali;*
- ✓ *contatto con gli Enti Pubblici per la gestione di adempimenti, verifiche, ispezioni, qualora lo svolgimento delle attività aziendali comporti lo smaltimento di rifiuti solidi, liquidi o gassosi, ovvero l'emissione di fumi o la produzione di inquinamento acustico/idrico soggetti a controlli da parte di soggetti pubblici;*
- ✓ *gestione dei rapporti con i soggetti pubblici relativi all'assunzione di personale appartenente a categorie protette o la cui assunzione è agevolata;*
- ✓ *gestione di trattamenti previdenziali del personale e/o gestione dei relativi accertamenti / ispezioni;*

- ✓ *gestione dei rapporti con organismi di vigilanza relativi allo svolgimento di attività regolate dalla legge;*
- ✓ *richiesta di provvedimenti amministrativi occasionali / ad hoc necessari allo svolgimento di attività strumentali a quelle tipiche aziendali gestione di beni mobili registrati legati all'attività aziendale;*
- ✓ *predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;*
- ✓ *adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc, differenti da quelli descritti ai precedenti punti e nelle verifiche, accertamenti e procedimenti sanzionatori che ne derivano.*

Il Consiglio di gestione della Consorzio Depurazione del Savonese potrà disporre, qualora se ne ravvisi la necessità, ulteriori integrazioni dei suddetti "processi sensibili" definendo, se del caso, gli opportuni provvedimenti operativi.

## 4. Procedure adottate.

### 4.1 Il sistema procedurale

Tutte le “operazioni sensibili” devono essere attuate conformandosi alle leggi vigenti, alle norme del “Codice Etico”, ai valori e alle politiche della società e alle regole contenute nel presente Modello.

Ne consegue che il sistema di organizzazione della società risulta rispettare i requisiti fondamentali della formalizzazione e della chiarezza, della comunicazione e della separazione dei ruoli con particolare riferimento all’attribuzione delle funzioni di responsabilità e di rappresentanza nonché si uniforma alla definizione delle linee gerarchiche e delle attività operative.

Tenuto conto che:

- a) la struttura organizzativa definisce le modalità di delega e di controllo sia dell’“autorità” gerarchicamente preposta alle diverse aree dell’attività sia delle responsabilità che ne derivano. Essa struttura dipende dalle dimensioni e dalla natura dell’attività; quest’ultimo aspetto, per il caso di cui trattasi:
  - richiede un particolare livello tecnologico del settore;
  - si colloca in una normativa e regolamentazione specifica che rilevano e influenzano il tipo di struttura organizzativa utilizzata.
- b) Il sistema di controllo interno:
  - deve essere progettato e funzionante in modo tale da fornire, con ragionevole attendibilità, il perseguimento degli scopi sociali, sempre nella considerazione che il “costo” del controllo interno non ecceda i benefici attesi dal medesimo;
  - è efficace nella misura in cui è efficace e professionale il personale preposto a detto sistema;
  - è efficace quando vi è separazione di compiti e funzioni.

La società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, etc.) improntati a principi generali come:

- a) diffusione adeguata all’interno della società, enfatizzando il messaggio che i comportamenti posti in essere in violazione delle procedure aziendali fissate danno luogo a sanzioni disciplinari da parte della società;
- b) una formale e precisa delimitazione dei ruoli, con una esauriente descrizione delle prerogative facenti capo a ciascuna funzione (e dei correlati poteri), con un più pregnante coinvolgimento per i soggetti che ricoprono posizioni di responsabilità;

- c) certezza del processo di comunicazione, che deve risultare chiaro, realistico e concreto, e che sussista la trasparenza e la riconoscibilità dei processi decisionali ed attuativi con una descrizione dei flussi informativi.

A seguito della mappatura dei processi sensibili si è proceduto abbinando ad essi le relative procedure aziendali per descrivere ed identificare il sistema di controllo necessario a mitigare il rischio di commissione dei reati; Nello specifico si è operato come descritto di seguito:

- *formalizzazione delle procedure non ancora disponibili in azienda;*
- *collegamento tra processi sensibili ex D.Lgs. 231/01 e sottosistemi procedurali già attivi (es. sistema di certificazione ambientale, unbandling tariffario, ecc.).*

In tale modo si è prodotto un quadro di collegamento tra il Modello e le procedure aziendali che sono state messe a disposizione dell'Organismo di Vigilanza e che dovranno essere soggette a periodiche verifiche di conformità e di efficacia in relazione all'evoluzione normativa del D.Lgs. 231/01.

Le procedure interne sono caratterizzate dai seguenti elementi:

- a) separazione, all'interno di ciascun processo, tra:
- il soggetto che lo avvia (impulso decisionale)
  - il soggetto che lo attua e lo porta a conclusione
  - e il soggetto che sovrintende ai controlli;
- b) tracciabilità di ciascun passaggio rilevante del processo;
- c) formalizzazione adeguata.

#### **4.2 Principi generali di comportamento.**

I seguenti divieti di carattere generale si applicano al Presidente e dai componenti del CdG, Dirigenti e Dipendenti di Consorzio Depurazione del Savonese, in via diretta, ed ai Consulenti, ai partner ed alle società del gruppo in forza di apposite clausole contrattuali.

E' fatto divieto di porre in essere, dare collaborazione o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate.

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare di:

- a) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- b) distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche

commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo adeguato per consentire le verifiche da parte dell'ODV;

- c) accordare vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto b);
- d) effettuare prestazioni in favore dei Consulenti, dei Partner e delle società del gruppo che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- e) riconoscere compensi in favore dei Consulenti, dei Partner e delle società del gruppo che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- f) effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- g) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati.

#### **4.3 Procedure specifiche generalmente applicabili.**

Ai fini dell'attuazione delle regole e divieti elencati devono essere rispettate le procedure qui di seguito descritte, oltre alle Regole e Principi Generali già contenuti nella Parte Generale del presente Modello.

Le regole qui di seguito descritte, devono essere rispettate sia nell'esplicazione dell'attività di Consorzio Depurazione del Savonese in territorio italiano, sia all'estero:

- a) ai soggetti che intrattengono rapporti formali con la P.A. per conto di Consorzio Depurazione del Savonese deve essere conferito potere in tal senso dalla stessa Consorzio Depurazione del Savonese;
- b) in seguito a criticità di rilievo o conflitto di interesse che sorgano nell'ambito del rapporto con la P.A. deve esserne informato l'ODV con nota scritta da parte del responsabile dell'operazione (si rimanda al §4.4);

- c) i contratti tra Consorzio Depurazione del Savonese e i consulenti esterni, i partner e le società del gruppo devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti;
- d) i contratti con consulenti esterni, partner devono contenere clausole standard al fine del rispetto del D. Lgs. 231/2001;
- e) nei contratti con consulenti esterni, partner e società del gruppo deve essere contenuta apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. 231/2001 e delle sue implicazioni per la società e di impegnarsi al rispetto del D.Lgs. 231/2001;
- f) nei contratti con consulenti esterni, partner e società del gruppo deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali, etc.);
- g) le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi o finanziamenti devono contenere solo elementi veritieri, nonché l'impegno della società beneficiaria, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti, secondo le finalità previste dalla specifica normativa di riferimento;
- h) coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari, etc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'ODV eventuali situazioni di irregolarità o anomalie.

Il Consorzio Depurazione Acque del Savonese adotta un proprio "modello di gestione trasparente dell'amministrazione" coerente con le disposizioni normative e dell'ANAC in materia.

E' stato altresì nominato il responsabile della prevenzione della corruzione ai sensi dell'art. 1 comma 7 della legge n. 190/2012 atto a prevenire la commissione di atti di corruzione. Tale elemento rafforza il sistema di controllo nell'ambito della prevenzione dei reati.

#### **4.4 Elementi fondamentali del processo decisionale.**

Per ogni operazione considerata sensibile occorre dare debita evidenza (ad esempio, la partecipazione a procedure di gara o di negoziazione diretta indette da Enti Pubblici italiani o stranieri per l'assegnazione di commesse).

A tal fine, il Presidente del CdG o un Dirigente da questi incaricato deve nominare un responsabile per la singola operazione ritenuta a rischio sopra indicata, il quale è in generale il soggetto che gestisce tale operazione e ne

costituisce il referente (qualora l'operazione sensibile abbia ad oggetto, ad esempio, un rapporto commerciale con la P.A., viene individuato nel soggetto incaricato di entrare in rapporto con la P.A.). Nell'ambito del Consorzio, il responsabile interno è il dirigente di settore coinvolto ed in caso questi lo ritenesse necessario un suo delegato.

Il Responsabile Interno:

- diviene il soggetto referente e responsabile dell'operazione a rischio;
- è responsabile in particolare dei rapporti con la P.A., nell'ambito del procedimento da espletare.

Per ogni singola operazione a rischio deve essere compilata dal Responsabile Interno un'apposita documentazione da tenere aggiornata nel corso dello svolgimento della procedura. I controlli dell'ODV

I controlli dell'ODV consistono in un'attività di analisi dei rischi reato ex D.Lgs. 231/2001 secondo quanto previsto nel presente Modello Organizzativo.

A tal fine, all'ODV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Inoltre, l'ODV può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nel punto 4.2 della "*Parte Generale*".

Durante la propria attività l'ODV dovrà mantenere la massima discrezione e riservatezza avendo come unici referenti gli Organi Sociali di cui al punto 4.3. della "*Parte Generale*".

## **PARTE SPECIALE II - Reati Societari**

## **1. Destinatari della “Parte Speciale - II”**

La presente Parte Speciale si riferisce a comportamenti posti in essere dal Presidente e dai componenti del CdG, dirigenti e dipendenti di Consorzio Depurazione del Savonese, nonché dai suoi consulenti, partner e società del Gruppo come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dal D.Lgs. 231/2001 al fine di prevenire il verificarsi dei Reati tutelati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- a) indicare le “regole di comportamento” e le procedure che il Presidente e i componenti del CdG, i dirigenti ed i dipendenti, nonché i consulenti, partner e società del Gruppo di Consorzio Depurazione del Savonese sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all’ODV, e ai responsabili delle altre funzioni aziendali che cooperano con lui, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

## 2. I reati societari (art. 25 ter del D.Lgs. 231/2001)

La “Parte Speciale II” riguarda i reati societari; in tema di disciplina degli illeciti penali ed amministrativi delle società le apposite norme riformulate dal D.Lgs. n. 61 dell’11 aprile 2002 sono accolte nelle disposizioni di cui al D.Lgs. 231/2001 e precisamente all’art. 25 ter.

Ne consegue che, per le fattispecie di reato di seguito descritte, *“se commessi nell’interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità agli obblighi inerenti alla loro carica”*, trova applicazione il sistema sanzionatorio di carattere pecuniario, qualora sia rilevata l’inesistenza del “Modello di organizzazione, gestione e controllo” ed il mancato rispetto degli obblighi di vigilanza. Le modalità di attuazione sono da ricercarsi sia attraverso specifiche misure organizzative e procedurali atte a fornire, con ragionevolezza, garanzie di prevenzione dei predetti reati sia attraverso una puntuale definizione dei compiti dell’organismo di vigilanza affinché assicurati, nella sua continuità, l’effettivo ed efficace funzionamento del citato Modello.

In particolare i reati che rilevano ai fini delle sanzioni di cui trattasi sono riconducibili a:

- a) ipotesi di falsità;
- b) tutela del capitale sociale e del patrimonio sociale;
- c) tutela del corretto funzionamento della società;
- d) tutela contro le frodi;
- e) tutela delle funzioni di vigilanza;
- f) illeciti commessi mediante omissione;
- g) operazioni realizzate dai liquidatori;
- h) corruzione tra privati.

### **a) Ipotesi di falsità.**

- ✓ *False comunicazioni sociali in danno dei soci e dei creditori (artt. 2621 e 2622 c.c.)*

Si realizza il delitto di false comunicazioni sociali qualora un soggetto investito di una carica sociale espone intenzionalmente nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci, ai creditori o al pubblico, fatti non rispondenti al vero, ancorché oggetto di valutazioni, idonei ad indurre in errore i destinatari della situazione economica, patrimoniale o finanziaria della società (o del gruppo al quale essa appartiene) con l’intenzione di ingannare i

soci, i creditori o il pubblico; ovvero omette, con la stessa intenzione, informazioni sulla situazione la cui comunicazione sociale è imposta dalla legge.

Si precisa, tra l'altro, che:

- le informazioni false o omesse sono rilevanti quando alterano sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società e sono dirette ai soci o a terzi soggetti con esclusione di quelle rivolte ad organi sociali di altre società, anche se collegate o appartenenti al medesimo gruppo o rivolte al Fisco (quest'ultima fattispecie è normalizzata dal D.Lgs. 74/2000);
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- oltre a possedere idoneità ingannatoria, l'informazione (o la sua omissione) deve riguardare fatti / accadimenti aziendali e non solo le valutazioni per le quali è prevista peraltro una "soglia" di non punibilità solo quando dette valutazioni – singolarmente considerate – non subiscono oscillazioni superiori al 10% della valutazione corretta;
- qualora le falsità o le omissioni determinino una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5% o una variazione del patrimonio netto non superiore all'1% sono considerate dalla prassi "non significative";
- nel termine "*comunicazioni sociali*" sono anche ricomprese le dichiarazioni trasfuse nella gestione contabile con la finalità di alterare fraudolentemente la verità;
- il reato di cui all'articolo 2622 c.c. è punibile a querela di parte, salvo che si tratti di società quotate, e per la sua qualificazione necessita che l'autore sia mosso sia dalla intenzione di fornire false informazioni sia dall'intento di conseguire un profitto.

✓ *Falsità nelle relazioni o nelle comunicazioni del revisore legale (27 D.Lgs. 39/2010)*

Il reato consiste in false attestazioni od occultamento di informazioni, da parte dei responsabili della revisione, concernenti la situazione economica, patrimoniale o finanziaria della società, al fine di conseguire per sé o per altri un ingiusto profitto. La sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

Soggetti attivi sono il revisore legale (reato proprio), ma i componenti degli organi di amministrazione e di controllo di Consorzio Depurazione del Savonese e i suoi dipendenti possono essere coinvolti a titolo di concorso nel reato. E', infatti,

ipotizzabile il concorso eventuale, ai sensi dell'art. 110 c.p., degli amministratori, dei sindaci, o di altri soggetti della società revisionata, che abbiano determinato o istigato la condotta illecita del revisore legale.

#### **b) Tutela del capitale sociale e del patrimonio sociale.**

##### ✓ *Formazione fittizia del capitale (art. 2632 c.c.)*

Tale ipotesi si ha quando il capitale sociale risulta formato o aumentato fittiziamente mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; oppure quando vengono sottoscritte reciprocamente azioni o quote; oppure quando vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione.

La norma tende a penalizzare le valutazioni irragionevoli sia in correlazione alla natura dei beni valutati sia in correlazione ai criteri di valutazione adottati.

##### ✓ *Indebita restituzione dei conferimenti (art. 2626 c.c.)*

Il reato riguarda la tutela della integrità del capitale sociale e si compie allorché gli amministratori in assenza di legittima riduzione del capitale sociale, provvedano alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

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

Allo scopo di garantire l'integrità del patrimonio sociale la norma prevede alcune precise limitazioni circa la distribuzione di utili o acconti su utili non effettivamente conseguiti.

Il reato consiste nella ripartizione di utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Si osserva peraltro che la restituzione degli utili percepiti o la ricostituzione delle riserve indisponibili prima del termine previsto per l'approvazione del bilancio estingue il reato (la norma non evidenzia chi debba provvedere alla restituzione).

Con la riforma societaria, dal 1° gennaio 2004, è previsto che l'ammontare degli acconti su utili non deve superare il minore importo tra quello degli utili conseguiti dall'inizio dell'esercizio, al netto delle somme da destinarsi a riserva, e quello delle riserve disponibili.

✓ *Illecite operazioni sulle azioni o quote sociali (art. 2628 c.c.)*

Il reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

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

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

La norma è posta alla tutela della effettività ed integrità del capitale sociale, considerata la sua funzione di garanzia patrimoniale nei confronti dei terzi.

Il reato – perseguibile solo a querela della parte lesa – si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di operazioni di riduzione del capitale sociale o di operazioni di fusione con altra società o scissioni, che cagionino danno ai creditori.

Si fa osservare che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

**c) Tutela del corretto funzionamento della società.**

✓ *Impedito controllo (art. 2625 c.c. e art. 29 D.Lgs. 39/2010)*

La norma è posta a tutela del corretto funzionamento della società.

Il reato – di natura dolosa – consiste nell'impedire od ostacolare, mediante occultamento di documenti con utilizzo di altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero il revisore legale.

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

La "condotta tipica" prevede che il reato si integra nel momento in cui con atti simulati o con frode si determini una maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto, maggioranza che non vi sarebbe stata qualora si fossero dedotti dai voti totali i voti illecitamente ottenuti.

**d) Tutela contro le frodi.**

✓ *Aggiotaggio (art. 2637 c.c.)*

La norma è posta a tutela contro le frodi, e prevede che chiunque diffonde notizie false ovvero pone in essere operazioni simulate o altri artifici,

concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari, sia punito con la reclusione.

#### **e) Tutela delle funzioni di vigilanza.**

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

La norma è posta a tutela delle funzioni di vigilanza.

*La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.*

Si tratta di un reato tipico la cui commissione è imputabile agli amministratori, direttori generali, sindaci e liquidatori di enti sottoposti per legge alle autorità pubbliche di vigilanza.

#### **f) Gli illeciti commessi mediante omissione**

- ✓ *Omessa comunicazione del conflitto di interessi (art. 2629-bis)*

Il reato si configura relativamente alle omissioni di comunicazioni rilevanti ai sensi dell'art. 2931 del C.C. in merito all'interesse portato dagli amministratori nelle operazioni societarie, in modo da permettere agli altri componenti il CdG e al Collegio Sindacale di valutare compiutamente le ragioni e la convenienza delle operazioni che si intendono effettuare.

- ✓ *Omessa esecuzione di denunce, comunicazioni, depositi (art. 2630) e omessa convocazione dell'assemblea (art. 2631)*

Tali reati prevedono sanzioni solo per coloro i quali commettono il reato e non prevedono pertanto alcuna responsabilità dell'ente.

#### **g) Operazioni realizzate dai liquidatori.**

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

Il reato – che può essere compiuto esclusivamente dai liquidatori – si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si osserva che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

#### **h) Corruzione tra privati (art. 2635 c.c.)**

L'articolo, come modificato dalla L. 190/12, sanziona al primo comma amministratori, direttori generali dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocimento alla società; il comma successivo sanziona – meno severamente – le stesse condotte qualora soggetto attivo sia invece chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti di cui al primo comma. Il terzo comma, sanziona la condotta di chi (soggetto "corruttore") da o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma; tale ipotesi, è l'unica ricompresa tra i reati presupposto; pertanto è sottoposto alla disciplina in tema di responsabilità ex D.Lgs. 231/01, solamente l'ente cui sia riconducibile il soggetto apicale o dipendente che ha posto in essere la condotta di corruzione.

### 3. Processi “sensibili” della Consorzio Depurazione del Savonese nell’ambito dei reati societari

Al fine di identificare i processi sensibili sono stati coinvolti i soggetti apicali della società con una metodologia composta dalle seguenti attività:

- identificazione reati previsti dal D.lgs. 231/01;
- valutazione del rischio riferito ad ogni reato all’interno dei processi aziendali determinandone l’applicabilità o meno per la società;
- identificazione dei processi sensibili sui quali si è valutata la gap analysis;
- documentazione delle attività svolta attraverso redazione di carte di lavoro.

I principali “processi sensibili” che Consorzio Depurazione del Savonese ha individuato al proprio interno sono i seguenti:

- ✓ *predisposizione delle comunicazioni a soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della Società (es. bilancio d’esercizio);*
- ✓ *gestione dei rapporti con il revisore legale in ordine all’attività di comunicazione da parte di quest’ultima a terzi relativa alla situazione economica, patrimoniale o finanziaria di Consorzio Depurazione del Savonese;*
- ✓ *operazioni relative al capitale sociale e destinazione dell’utile;*
- ✓ *gestione rapporti con soci e con il Consiglio di Sorveglianza;*
- ✓ *rapporti con Autorità di vigilanza;*
- ✓ *comunicazione, svolgimento e verbalizzazione delle Assemblee.*

Il Consiglio di gestione della Consorzio Depurazione del Savonese potrà disporre, qualora se ne ravvisi la necessità, ulteriori integrazioni dei suddetti “processi sensibili” definendo, se del caso, gli opportuni provvedimenti operativi.

## 4. Procedure adottate

### 4.1 Il sistema procedurale

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli amministratori, i dirigenti ed i dipendenti di Consorzio Depurazione del Savonese (e i consulenti nella misura necessaria alle funzioni dagli stessi svolte) devono in generale conoscere e rispettare:

- a) le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale ed organizzativa della società ed il sistema di controllo della gestione;
- b) il Codice Etico;
- c) le norme inerenti il sistema amministrativo, contabile, finanziario, di *reporting* della società;
- d) in generale, la normativa italiana e straniera applicabile.

A seguito della mappatura dei processi sensibili si è proceduto abbinando ad essi le relative procedure aziendali per descrivere ed identificare il sistema di controllo necessario a mitigare il rischio di commissione dei reati; Nello specifico si è operato come descritto di seguito:

- *formalizzazione delle procedure non ancora disponibili in azienda;*
- *collegamento tra processi sensibili ex D.Lgs. 231/01 e sottosistemi procedurali già attivi (es. sistema di controllo analogo, umbandling tariffario, ecc.).*

In tale modo si è prodotto un quadro di collegamento tra il Modello e le procedure aziendali che sono state messe a disposizione dell'Organismo di Vigilanza e che dovranno essere soggette a periodiche verifiche di conformità e di efficacia in relazione all'evoluzione normativa del D.Lgs. 231/01.

### 4.2 Principi generali di comportamento

I seguenti divieti di carattere generale si applicano al Presidente e ai componenti del CdG, dirigenti e dipendenti di Consorzio Depurazione del Savonese – in via diretta – ai consulenti, partner e società del Gruppo in forza di apposite clausole contrattuali.

E' fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino,

direttamente o indirettamente, le fattispecie di reato rientranti tra quelle riportate al precedente punto 2.

La presente Parte Speciale prevede, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società, l'espresso obbligo a carico dei soggetti sopra indicati di:

- a) *rispettare le norme di legge e le procedure aziendali interne in tutte le attività connesse alla formazione del bilancio e delle altre comunicazioni sociali tenendo un comportamento corretto, trasparente e collaborativo.*

Con riferimento al comportamento richiesto si specifica ulteriormente che è vietata:

- la rappresentazione o trasmissione di dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società per la redazione di bilanci, relazioni e prospetti o altre comunicazioni sociali e l'informativa societaria in genere;
  - l'omissione di dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società.
- b) *Osservare tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.*

Con riferimento al comportamento richiesto si specifica ulteriormente che è vietata:

- la restituzione di conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
  - la ripartizione di utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
  - l'acquisto o la sottoscrizione di azioni della società o di società controllate fuori dai casi previsti dalla legge, ledendo così l'integrità del capitale sociale;
  - l'effettuazione di operazioni di riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
  - l'effettuazione di aumenti (o formazione) fittizia del capitale sociale, attraverso l'attribuzione, in sede di aumento del capitale sociale, di azioni per un valore inferiore al loro valore nominale.
- c) *Assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione*

*sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.*

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di porre in essere comportamenti che impediscano o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte degli organi di controllo.

#### **4.3. Procedure specifiche generalmente applicabili**

Ai fini dell'attuazione delle regole elencate al precedente paragrafo 4.2, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del presente Modello, le procedure specifiche qui di seguito descritte per i singoli "processi sensibili":

- a) comunicazioni ai soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della società;
- b) gestione dei rapporti con il revisore legale;
- c) operazioni relative al capitale sociale.

*a) Comunicazioni ai soci e/o a terzi relative alla situazione economica, patrimoniale e finanziaria della società.*

Le comunicazioni aventi carattere di informativa finanziaria (quali ad esempio: il bilancio d'esercizio ed i comunicati) devono essere redatti in base alle specifiche procedure aziendali in essere ed in modo tale da:

- determinare con *chiarezza e completezza*:
  - i dati e le notizie che ciascuna funzione deve fornire;
  - i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;
- prevedere la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consenta:
  - la tracciatura dei singoli passaggi;
  - l'identificazione dei soggetti che inseriscono i dati nel sistema.

Al fine di garantire una completa applicazione delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- la predisposizione di un programma di formazione di base rivolto a tutti i responsabili delle funzioni coinvolte nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni e problematiche

giuridiche e contabili sul bilancio, curando, in particolare, sia la formazione dei neo assunti, sia l'effettuazione di corsi di aggiornamento periodici;

- l'istituzione di meccanismi idonei ad assicurare che le comunicazioni periodiche ai terzi siano redatte con il contributo di tutte le funzioni interessate al fine di assicurare la correttezza del risultato e la condivisione dello stesso. Tali meccanismi comprenderanno idonee scadenze, la definizione dei soggetti interessati, gli argomenti da trattare, i flussi informativi, il rilascio di apposite certificazioni.

*b) Gestione dei rapporti con il revisore legale.*

Nei rapporti tra Consorzio Depurazione del Savonese e revisore legale si sottolinea: l'impossibilità di attribuire incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile.

*c) Operazioni relative al capitale sociale.*

Tutte le operazioni sul capitale sociale di Consorzio Depurazione del Savonese e delle società da essa direttamente controllate, nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle procedure aziendali all'uopo predisposte.

## **5. I controlli dell'ODV**

I controlli dell'ODV consistono in un'attività di analisi dei rischi reato ex D.Lgs. 231/2001 secondo quanto previsto nel presente Modello Organizzativo.

A tal fine, all'ODV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Inoltre, l'ODV può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nel punto 4.2 della *"Parte Generale"*.

Durante la propria attività l'ODV dovrà mantenere la massima discrezione e riservatezza avendo come unici referenti gli Organi Sociali di cui al punto 4.3. della *"Parte Generale"*.

**PARTE SPECIALE III - Omicidio colposo e lesioni gravi o gravissime, commessi in violazione delle norme anti-infortunistiche e sulla tutela dell'igiene e della salute sul lavoro**

## 1. Destinatari della “Parte Speciale - III”

La presente Parte Speciale si riferisce ai comportamenti posti in essere dai datori di lavoro, dirigenti, preposti, lavoratori di Consorzio Depurazione del Savonese S.p.a., dalle altre figure disciplinate dal D. Lgs. n. 81/08 (ad es. Medico competente, Responsabile del Servizio di Prevenzione e Protezione, RLS etc.) e da ogni altra disposizione in materia di tutela della salute e sicurezza nei luoghi di lavoro, nonché dai consulenti di Consorzio Depurazione del Savonese S.p.a. e partners come individuati nella Parte Generale.

Più in dettaglio, i principali destinatari della normativa in materia di tutela della salute e sicurezza sul lavoro sono:

- Datore di lavoro: ovvero il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa (art. 2 co. 1 lett. b) D. Lgs. 81/08);

- Dirigente, ovvero la persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa (art. 2 co. 1 lett. d) D. Lgs. 81/08);

- Preposto, ovvero la persona che, in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa (art. 2 co. 1 lett. e) D. Lgs. 81/08);

- Lavoratore, ovvero la persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito di un'organizzazione del datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari;

- Medico competente, ovvero il medico in possesso di determinati titoli e requisiti professionali individuati dalla legge, che collabora con il datore di lavoro ai fini della valutazione dei rischi e della sorveglianza sanitaria;

- Responsabile del servizio di prevenzione e protezione, ovvero la persona in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del D.Lgs. n. 81/08 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi.

- I progettisti, i fabbricanti, i fornitori e gli installatori.

Di particolare rilievo sono altresì le attribuzioni previste in capo alla figura dei Rappresentanti dei lavoratori per la sicurezza, i quali intervengono nei casi e secondo le modalità previste dall'art. 50 del D.Lgs. n. 81/08.

In considerazione dell'attuale struttura aziendale la figura del "datore di lavoro" ex art. 2 lett. b) è stata assunta dal Presidente del CdG D.Lgs. 81/08, il quale ha onorato gli adempimenti di natura indelegabile previsti dall'art. 17 D.lgs. 81/08; si è inoltre provveduto a conferire, ricorrendo allo strumento della procura notarile, specifica delega di funzioni in materia di salute e sicurezza nei luoghi di lavoro in capo al direttore tecnico, il quale ha perciò assunto il ruolo di "datore di lavoro delegato" con relativi poteri e oneri.

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra indicati, adottino regole di condotta conformi a quanto prescritto dal D. Lgs. 81/08 e dal D. Lgs. 231/01 al fine di prevenire il verificarsi dei reati previsti dall'art. 25 septies del D. Lgs. n. 231/01.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- illustrare il sistema di gestione della salute e sicurezza nei luoghi di lavoro adottato da Consorzio Depurazione del Savonese S.p.a. e che dovrà essere osservato da parte dei datori di lavoro, dirigenti, preposti, lavoratori di Consorzio Depurazione del Savonese S.p.a., dalle altre figure disciplinate dal D. Lgs. n. 81/08, nonché da tutti gli altri partners di Consorzio Depurazione del Savonese S.p.a.;
- fornire all'ODV ed ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti per esercitare le attività di controllo, monitoraggio e verifica.

## 2. I reati relativi alla tutela della salute e sicurezza nei luoghi di lavoro (art. 25 septies del D. Lgs. 231/01)

L'art. 25 *septies* del D. Lgs. 231/01 prevede la responsabilità amministrativa delle persone giuridiche nel caso di commissione dei reati di omicidio colposo (art. 589 c.p.) e di lesioni colpose gravi o gravissime (art. 590 c.p.), commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Anche in relazione ai reati colposi, la responsabilità dell'ente si prefigura quando il reato sia stato commesso nell'interesse od a vantaggio dell'ente stesso. Nello specifico le Linee Guida di Confindustria precisano che tali requisiti, con riferimento ai reati di natura colposa, possono configurarsi nel risparmio di costi o di tempi che potrebbero derivare dall'aver omesso determinate misure prevenzionali.

Avuto particolare riguardo al delitto di lesioni colpose, giova precisare che la norma citata ha individuato profili di responsabilità per l'ente con riferimento alle sole fattispecie di lesioni personali gravi o gravissime, commesse in violazione delle norme poste a tutela della salute e sicurezza sul lavoro.

Sussiste una lesione personale grave (art. 583, comma 1 c.p.) quando:

- a) dalla stessa sia derivata una malattia che abbia messo in pericolo la vita della persona offesa;
- b) dalla stessa sia derivata una malattia o incapacità di attendere alle proprie occupazioni per un tempo superiore a 40 giorni;
- c) la lesione abbia prodotto un indebolimento permanente di un senso o di un organo.

Sussiste una lesione personale gravissima (art. 583, comma 2 del c.p.):

- a) se dal fatto deriva una malattia certamente o probabilmente insanabile;
- b) se vi è la perdita di un senso;
- c) se dal fatto deriva la perdita di un arto, o una mutilazione che renda l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una grave e permanente difficoltà nell'eloquio;
- d) se dal fatto deriva la deformazione ovvero lo sfregio permanente del viso.

L'art. 2, comma 1, let. dd) del D. Lgs. n. 81/08 (Testo Unico in materia di tutela della salute e sicurezza sul lavoro) definisce il Modello di Organizzazione e Gestione in materia di salute e sicurezza sul lavoro come il "*modello organizzativo e gestionale per la definizione e l'attuazione di una politica aziendale per la salute e sicurezza, ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8*

*giugno 2001, n. 231, idoneo a prevenire i reati di cui agli articoli 589 e 590, comma 3, del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro*".

Nello specifico e sempre in relazione alla disciplina della responsabilità degli enti ai sensi del D. Lgs. 231/01, l'art. 30 del "Testo Unico in materia di tutela della salute e sicurezza sul lavoro" prescrive le modalità per assicurare un corretto sistema di organizzazione e gestione aziendale adempiente a tutti gli obblighi giuridici relativi:

*"a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici, e biologici;*

*b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;*

*c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;*

*d) alle attività di sorveglianza sanitaria;*

*e) alle attività di informazione e formazione dei lavoratori;*

*f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;*

*g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;*

*h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.*

*2. il modello organizzativo e gestionale di cui al comma 1, deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.*

*3. il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.*

*4. il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.*

*5. in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e*

*sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6.*

*6. l'adozione del modello di organizzazione e di gestione di cui al presente articolo nelle imprese fino a 50 lavoratori rientra tra le attività finanziabili ai sensi dell'articolo 11."*

*Delitti di omicidio colposo e di lesioni colpose gravi o gravissime, conseguenti a violazione delle norme in tema di salute e sicurezza nei luoghi di lavoro.*

Come già esplicitato, i reati colposi che possono coinvolgere la responsabilità amministrativa di Consorzio Depurazione del Savonese S.p.a. ai sensi del D. Lgs. 231/01 sono i delitti di omicidio colposo e di lesioni personali colpose gravi o gravissime commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro, per i quali l'art. 25-septies D.Lgs 231/01, così come modificato dall'articolo 300 del "Testo Unico in materia di tutela della salute e sicurezza sul lavoro", stabilisce che:

*- "In relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 123 del 2007 in materia di salute e sicurezza nel lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.*

*- Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.*

*- In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'art. 9, comma 2, per una durata non superiore a sei mesi.*

Si riportano gli articoli del codice penale richiamati dall'art. 25-septies del D. Lgs. n. 231/01:

a) *Art. 589 Codice Penale: Omicidio Colposo.* 1. Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. 2. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni. 3. Si applica la pena da tre a dieci anni se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale da: 1) soggetto in stato di ebbrezza alcolica ai sensi dell'art. 186, comma 2, lett. c), del decreto legislativo 30 aprile 1992 n. 285, e successive modificazioni; 2) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope. 4. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici".

b) *Art. 590 codice penale: Lesioni personali colpose.* 1. Chiunque cagiona ad altri per colpa una lesione personale è punito con la reclusione fino a tre mesi o con la multa fino a euro 309. 2. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima (c.p. 583), della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239. 3. Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena per le lesioni gravi è della reclusione da tre mesi a un anno o della multa da euro 500 a euro 2.000 e la pena per lesioni gravissime è della reclusione da uno a tre anni. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'art. 186 comma 2 lett. c) del decreto legislativo 30 aprile 1992 n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni. 4. Nel caso di lesioni di più persone si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse, aumentata fino al triplo, ma la pena della reclusione non può superare gli anni cinque. 5. Il delitto è punibile querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale".

c) *Art. 583 codice penale. Circostanze aggravanti.* "La lesione personale è grave: 1. se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni; 2. se il fatto produce l'indebolimento permanente di un senso o di un organo; La lesione personale è gravissima ...se dal fatto deriva: 1. una malattia certamente o probabilmente insanabile; 2. la perdita di un senso; 3. la perdita di un arto, o una mutilazione che renda l'arto inservibile,

ovvero la perdita dell'uso di un organo o della capacità di procreare, ovvero una permanente e grave difficoltà della favella; 4. la deformazione, ovvero lo sfregio permanente del viso.

Ai sensi dell'art. 43 c.p. (Elemento psicologico del reato) "Il delitto: ... è colposo, o contro l'intenzione quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline".

Nelle ipotesi di reato indicate dalla norma richiamata, il legislatore ha altresì previsto la possibilità di applicazione delle sanzioni interdittive di cui all'articolo 9 comma 2 D. Lgs. n. 231/01.

### **3. Processi sensibili e definizione del modello di organizzazione ex art. 30 D.Lgs. 81/08.**

Al fine di identificare i processi sensibili sono stati coinvolti i soggetti apicali della società con una metodologia composta dalle seguenti attività:

- identificazione reati previsti dal D.lgs. 231/01;
- valutazione del rischio riferito ad ogni reato all'interno dei processi aziendali determinandone l'applicabilità o meno per la società;
- identificazione dei processi sensibili sui quali si è valutata la gap analysis;
- documentazione delle attività svolta attraverso redazione di carte di lavoro.

La costruzione del Modello ex art. 30 D.Lgs. 81/08, in conformità alle Linee Guida di Confindustria, si è svolta mediante:

#### A) individuazione degli ambiti aziendali di attività;

- introduzione attrezzature di lavoro;
- manutenzione attrezzature di lavoro;
- gestione dispositivi di protezione individuale;
- gestione attività di informazione, formazione ed addestramento;
- agenti chimici;
- agenti fisici (rumore, radiazioni ottiche)
- agenti biologici
- gestione sorveglianza sanitaria e prescrizioni;
- gestione appalti e Duvri;
- riunione periodica;
- consultazione RLS;
- gestione attività di vigilanza da parte dei preposti;
- verifiche obbligatorie;
- gestione emergenze;

L'attività si è sviluppata attraverso interviste ai soggetti coinvolti nel sistema di gestione ed organizzazione della salute e sicurezza dei lavoratori nonché attraverso l'acquisizione di documentazione rilevante a tale fine;

#### B)analisi dei rischi potenziali; output di fase: potenziali modalità attuative degli illeciti.

In merito si premette innanzitutto che riguardo al rischio di comportamenti integranti i reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme di tutela della salute e sicurezza del lavoro, l'analisi del Modello deve necessariamente estendersi alla totalità delle aree/attività aziendali.

Ciò premesso, l'analisi delle possibili modalità attuative dei reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione degli obblighi di tutela della salute e sicurezza sul lavoro, corrisponde alla valutazione dei rischi lavorativi effettuata secondo i criteri previsti dall'art. 28 del D. Lgs. 81/08 e dalle altre disposizioni normative e regolamentari aventi lo stesso oggetto e profilo.

### **3.1 Il sistema procedurale**

Le attività di Consorzio Depurazione del Savonese sono gestite nel pieno rispetto della normativa vigente in materia di prevenzione e protezione dai rischi professionali. La gestione operativa, governata anche con il contributo di alcune specifiche procedure ed istruzioni operative, è improntata a criteri di salvaguardia ambientale e di efficienza perseguendo il miglioramento delle condizioni di salute e di sicurezza sul lavoro.

A seguito della mappatura dei processi sensibili si è proceduto abbinando ad essi le relative procedure aziendali. Nello specifico si è operato collegando i processi sensibili ex D.Lgs. 231/01 con il sottosistema procedurale già attivato per ottemperare al D.Lgs. 81/08 e di seguito rappresentato. In tale modo si è prodotto un quadro di collegamento tra il Modello e le procedure aziendali che sono state messe a disposizione dell'Organismo di Vigilanza e che dovranno essere soggette a periodiche verifiche di conformità e di efficacia in relazione all'evoluzione normativa del D.Lgs. 231/01.

Il Consorzio Depurazione del Savonese S.p.a. garantisce il corretto adempimento degli obblighi in materia di tutela della salute e sicurezza nei luoghi di lavoro previsti dal D. Lgs. n. 81/08 e, in particolare, gli obblighi relativi a:

1. rispetto degli standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
2. attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
3. attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
4. attività di sorveglianza sanitaria;
5. attività di informazione e formazione dei lavoratori;
6. attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

7. acquisizione di documentazioni e certificazioni obbligatorie per legge;
8. periodiche verifiche dell'applicazione e dell'efficacia delle procedure applicate.

I destinatari del presente Modello devono scrupolosamente garantire il rispetto delle prescrizioni e delle procedure dallo stesso previste; i lavoratori, inoltre, sono tenuti a rispettare gli obblighi dell'art. 20 del D. Lgs. n.81/08.

In virtù delle suddette prescrizioni normative i dipendenti devono tra l'altro osservare le disposizioni e le istruzioni impartite ai fini della protezione collettiva ed individuale.

I Lavoratori sono chiamati a utilizzare correttamente le apparecchiature, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza in modo appropriato. Debbono altresì segnalare le deficienze dei mezzi, dispositivi e apparecchiature nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli.

I dipendenti non devono rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo, non devono compiere di propria iniziativa operazioni o attività che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori.

### **3.2 Il Responsabile**

Consorzio Depurazione del Savonese, inoltre, ponendosi come obiettivo la tutela della sicurezza e salute, promuove i principi in materia di tutela della salute e sicurezza nei luoghi di lavoro enunciati nel "Codice Etico" di Consorzio Depurazione del Savonese.

In relazione a diverse aree di rischio identificate, si è provveduto ad individuare modalità comportamentali assunte quali procedure/istruzioni nel sistema di controllo aziendale.

Nelle suddette procedure/istruzioni vengono previsti scopo e campo di applicazione, compiti e responsabilità, modalità operative, documenti richiamati per la realizzazione delle attività e per l'effettuazione delle necessarie verifiche.

L'RSPP provvede inoltre alla verifica dei documenti attestanti l'attività svolta e provvede ad emettere periodico report di verifica sull'attuazione effettiva delle procedure/istruzioni, sulla loro efficacia e sulle misure eventualmente suggerite per il miglioramento dell'attività in oggetto. Il report emesso dall'RSPP verrà inviato all'OdV.

E' previsto altresì un corretto sistema di archiviazione di tutti i dati e le informazioni raccolte a cura del Servizio di Prevenzione e Protezione, onde garantire altresì all'OdV di poter correttamente espletare le proprie funzioni di controllo.

La società ha adottato un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure e procedure indicate nel Modello, in ottemperanza alle disposizioni di cui all'art. 30 co. 3 del D. Lgs. 81/08, così come previsto nel punto 7 della Parte Generale.

Le inosservanze alle prescrizioni, alle procedure ed agli obblighi richiamati viene col presente Modello sanzionata con il ricorso agli opportuni provvedimenti disciplinari (cfr. Parte Generale punto 6).

Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

#### **4. I controlli dell'ODV**

I controlli dell'ODV consistono in un'attività di analisi dei rischi reato ex D.Lgs. 231/2001 secondo quanto previsto nel presente Modello Organizzativo.

A tal fine, all'ODV viene garantito libero accesso a tutta la documentazione aziendale rilevante.

Inoltre, l'ODV può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nel punto 4.2-4.3 della "Parte Generale".

Qualora dovessero emergere problematiche di rilievo nell'applicazione del sistema sopra indicato tali da suggerire una rielaborazione dello stesso, sarà cura dell'OdV, anche su segnalazione dei datori di lavoro, dei dirigenti delegati e/o dell'RSPP, darne tempestiva comunicazione al CdG, al Consiglio di Sorveglianza proponendo le soluzioni opportune per una eventuale adeguata revisione del Modello.

Durante la propria attività l'ODV dovrà mantenere la massima discrezione e riservatezza avendo come unici referenti gli Organi Sociali di cui al punto 5.3. della "Parte Generale".

**PARTE SPECIALE IV - Reati ambientali di cui all' art. 25  
undecies del D.Lgs. 231/01**

## 1. Destinatari della “Parte Speciale IV”

La presente Parte Speciale del Modello di Organizzazione e Gestione si rivolge al Presidente e ai componenti del CdG, ai dirigenti e ai dipendenti Consorzio Depurazione del Savonese che operano nell’ambito delle attività e/o processi sensibili individuati ai sensi della presente Parte Speciale, nonché a tutti coloro che, anche in virtù di vincoli contrattuali (appaltatori, consulenti, partners, ecc.), intrattengono rapporti con Consorzio Depurazione del Savonese inerenti profili di gestione ambientale.

L’obiettivo della Presente Parte Speciale è dunque di far sì che tutti i destinatari del Modello, nell’ambito delle attività e/o dei processi sensibili come individuati adottino, nei limiti dei propri compiti e delle connesse responsabilità, regole di condotta conformi ai principi contenuti nel Modello (sia nella Parte Generale che nella presente Parte Speciale) e nel Codice Etico al fine di prevenire la commissione dei reati considerati rilevanti ai sensi dell’articolo 25 *undecies* del Decreto.

In particolare, la presente Parte Speciale ha lo scopo di:

1) indicare le “regole di comportamento” e le procedure che i destinatari del Modello (Presidente e i componenti del CdG, dirigenti, dipendenti, organi sociali, consulenti e collaboratori esterni) sono tenuti ad osservare al fine di una corretta ed efficace applicazione del Modello stesso;

2) fornire all’OdV ed alle funzioni aziendali che con lo stesso collaborano, gli strumenti effettivi per lo svolgimento delle attività di vigilanza, controllo e monitoraggio sull’applicazione del Modello.

## **2. I reati ambientali (art. 25 undecies del D.Lgs. 231/01).**

E' opportuno innanzitutto premettere che, in considerazione della peculiare struttura della disciplina in tema di tutela dell'ambiente, sia essa contenuta nel D.Lgs. 152/2006 (c.d. Testo Unico Ambientale), ovvero in differenti provvedimenti legislativi, disciplina connotata da una notevole complessità tecnica, si è ritenuto di limitarsi in questa sede ad una sintetica disamina delle singole condotte rilevanti ai sensi del Decreto con esclusione di quelle la cui irrilevanza con riferimento alla realtà di Consorzio Depurazione del Savonese può ritenersi di immediata evidenza (*reati in materia di inquinamento provocato dalle navi ex D. Lgs. 202/07, reati in materia di commercio internazionale delle specie animali e vegetali in via di estinzione ex Legge 150/92 e violazione dei divieti di scarico (sversamento) in mare di sostanze e/o materiali inquinanti da navi ed aeromobili stabiliti da convenzioni internazionali ratificate dall'Italia*).

### **Disciplina delle acque di cui al Testo Unico Ambientale (D.Lgs. 152/06)**

L'articolo 25 *undecies* del Decreto include nel novero dei reati-presupposto alcune delle ipotesi contravvenzionali di cui all'art. 137 T.U.A. ed in particolare:

- (art. 137 co.5 primo periodo TUA): superamento, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza TUA, nell'effettuazione di uno scarico di acque reflue industriali, dei valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, dei valori limite fissati nella tabella 4 dell'Allegato 5 parte III, oppure superamento dei limiti più restrittivi fissati dalle Regioni, dalle province autonome o dall'autorità d'ambito (sanzione pecuniaria da 150 a 250 quote)
- (art. 137 co.2 TUA): apertura o effettuazione di nuovi scarichi in assenza della prescritta autorizzazione ovvero continuazione o mantenimento di detti scarichi dopo la revoca o la sospensione dell'autorizzazione medesima, quando dette condotte riguardano gli scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del TUA (sanzione pecuniaria da 200 a 300 quote e sanzioni interdittive di cui all'art. 9 co.2 D. Lgs. 231/01 per una durata non superiore a sei mesi)
- (art. 137 co.5 secondo periodo TUA): supero, in relazione alle sostanze di cui alla tabella 5, Allegato 5, Parte III del TUA - nell'effettuazione di uno scarico di acque reflue industriali - dei valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5, Parte III, ovvero dei valori più restrittivi fissati dalle Regioni, dalle Province autonome e dalle Autorità d'ambito, con riferimento anche ai valori limite fissati per le sostanze contenute nella tabella

- 3/A del medesimo Allegato 5 (sanzione pecuniaria da 200 a 300 quote e sanzioni interdittive di cui all'art. 9 co.2 D. Lgs. 231/01 per una durata non superiore a sei mesi).
- (art. 137 co.11 TUA): violazione dei divieti di scarico individuati dagli artt. 103 e 104 TUA, i quali stabiliscono in generale il divieto di scarico sul suolo o negli strati superficiali del sottosuolo (art. 103), nel sottosuolo o nelle acque sotterranee, fatte salve alcune eccezioni quali le fognature statiche al servizio di piccoli insediamenti e case isolate di cui all'art. 100 co.3, gli scarichi che provengono dal lavaggio di sostanze minerali ecc. (art. 103) ovvero, in presenza di apposita autorizzazione, lo scarico di acque provenienti dal processo di estrazione degli idrocarburi, dal lavaggio o dalla lavorazione degli inerti ecc. (sanzione pecuniaria da 200 a 300 quote e sanzioni interdittive di cui all'art. 9 co.2 D. Lgs. 231/01 per una durata non superiore a sei mesi).

#### **Disciplina dei rifiuti di cui al Testo Unico Ambientale (D.Lgs. 152/06)**

L'articolo 25 *undecies* del Decreto prevede le seguenti ipotesi:

- con riferimento all'art. **256 TUA**:
  - ✓ (art. 256 co.1 lett. a TUA): svolgimento di attività connesse con la gestione di rifiuti non pericolosi in assenza dell'autorizzazione, iscrizione e/o comunicazione prescritte agli artt. 208-216 D. Lgs. 152/06; in particolare, la norma elenca una serie di attività quali la raccolta, il recupero, il trasporto, lo smaltimento, il commercio e l'intermediazione (sanzione pecuniaria fino a 250 quote).
  - ✓ (art. 256 co.6 primo periodo TUA): deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, in violazione delle disposizioni di cui all'art. 227 TUA (sanzione pecuniaria fino a 250 quote).
  - ✓ (art. 256 co.1 lett. b TUA): svolgimento di attività connesse con la gestione di rifiuti pericolosi in assenza dell'autorizzazione, iscrizione e/o comunicazione prescritte agli artt. 208-216 del D. Lgs. 152/06; in particolare, la norma elenca una serie di attività quali la raccolta, il recupero, il trasporto, lo smaltimento, il commercio e l'intermediazione (sanzione pecuniaria da 150 a 250 quote).
  - ✓ (art. 256 co.3 primo periodo TUA): realizzazione o gestione di discarica non autorizzata (sanzione pecuniaria da 150 a 250 quote).
  - ✓ (art. 256 co.5 TUA): attività non consentite di miscelazione di rifiuti - in violazione del disposto dell'art. 187, che stabilisce il divieto di miscelare diverse categorie di rifiuti pericolosi o rifiuti pericolosi con rifiuti non pericolosi - in modo da dare origine ad una miscela per cui non è previsto

uno specifico codice identificativo; fatte salve alcune eccezioni che possono essere autorizzate qualora siano rispettate le condizioni di cui all'art. 178 co.2, secondo cui la gestione dei rifiuti è effettuata conformemente ai principi di precauzione, di prevenzione, di sostenibilità, di proporzionalità, di responsabilizzazione e di cooperazione di tutti i soggetti coinvolti nella produzione, nella distribuzione, nell'utilizzo e nel consumo di beni da cui originano i rifiuti, nonché del principio "chi inquina paga" (sanzione pecuniaria da 150 a 250 quote).

- ✓ (art. 256 co.3 secondo periodo TUA): realizzazione o gestione di discarica non autorizzata qualora la condotta abbia ad oggetto, anche in parte, rifiuti pericolosi (sanzione pecuniaria da 200 a 300 quote e sanzioni interdittive di cui all'art. 9 co.2 D. Lgs. 231/01 per una durata non superiore a sei mesi).
- ✓ (art. 256 co.4 TUA): inosservanza, con riferimento alla gestione di una discarica o ad altre attività concernenti i rifiuti, delle prescrizioni autorizzative ovvero carenza dei requisiti e condizioni richiesti per le iscrizioni o comunicazioni (sanzione pecuniaria prevista per i reati di cui all'art. 256 commi 1 e 3 ridotta della metà).
- con riferimento all'art. **257 TUA**:
  - ✓ la condotta di chi cagioni l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (CSR) senza provvedere, successivamente all'inquinamento, alla bonifica del sito inquinato in conformità al progetto approvato secondo il procedimento di cui all'art. 242 TUA; il secondo periodo della norma punisce la condotta di chi, provocando un evento potenzialmente in grado di contaminare un sito, ometta di effettuare l'immediata comunicazione alle autorità competenti di cui all'art. 242 TUA (sanzione pecuniaria fino a 250 quote).
  - ✓ il secondo comma dell'art. 257 TUA punisce - con pena più severa - le stesse condotte di cui al precedente punto a) quando l'inquinamento è provocato da sostanze pericolose (sanzione pecuniaria da 150 a 250 quote).
  - ✓ del successivo articolo 258 TUA rientra, quale reato-presupposto, la sola ipotesi del comma 4 che punisce con la pena prevista per il reato di falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.) chiunque fornisca false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un

certificato di analisi di rifiuti e chiunque faccia uso di un certificato falso durante il trasporto (sanzione pecuniaria da 150 a 250 quote).

- ✓ l'art. 259 TUA sanziona chiunque effettui una spedizione di rifiuti costituente traffico illecito ai sensi dell'art. 26 del regolamento CEE 259/1993 (ora art. 2 co.35 regolamento CEE 1013/2006), ovvero traffico illecito transfrontaliero (sanzione pecuniaria da 150 a 250 quote).
- ✓ l'art. 260 TUA sanziona l'attività di cessione, ricevimento, trasporto, esportazione, importazione, o comunque gestione abusiva di ingenti quantitativi di rifiuti al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate (sanzione pecuniaria da 300 a 500 quote - ovvero da 400 a 800 nel caso in cui le suddette attività riguardino rifiuti ad alto contenuto radioattivo - e sanzioni interdittive di cui all'art. 9 co.2 D. Lgs. 231/01 per una durata non superiore a sei mesi).

A norma del disposto di cui all'art. 25 undecies co.8 D.Lgs. 231/01, *“se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione dei reati di cui all'art. 260 D.Lgs. 152/06 e all'art. 8 D.Lgs. 202/07, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16 co.3 D.Lgs. 231/01”*.

- con riferimento all'art. **260 bis TUA**:

- ✓ (art. 260 bis co. 6 TUA): predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, recante false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti ovvero inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (sanzione pecuniaria da 150 a 250 quote).
- ✓ (art. 260 bis co.7 secondo periodo TUA): condotta del trasportatore che, con riferimento a rifiuti pericolosi, omette di accompagnare il trasporto con la copia cartacea della scheda di movimentazione SISTRI e, se necessario, con la copia del certificato analitico (sanzione pecuniaria da 150 a 250 quote).
- ✓ (art. 260 bis co.7 terzo periodo TUA): condotta del trasportatore che durante il trasporto fa uso di un certificato di analisi dei rifiuti contenente false indicazioni sulla natura, composizione, e/o caratteristiche chimico-fisiche dei rifiuti trasportati (sanzione pecuniaria da 150 a 250 quote).
- ✓ (art. 260 bis co.8 TUA): trasporto di rifiuti da parte del trasportatore con una copia cartacea della scheda SISTRI - Area Movimentazione

fraudolentemente alterata (sanzione pecuniaria da 150 a 250 quote ovvero da 200 a 300 se il trasporto riguarda rifiuti pericolosi).

#### **Disciplina delle emissioni di cui al Testo Unico Ambientale (D.Lgs. 152/06)**

L'art. 25 *undecies* prevede nel novero dei reati-presupposto anche la fattispecie di cui all'art. 279 co. 5 D. Lgs. 152/06.

In particolare, è sanzionata la violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione o delle prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla Parte V del D. Lgs. 152/06, dai piani e dai programmi o dalla normativa di cui all'art. 271 D. Lgs. 152/06 o dalle prescrizioni altrimenti imposte dall'autorità competente o come stabiliti nell'autorizzazione integrata ambientale, quando il suddetto superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa (sanzione pecuniaria da 150 a 250 quote).

#### **Reati-presupposto in materia ambientale disciplinati dal Codice Penale a tutela dell'habitat e delle specie animali e vegetali selvatiche protette.**

A seguito della valutazione del management aziendale, tale fattispecie appare non applicabile al Consorzio Depurazione Acque Savonese.

#### **Reati in materia di impiego di sostanze nocive per l'ozono ex Legge 549/93.**

L'art. 3 co. 6 L. 549/93 punisce la violazione delle disposizioni sull'impiego delle sostanze nocive per lo strato di ozono (sanzioni pecuniarie da 150 a 250 quote).

Anche con riferimento alle fattispecie ambientali sopra richiamate rilevanti quali reati - presupposto ai sensi del D.Lgs. 231/01, la responsabilità della Società può configurarsi, a norma del disposto di cui all'art. 5 D. Lgs. 231/01, esclusivamente nell'ipotesi in cui il reato sia stato commesso nell'interesse (*il fine in vista del quale il soggetto ha posto in essere la condotta illecita e la cui sussistenza viene accertata con una valutazione ex ante, a prescindere dagli esiti della condotta delittuosa posta in essere*) e vantaggio (*l'oggettiva realizzazione di un profitto direttamente in capo all'Ente e la cui sussistenza viene accertata con una valutazione ex post tenendo conto degli effetti favorevoli per la Società derivanti dal reato commesso con particolare riferimento alla concreta acquisizione di un'utilità economica*) dell'ente.

Le nozioni di *interesse* e *vantaggio*, originariamente previste solo per reati dolosi, hanno suscitato difficoltà interpretative e/o applicative quanto alla loro riferibilità anche ai reati colposi qual è la maggior parte di quelli oggetto della

presente Parte Speciale, ciò con specifico riferimento alla concreta individuazione del possibile interesse e vantaggio dell'Ente.

Secondo le prime interpretazioni dottrinali (cfr. Relazione al D.Lgs. 121/11 dell'Ufficio del Massimario presso la Corte Suprema di Cassazione) *“la scelta di non riconfigurare i summenzionati parametri di imputazione e la circostanza che la maggior parte dei nuovi reati presupposto selezionati siano delle contravvenzioni, la cui condotta tipica è indifferentemente sorretta dal dolo e dalla colpa, potrebbe dover essere letta come indice della volontà del legislatore di interpretare il concetto di interesse in senso oggettivo e di correlare quest'ultimo, per l'appunto, alla condotta tenuta dall'agente qualificato nell'ambito dell'attività svolta per conto dell'ente”*.

L'elaborazione di un criterio di interesse in senso oggettivo sembra riconducibile a quanto già affermato sul punto in sede giurisprudenziale con riferimento ai reati colposi di omicidio e lesioni personali commessi con violazione della disciplina sulla salute e sicurezza nei luoghi di lavoro di cui all'art. 25 septies D.lgs. 231/01.

In particolare, secondo tale giurisprudenza la responsabilità dell'ente non dipenderebbe dalla direzione volontaristica attribuita alla condotta da parte dell'agente, essendo sufficiente che il reato sia connesso ad un *“obbiettivo riconducibile alla politica di impresa”* (cfr. Tribunale di Trani, sez. dist. di Molfetta, 11.01.10).

Con riferimento al criterio dal vantaggio, la medesima giurisprudenza ha ritenuto che *“esso può essere ravvisato laddove il soggetto agisca per conto dell'ente, con sistematiche violazioni di norme cautelari così da far rientrare quella condotta nella politica di impresa volta alla svalutazione della gestione in materia di sicurezza, con conseguente abbattimento dei costi e spese per l'adozione e l'attuazione dei presidi antinfortunistici, nonché ottimizzazione dei profitti”*.

Tale interpretazione è stata fatta propria anche dalle citate Linee Guida di Confindustria secondo le quali, proprio con riferimento ai reati di natura colposa ex art. 25 septies D.Lgs. 231/01 l'interesse o vantaggio dell'Ente può configurarsi nel risparmio di costi e/o di tempi che potrebbero discendere dall'omessa adozione delle misure prevenzionali la cui mancanza ha causato la commissione del reato stesso.

Secondo tali interpretazioni la Società potrà quindi essere chiamata a rispondere, ai sensi del D. Lgs. 231/01, delle violazioni delle richiamate norme in materia di tutela ambientale individuandone l'interesse e vantaggio nel risparmio dei relativi costi.

### **3. Processi “sensibili” della Consorzio Depurazione del Savonese nell’ambito dei reati ambientali.**

Al fine di identificare i processi sensibili sono stati coinvolti i soggetti apicali della società con una metodologia composta dalle seguenti attività:

- identificazione reati previsti dal D.lgs. 231/01;
- valutazione del rischio riferito ad ogni reato all’interno dei processi aziendali determinandone l’applicabilità o meno per la società;
- identificazione dei processi sensibili sui quali si è valutata la gap analysis;
- documentazione delle attività svolta attraverso redazione di carte di lavoro.

Consorzio Depurazione del Savonese attualmente svolge attività inerenti il trattamento e la depurazione di acque reflue da uso domestico e industriale, la gestione di un impianto di rifiuti liquidi industriali non pericolosi e la manutenzione delle reti fognarie di alcuni comuni azionisti.

Stante la particolare tipologia di attività svolta da Consorzio Depurazione del Savonese, risulta di primaria importanza l’individuazione ed identificazione delle aree e processi sensibili nell’ambito dei quali sussiste un concreto rischio di commissione di alcune delle fattispecie previste dall’art. 25undecies del Decreto (soprattutto in materia di disciplina in tema di inquinamento idrico e di rifiuti).

Nell’ambito del Consorzio Depurazione Savonese sono emerse le seguenti aree a rischio/attività sensibili:

- individuazione dei soggetti responsabili in materia ambientale e dei relativi poteri/doveri, nonché dei soggetti/figure aziendali destinatari di incarichi, istruzioni operative, comunicati e comunicazioni organizzative, adempimenti, obblighi di vigilanza;
- pianificazione/programmazione aziendale ed economica con specifico riferimento alla tematica ambientale;
- verifica e manutenzione di impianti/stabilimenti/macchinari/immobili e infrastrutture;
- informazione/formazione degli apicali e delle altre figure interessate;
- documentazione e diffusione delle direttive e delle procedure in tema ambientale;
- verifica del rispetto di piani, programmi, istruzioni, direttive, procedure;
- rilevazione e comunicazione di eventuali criticità;

- verifica dei requisiti di idoneità tecnico- professionale degli appaltatori nonché del loro rispetto della politica aziendale in materia ambientale in caso di affidamento di lavori/servizi in appalto;
- interferenza dei siti/impianti con Zone di protezione speciale /Siti di interesse comunitario ai sensi delle direttive 2009/147/CE e 93/43/CE o in territori confinanti;
- gestione delle acque reflue e degli scarichi;
- gestione delle emergenze quali, ad esempio, incendi e/o sversamenti;
- gestione dei processi autorizzativi e/o di altri adempimenti amministrativi, anche in caso di apertura di nuovi impianti e/o modifica degli stessi;
- presenza di vasche, serbatoi interrati e dei sistemi di contenimento in caso di fuoriuscite e/o sversamenti;
- gestione dei rifiuti, con particolare riferimento alla loro caratterizzazione;
- rapporti con i trasportatori e verifica dei loro requisiti;
- rapporti con recuperatori/smaltitori e verifica dei loro requisiti;
- gestione dei registri e dei formulari in tema di rifiuti;
- gestione del sistema SISTRI;
- presenza di punti di emissione emissioni derivanti dagli impianti di deodorizzazione, dall'utilizzo di caldaie a gas naturale, gasolio e dal riscaldamento dei luoghi lavorativi;
- presenza di impianti che possono interessare la disciplina di cui al D. Lgs. 152/06;
- attività di gestione degli impianti di depurazione

All'esito dell'attività di mappatura sono state ritenute in ipotesi realizzabili nell'esercizio dell'attività sociale di Consorzio Depurazione del Savonese le fattispecie di reato presupposto elencate nel paragrafo n. 2 della Presente Parte Speciale.

Pare invece possibile escludere la sussistenza del rischio di commissione relativamente alle seguenti ipotesi di reato presupposto.

- reati in materia di inquinamento provocato dalle navi ex D. Lgs. 202/07;
- reati in materia di commercio internazionale delle specie animali e vegetali in via di estinzione ex Legge 150/92.

### **3.1 Principi generali di comportamento.**

Di seguito vengono individuati precisi divieti di carattere generale, che dovranno essere rispettati dal Presidente e dai componenti del CdG, dai Dirigenti, dai Dipendenti Consorzio Depurazione del Savonese e da tutti coloro che sono tenuti al rispetto del Modello, anche eventualmente in virtù di specifiche clausole contrattuali.

In via generale è fatto divieto di porre in essere, partecipare o dare causa a comportamenti idonei ad integrare le fattispecie rilevanti previste dall'art. 25 undecies del Decreto in materia di tutela dell'ambiente e del territorio, ed in particolare:

- violare i principi dettati nel Codice Etico nonché le regole contenute e richiamate nel Modello (Parte Generale e Parti Speciali);
- violare la disciplina normativa di settore, con particolare riferimento alla disciplina in tema di inquinamento idrico e gestione dei rifiuti;
- violare le prescrizioni dettate da eventuali provvedimenti autorizzativi, dalle disposizioni di legge vigenti inerenti la disciplina ambientale, dalle prescrizioni dell'autorità di vigilanza;
- violare le prescrizioni imposte dalla normativa in relazione al sistema SISTRI se ed in quanto vigente;
- porre in essere, partecipare o dare causa a comportamenti che, individualmente o collettivamente, siano suscettibili di arrecare un danno all'ambiente;
- omettere di verificare i requisiti di idoneità e professionalità dei soggetti cui sono affidati incarichi inerenti la materia ambientale;
- omettere di vigilare sull'operato dei soggetti di cui al punto precedente.

Le inosservanze degli obblighi, delle procedure o delle disposizioni organizzative emanate così come richiamate dal presente Modello vengono sanzionate con il ricorso agli opportuni provvedimenti disciplinari, come previsto nel punto 6 della Parte Generale del Modello.

## **4. Procedure adottate.**

### **4.1 Il sistema procedurale**

In linea generale il sistema di organizzazione della Società rispetta i requisiti fondamentali di formalizzazione e chiarezza nella comunicazione e nella separazione dei ruoli delle diverse funzioni aziendali, ciò con specifico riferimento alle attribuzioni di responsabilità e di rappresentanza della Società

A seguito della mappatura dei processi sensibili si è proceduto abbinando ad essi le relative procedure aziendali. Nello specifico si è operato collegando i processi sensibili ex D.Lgs. 231/01 con il sottosistema procedurale già attivato per ottemperare al sistema di certificazione ambientale e di seguito rappresentato. In tale modo si è prodotto un quadro di collegamento tra il Modello e le procedure aziendali che sono state messe a disposizione dell'Organismo di Vigilanza e che dovranno essere soggette a periodiche verifiche di conformità e di efficacia in relazione all'evoluzione normativa del D.Lgs. 231/01.

In particolare è stato individuato nella persona del Direttore Tecnico, mediante delega di funzioni attribuita con idonea procura notarile, il soggetto responsabile cui fanno capo specifici poteri e doveri anche di carattere organizzativo (quali, tra gli altri, individuazione e predisposizione di procedure, comunicati e comunicazioni organizzative, istruzioni operative) volti ad assicurare il puntuale rispetto di ogni adempimento in materia ambientale, comprese le previsioni della presente Parte Speciale.

Di conseguenza, le funzioni/figure aziendali di Consorzio Depurazione del Savonese interessate alle attività considerate a rischio di commissione dei reati di cui all'art. 25undecies del Decreto sono da individuarsi nel predetto soggetto, destinatario degli adempimenti di legge, nonché nei soggetti individuati sulla base delle singole procedure e conseguenti incarichi, cui è affidata la realizzazione di specifici adempimenti e/o obblighi di vigilanza e segnalazione, nonché nelle figure aziendali comunque coinvolte nei processi di gestione di attività direttamente o indirettamente interessate dalla disciplina in esame.

Il sistema sopra indicato trova puntuale esplicitazione nel Sistema di gestione Ambientale certificato EMAS adottato dall'azienda; la Società infatti, così come messo in evidenza nella parte generale, ha ottenuto la certificazione ambientale EMAS adottando un piano di miglioramento ambientale per il periodo 2012-2015 e aggiornato periodicamente.

Il succitato sistema prevede:

- Politica ambientale
  - Individuazione dei soggetti destinatari di specifiche procedure ed istruzioni operative
  - Puntuale registrazione delle attività compiute ed archiviazione delle relative evidenze documentali
- azioni di controllo mediante audits periodici interni ed esterni,

L'attività della Società, con riferimento al citato sistema di gestione ambientale è pertanto strutturata in modo da garantire:

- separazione/interruzione, all'interno di ciascuna operazione sensibile, tra il soggetto che avvia il procedimento, quello che lo esegue e/o conclude e quello che svolge l'attività di controllo;
- tracciabilità (per iscritto su supporto cartaceo e/o informatico) di ciascun passaggio rilevante del processo mediante adeguato livello di formalizzazione;
- esclusione di sistemi premianti, nei confronti dei soggetti dotati di poteri di spesa o di facoltà decisionali a rilevanza esterna, basati su obiettivi di risultato oggettivamente inadeguati.

Il rispetto delle singole prescrizioni contenute nel sistema di gestione ambientale costituisce, ai fini della presente Parte Speciale, specifica misura procedurale e organizzativa sicché il mancato rispetto delle suddette prescrizioni, così come delle procedure e degli obblighi richiamati nella presente Parte Speciale, integra specifica violazione disciplinare, sanzionata con il ricorso agli opportuni provvedimenti disciplinari, come previsto nel punto 6 della Parte Generale del Modello.

## **5. Flussi di comunicazione e sistema disciplinare**

Al fine di assicurare l'efficace attuazione del presente Modello viene garantito un periodico monitoraggio sullo suo stato di attuazione da parte del il responsabile del Sistema di gestione ambientale EMAS quale soggetto ritenuto più idoneo e qualificato per assicurare i dovuti coordinamenti tra i vari soggetti e le varie funzioni interessate.

Egli, in tale veste, dovrà pertanto garantire adeguati flussi informativi nei confronti dell'OdV e del Procuratore destinatario di delega di funzioni in materia ambientale (report trimestrale) con particolare riferimento alla puntuale osservanza delle procedure e delle istruzioni emanate per assicurare l'adempimento di tutti gli obblighi di legge, sulle attività e le disposizioni oggetto della presente Parte Speciale e sullo stato di attuazione del sistema previsto dal Modello di Organizzazione e Gestione.

Qualora dovessero emergere situazioni rilevanti che compromettano l'applicazione ed attuazione del Modello di Organizzazione e Gestione sarà cura dell'OdV, anche su segnalazione del Responsabile EMAS ovvero del Procuratore, destinatario di delega di funzioni in materia ambientale, darne tempestiva comunicazione al Consiglio di gestione proponendo le soluzioni opportune per una eventuale adeguata revisione del Modello.

Con riferimento al sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello, saranno passibili di sanzione coloro che, individuati quali destinatari della presente Parte Speciale, delle procedure gestionali nonché di istruzioni operative, ove previste, si dovessero rendere alle stesse inosservanti.

Per quanto concerne invece i criteri di accertamento, contestazione, ed irrogazione della sanzione si rimanda integralmente alle disposizioni previste dal punto 6 - "Il sistema disciplinare" nella Parte Generale del Modello.

## **6. I controlli dell'ODV.**

Con riferimento alle funzioni di verifica e controllo dell'OdV, si rimanda integralmente a quanto già enunciato nella Parte Generale del Modello.

Dovranno in ogni caso essere comunicati senza indugio all'OdV da parte del Procuratore, soggetto responsabile degli adempimenti ambientali, e/o dall'organo dirigente:

- gli esiti non conformi e rilevanti di eventuali ispezioni e/o accertamenti da parte degli organismi di vigilanza deputati al controllo del rispetto della normativa in materia di tutela ambientale;
- l'instaurazione di procedimenti, di natura amministrativa e penale, per violazione delle norme direttamente e/o indirettamente richiamate dall'art. 25 undecies del Decreto.

## **PARTE SPECIALE V - REATI INFORMATICI**

## **1. Destinatari della “Parte Speciale VI”**

La presente Parte Speciale del Modello di Organizzazione e Gestione si rivolge agli amministratori, ai dirigenti e ai dipendenti Consorzio Depurazione del Savonese che operano nell’ambito delle attività e/o processi sensibili individuati ai sensi della presente Parte Speciale, nonché a tutti coloro che, anche in virtù di vincoli contrattuali (appaltatori, consulenti, partners, ecc.), intrattengono rapporti con Consorzio Depurazione del Savonese inerenti profili di gestione informatica.

L’obiettivo della Presente Parte Speciale è dunque di far sì che tutti i destinatari del Modello, nell’ambito delle attività e/o dei processi sensibili come individuati adottino, nei limiti dei propri compiti e delle connesse responsabilità, regole di condotta conformi ai principi contenuti nel Modello (sia nella Parte Generale che nella presente Parte Speciale) e nel Codice Etico al fine di prevenire la commissione dei reati considerati rilevanti ai sensi dell’articolo 24-bis e 25-nonies del Decreto.

In particolare, la presente Parte Speciale ha lo scopo di:

1. indicare le “regole di comportamento” e le procedure che i destinatari del Modello (amministratori, dirigenti, dipendenti, organi sociali, consulenti e collaboratori esterni) sono tenuti ad osservare al fine di una corretta ed efficace applicazione del Modello stesso;
2. fornire all’OdV ed alle funzioni aziendali che con lo stesso collaborano, gli strumenti effettivi per lo svolgimento delle attività di vigilanza, controllo e monitoraggio sull’applicazione del Modello.

## **2. I reati relativi ai delitti informatici e trattamento illecito di dati introdotti dell'art. 24-bis del decreto legislativo 231/01 e dei delitti in violazione del diritto d'autore introdotti dall' art. 25-nonies del decreto legislativo 231/01**

In questo capitolo introduttivo vengono descritte le fattispecie di reati contemplati nella presente Parte Speciale del Modello Organizzativo 231, così come indicati agli artt. 24-bis e 25-nonies del Decreto.

Pur rilevando che le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Sezione in quanto:

- entrambe le fattispecie hanno un comune presupposto: il corretto utilizzo delle risorse informatiche e principi etici da parte degli utenti;
- le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

La prevenzione dei reati tecnologici è diventata una priorità non solo per l'introduzione delle specifiche norme ma per la crescita di sensibilità che avviene nelle strutture dirigenziali. Gli articoli 24-bis prima e 25-nonies dopo, hanno affrontato una serie di illeciti la cui prevenzione è indispensabile in ogni struttura organizzata per poter sopravvivere in un mercato sempre più competitivo ed attento.

L'obiettivo del Modello Organizzativo è principalmente la prevenzione e, in secondo luogo, il monitoraggio e la valutazione dei dati disponibili al fine di garantire informazioni utili all'individuazione dell'utente che - eventualmente - commette un illecito. Il tutto permette all'Ente collettivo di disporre di una struttura monitorata ove, senza commettere alcun illecito in materia di privacy o in lesione degli artt. 4 e 8 dello Statuto dei Lavoratori, si acquisiscono dati utili a poter ricondurre un'eventuale condotta ad un'utente della rete. Informazioni che, opportunamente utilizzate, costituiscono un ottimo deterrente al fine preventivo.

L'organizzazione dei sistemi informativi deve tenere conto che l'attività di lavoro o un'eventuale attività illecita possano essere gestite con lo stesso strumento, per cui solo la prevenzione ed il monitoraggio possono permettere di ottenere un risultato.

I punti cardine di un sistema sono organizzazione e auditing continuo, con acquisizione di dati utili e strutturati a poter individuare nel tempo una condotta e valutarne l'utente che l'ha messa in pratica. Gli unici strumenti efficaci sono i files di *log*, ovvero la scatola nera del sistema informatico. Tali files sono, per loro natura, modificabili ed alterabili, per cui l'ente deve poter garantire la loro conservazione al fine di poterli utilizzare in un'eventuale gestione di cosiddetto "incidente informatico".

## **Le tipologie di delitti informatici ed il trattamento illecito di dati introdotte dall' art. 24-bis del decreto legislativo 231/01**

In questo capitolo si procede con l'elencazione degli articoli del Codice Penale introdotti dagli articoli del D.Lgs. 231/01 al fine di conoscerne i dettagli, le pene inflitte, e le possibili modalità di commissione. Conoscere la fattispecie di reato è già di per se un deterrente alla commissione. Spesso il reato informatico non viene nemmeno percepito come tale e rientra in una ormai normale "cattiva abitudine".

Nelle prossime pagine verranno affrontate una ad una tutte le fattispecie di reato previste nel D.Lgs. 231/01. Per ogni reato viene introdotto il testo, le pene previste dal codice, e :

- modalità di commissione: la percezione del reato informatico è spesso molto bassa e la sola descrizione della modalità di commissione permette all'utente di comprendere quando la propria condotta rientra in una fattispecie di reato ed evitarlo;
- modalità di prevenzione: descrizione delle misure messe in atto per la prevenzione del reato;
- rischio: grado di rischio dell'ente nello specifico reato.

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sotto descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per Consorzio Depurazione del Savonese.

Pertanto, nell'ambito della descrizione delle singole fattispecie criminose, così come nella successiva descrizione dei Delitti in Violazione del Diritto d'Autore, si è tenuto conto di tale rilevante aspetto per l'elaborazione dei casi pratici proposti.

### ***Art. 491-bis cod.pen - Falsità in documenti informatici***

Norma: "Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria<sup>3</sup>, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private<sup>45</sup>. La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale

---

<sup>3</sup> Le parole "avente efficacia probatoria" sono state introdotte dalla legge 18 marzo 2008, n. 48 (ratifica della "convenzione di Budapest")

<sup>4</sup> Il secondo periodo ("A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli") è stato soppresso dalla legge 18 marzo 2008, n. 48 (ratifica della "convenzione di Budapest")

<sup>5</sup> Articolo aggiunto dall'art. 3, L. 23 dicembre 1993, n. 547.

(cfr. Capo III, Titolo VII, Libro II), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un Documento Informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

La falsità può essere materiale e/o ideologica, in dettaglio:

- *Falsità materiale*: si ha quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.
- *Falsità ideologica*: Si ha quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere. Nel falso ideologico è lo stesso autore del documento che attesta fatti non rispondenti al vero.

Integra comunque il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati “sensibili” in vista di una possibile attività ispettiva.

#### *Modalità di commissione:*

Realizzazione di un documento contenente informazioni non corrispondenti al vero o realizzato da utente differente dal firmatario indicato. Sono casi estremamente difficili da prevenire in quanto lo strumento informatico trova la stessa applicazione sia nella gestione di dati corretti che in quelli falsi.

#### *Modalità di prevenzione:*

l'unica modalità di prevenzione di questo reato avviene attraverso il monitoraggio del file system dei server – soprattutto – ma anche – ove è possibile – dei terminali, al fine di poter individuare il reale utente della rete che crea / modifica / stampa il documento.

Per la prevenzione di questo reato è importante dare continuità ad attività di formazione in cui vengano chiaramente illustrate le conseguenze derivanti dal reato.

Attualmente il sistema informatico non dispone di un software di auditing automatico del file system ma è stato accertato che, attraverso normali attività di analisi, è possibile individuare le credenziali dell'utente che ha creato / modificato un documento.

L'introduzione di un sistema automatico di monitoraggio permetterebbe nel tempo di ridurre ulteriormente il rischio.

***Art. 615-ter cod. pen.- Accesso abusivo ad un sistema informatico o telematico***

Norma : "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Tale reato si concretizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

Viene punito l'accesso abusivo ad un sistema informatico o telematico comunque questo venga compiuto, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: ciò si verifica quando un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire l'accesso. L'accesso abusivo è – normalmente – propedeutico ad altri reati come la copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

La suddetta fattispecie delittuosa si realizza anche nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, si sia trattenuto contro la volontà del titolare del sistema, oppure abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

*Modalità di commissione:*

Il delitto potrebbe essere configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa. Tipici, nella commissione di questo reato, sono gli accessi ad un sistema informatico di un precedente datore di lavoro, per acquisire dati e sfruttarli nell'interesse del nuovo datore di lavoro.

I dipendenti dovranno essere anche valutati in termini di *performance* con particolare riferimento ad attività concorrenziali nei riguardi di precedenti datori di lavoro.

***Art. 615-quater cod. pen. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici***

Norma : "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater."

Il reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei (sia a livello software che hardware) all'accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo. Conseguentemente L'art. 615-quater cod. pen., punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. Importante che i sistemi informatici, come già nel caso precedente, sono intesi protetti a livello normativo quando sono gestiti attraverso un qualsiasi livello di protezione (password, firewall, etc.).

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card). Ma anche da tool software e/o hardware che trovano un ampio mercato sulla rete internet.

In conclusione tale fattispecie si configura tra l'altro:

- quando il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi senza autorizzazione a terzi soggetti;
- quando il soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater cod.pen. punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

*Modalità di commissione:*

Molto diffuso è il caso di un soggetto A che passando da un'azienda X ad un'azienda Y continui ad accedere ai dati della società X attraverso gli strumenti della società Y e tragga vantaggio per se e per l'azienda Y dai dati acquisiti dal sistema informativo della società X.

***Art. 615-quinquies cod. pen. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico***

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

Tale fattispecie di reato si realizza quando qualcuno, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegna o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

***Art. 617-quater cod. pen. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche***

Norma : “Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle

comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato (1).”

Tale fattispecie di reato si realizza quando un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

*Modalità di commissione:*

Il reato potrebbe configurarsi con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione ad una gara.

Altra modalità attraverso cui è possibile compiere il reato è quello di intercettare una comunicazione informatica (tra cui sono comprese anche quelle tra apparati mobili) da cui acquisire dati utili ad attività vantaggiose per l'ente per da cui si dipende.

***Art. 617-quinquies cod. pen. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche***

Norma : “Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater.”

Questa fattispecie di reato si realizza nel caso in cui qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La condotta vietata dall'art. 617-quinquies cod. pen. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.

*Modalità di commissione:*

Un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

Tipico il caso di un ex-dipendente che si reca presso la precedente società datrice di lavoro ed avvicina ex-colleghi con qualsivoglia scusa al fine di poter installare uno strumento di intercettazione da cui trarre dati da utilizzarsi a vantaggio dell'attuale datore di lavoro.

***Art. 635-bis cod. pen. - Danneggiamento di informazioni, dati e programmi informatici***

Norma : "Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, e' punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto e' commesso con abuso della qualità di operatore del sistema, la pena e' della reclusione da uno a quattro anni."

La fattispecie di reato si realizza qualora un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

*Modalità di commissione:*

Il danneggiamento potrebbe essere commesso a vantaggio della società laddove l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

***Art. 635-ter cod. pen. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità***

Norma: "Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro

anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.”

Tale reato si realizza qualora un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità.

E' una fattispecie di reato che deve essere tenuta in considerazione con molta attenzione da parte dell'ente Consorzio Depurazione del Savonese in quanto l'oggetto della propria attività è la trattazione di dati provenienti anche da enti pubblici (es. vari Comuni).

#### ***Art. 635-quater cod. pen. - Danneggiamento di sistemi informatici o telematici***

Norma : Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata”.

Questo reato si realizza qualora un soggetto mediante le condotte di cui all'art. 635-bis cod. pen., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

#### ***Modalità di commissione:***

La commissione del reato richiede specifiche competenze tecniche e l'esecuzione di un accesso abusivo al sistema informatico per poter essere messo a compimento.

#### ***Art. 635-quinquies cod. pen. - Danneggiamento di sistemi informatici o telematici di pubblica utilità***

Norma : “Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema

informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata)".

Questo reato si configura quando la condotta di cui al precedente art. 635- quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Come già citato in precedenza, l'ente deve tenere conto del fatto che tratta dati ed il sistema informatico è interconnesso anche con quello di enti pubblici.

Modalità: vedasi paragrafo precedente.

***Art.640-quinquies c.p. - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica***

Norma : "Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".

Questo reato si configura quando un soggetto che presta servizi di certificazione di Firma Elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di Firma Elettronica qualificata.

Modalità: non applicabile

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei Delitti Informatici possono essere di natura pecuniaria, da 100 a 500 quote (considerato che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell'Ente, tra un minimo di Euro 258 ed un massimo di Euro 1.549 e le stesse possono variare da un minimo di circa Euro 26.000 ad un massimo di circa Euro 800.000) e di natura interdittiva, che variano a seconda della fattispecie criminosa realizzata.

I destinatari del presente Parte Speciale dovranno prestare attenzione alla correlazione e concorso tra i reati con l'attribuzione della responsabilità penale per più reati informatici nel caso di una violazione commessa (es. di correlazione: detenzione

abusiva dei codici d'accesso/accesso abusivo/diffusione di software dannosi). La specificità dei reati informatici è tale che difficilmente potrà essere commesso un reato unico. Ad esempio l'accesso abusivo (635 ter) è da intendersi a livello tecnico un reato di tipo propedeutico alla commissione di ulteriori fattispecie.

Come già citato sarà molto importante valutare le *performance* del singolo soggetto lavoratore al fine di accertare anomalie di risultati che potrebbero evidenziare l'utilizzo illecito di dati, la cui provenienza potrebbe derivare da una condotta fraudolenta compiuta attraverso un reato informatico tra quelli in precedenza descritti.

### **Le tipologie di delitti in violazione del diritto d'autore introdotte dall' art. 25-nonies del decreto legislativo 231/01**

L'art. 25-nonies contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (e, in particolare, dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies della Legge 22/04/1941) quali, a titolo d'esempio:

- l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE;
- la riproduzione o il reimpiego del contenuto di banche dati;
- l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico;
- l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie di cui all'art. 25-nonies del D. Lgs. 231/2001.

### **Art. 171 comma 1 lett. a bis e comma 3 Legge sul diritto d'autore - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio**

In relazione alla fattispecie delittuosa di cui all'art. 171, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

1. la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno protetta o di parte di essa;
2. la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

**Art. 171 bis Legge sul diritto d'Autore. - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio**

La norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati. Per i software, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata". Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

Le sanzioni applicabili all'Ente nell'ipotesi di commissione dei Delitti in Violazione del Diritto d'Autore possono essere di natura pecuniaria fino a 500 quote (e dunque fino ad un massimo di circa Euro 800.000) e di natura interdittiva, quali l'interdizione dall'esercizio dell'attività o la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito per una durata non superiore ad un anno.

**Art.640-ter cod. pen. - Frode informatica**

Norma : Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 516 a due 1.032. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

### **3. Processi sensibili della Consorzio Depurazione del Savonese per i delitti informatici**

#### **3.1 Aree a Rischio**

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute in genere a rischio risultano essere, ai fini della presente Sezione, le seguenti:

- tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;
- gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;
- gestione dei flussi informativi elettronici con la pubblica amministrazione;
- utilizzo di software e banche dati;
- gestione dei contenuti del sito Internet.

I destinatari del presente Parte Speciale sono in generale:

- i designati dello sviluppo, installazione, assistenza e manutenzione degli applicativi e dell'infrastruttura tecnologica;
- gli incaricati della gestione dei dati nei sistemi contabili ed informatici in generale;

I compiti attribuiti agli Amministratori di Sistema - con atto di incarico scritto – sono monitorati attraverso l'adozione di misure previste dal Garante della Privacy con l'archiviazione dei log amministrativi per un periodo di 180 giorni.

Si precisa che per i reati informatici commessi da amministratori di sistema non è necessaria la querela di parte, poiché sono procedibili d'ufficio.

Nella redazione del presente modello – come detto - è stata valutata la gestione dei files di Log obbligatori per effetto delle norme imposte dal Garante sulla Privacy in materia di accessi amministrativi (amministratori di sistema).

#### **3.2 Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001**

Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall'art. 24-bis del D.Lgs. 231/2001, sono tra l'altro le seguenti:

- Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell'ambito della quale sono ricomprese le attività di:
  - ✓ gestione del profilo utente e del processo di autenticazione;

- ✓ gestione e protezione della postazione di lavoro;
- ✓ gestione degli accessi verso l'esterno;
- ✓ gestione e protezione delle reti;
- ✓ gestione degli output di sistema e dei dispositivi di memorizzazione;
- Sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)
- Utilizzo e gestione di dati aziendali con strumenti informatici dotati di software standard (commerciali) e/o piattaforma gestionale aziendale (fornita da gestore esterno);

#### **4. Procedure adottate**

##### **4.1 Il sistema procedurale**

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli utenti della rete informatica della società Consorzio Depurazione del Savonese, chiamati Destinatari. Obiettivo della presente Sezione è che tali Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di Consorzio Depurazione del Savonese – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di quelli commessi in violazione del diritto d'autore.

In particolare, la presente Sezione ha la funzione di:

- fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, tutti i dirigenti, dipendenti e consulenti dell'ente sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti nei seguenti documenti, per le parti di proprio interesse:

- Organigramma aziendale e schemi organizzativi;
- Controllo degli accessi logici alle risorse informative rendendo riservati e personali i propri codici di accesso e le proprie password;
- Procedure interne di gestione password provvedendo alla sostituzione come previsto e senza ideare metodologie elusive delle logiche di sicurezza;

- Verifica periodica dei files di Log obbligatori da parte degli amministratori di sistema (accessi amministrativi e posta elettronica);
- Audit periodica, anche attraverso l'impiego di esperti esterni in appoggio all'OdV, tramite cui effettuare valutazioni inerenti l'applicazione del presente Modello Organizzativo e su valutazioni a campione delle condotte nell'uso degli strumenti informatici;
- Valutazione periodica del livello di sicurezza informatica, che per sua natura si riduce con il passar del tempo, se non vengono gestiti opportuni investimenti;
- Verifica periodica degli investimenti svolti in materia informatica, con particolare riferimento all'aggiornamento degli strumenti, compreso quelli di rete, e dei software.

Gli obiettivi fondamentali della sicurezza informatica che Consorzio Depurazione del Savonese si pone sono i seguenti:

- *Riservatezza*: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate risultano essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- *Integrità*: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Risulta garantito che le informazioni risultano trattate in modo tale che non possono essere manomesse o modificate da soggetti non autorizzati, e comunque, in caso di manomissione identificare l'esecutore;
- *Disponibilità*: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei lavoratori dipendenti e dei consulenti di Consorzio Depurazione del Savonese (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/2001 e art. 25-nonies del D.Lgs 231/2001);
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- b) accedere abusivamente al sistema informatico o telematico proprio o di terzi di soggetti pubblici o privati;
- c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni, o di sottrarle al fine di poterle reimpiegare in attività concorrenziali e di vantaggio per l'ente Consorzio Depurazione del Savonese;
- d) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate. Si richiede agli utenti della rete di segnalare con tempestività la presenza di tali situazioni.
- e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- f) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- h) installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
- l) acquisire, distribuire, vendere o detenere a scopo commerciale o imprenditoriale programmi in supporti non contrassegnati dal marchio SIAE, opere tutelate dal diritto d'autore o banche dati e software pirati.
- m) Installare o utilizzare software tutelati dal diritto d'autore, non autorizzati da Consorzio Depurazione del Savonese, ed installati dal personale tecnico interno,

per qualsivoglia attività lavorativa e di gestione di dati di proprietà Consorzio Depurazione del Savonese;

Pertanto, i soggetti sopra indicati, in particolare i dipendenti Consorzio Depurazione del Savonese, devono rispettare i seguenti principi:

- *L'uso dei sistemi informatici deve svolgersi nel rigoroso rispetto delle norme vigenti, Codice Etico in vigore e nel rispetto dei regolamenti emanati dall'ente;*
- *La società rispetta tutte le normative in materia di Privacy al quale tutti gli amministratori, i dipendenti ed i collaboratori sono tenuti ad attenersi;*
- *Tutti i software installati nei sistemi della società risultano regolarmente licenziati e nessuno è autorizzato alla loro rimozione, reinstallazione, o modifica;*
- *Ogni utente è personalmente responsabile dell'integrità (fisica e funzionale) dei sistemi medesimi, dei dati, delle informazioni e dei programmi ad essi relativi, ed alla loro custodia quando trasferiti all'esterno del perimetro aziendale (dispositivi mobili) ove possono essere oggetto di furto mirato all'acquisizione di dati aziendali;*
- *L'accesso ad ogni singolo sistema informatico e telematico è limitato ad uno o più utenti identificati, attraverso la sorveglianza dei locali ed il ricorso a chiavi logiche (user ID e password) e fisiche (le porte di accesso ai locali sono chiuse a chiave);*
- *Ad ogni User-ID corrisponde un profilo di accesso alle reti aziendali ed internet (ove presente). Ad ogni profilo corrispondono l'utilizzo concesso degli applicativi, il limite di accesso al sistema informativo aziendale (modulo) e le attività concesse (visualizzazione, inserimento dati, modificazione dei dati inseriti);*
- *Le assegnazioni in uso di un sistema informatico o telematico o di User-ID (profilo) sono richieste dal responsabile di funzione e devono essere disattivate tempestivamente al cessare del rapporto di lavoro, sempre su richiesta del responsabile di funzione;*
- *Le assegnazioni in uso di un sistema informatico o telematico o di User-ID (profilo) sono richieste dal responsabile di funzione. La richiesta è motivata con riferimento alle attività che l'utente è chiamato a compiere. I profili assegnati sono registrati e conservati dall'area informatica referente. Esistono procedure formali per l'assegnazione di privilegi speciali (es. super-user, power-user);*
- *Ad ogni cambio di mansione il responsabile di funzione dell'utente e/o il responsabile della funzione risorse umane, provvedono a comunicare la necessità di aggiornamento del profilo utente alla Funzione Organizzazione, il quale provvede immediatamente alla revoca del precedente profilo. I profili sono*

*soggetti a revisione periodica. Per l'assegnazione di un nuovo profilo si applicano i principi sopra indicati;*

- *Risulta in uso agli utenti una casella di posta elettronica con account personale (es: cognome.inizialenome@depuratore.sv.it). L'uso di posta elettronica attraverso questa casella è destinata ad esclusivo scopo istituzionale.*
- *L'ente offre la possibilità di consultare una casella di posta personale via web, nel rispetto del regolamento dell'Ente.*
- *Nei limiti della normativa vigente, gli Amministratori di Sistema (anche per il tramite di un delegato) sono autorizzati dalla Società e dagli utenti ad accedere ai sistemi informatici a fini di garanzia della continuità dell'attività d'impresa (assenza prolungata dell'utente), di manutenzione, di tutela della sicurezza dei sistemi medesimi e di prevenzione dei reati di cui all'art. 24bis D. Lgs. 231/2001;*
- *La società può altresì revocare, in tutto o in parte l'uso dei sistemi informatici, ovvero impedire, in tutto o in parte, l'accesso alle reti informatiche aziendali e non, ad uno o più utenti (a titolo d'esempio, facendo uso di filtri);*
- *Amministratori, dipendenti e collaboratori aderiscono ai predetti principi generali di utilizzo dei sistemi informatici e, quindi, espressamente accettano anche l'accesso ai medesimi, senza limitazione alcuna, da parte dei propri superiori, dell'amministratore di sistema o dei suoi delegati;*
- *L'utilizzo delle firme elettroniche certificate avviene su apposita delega scritta del rappresentante legale dell'azienda;*
- *E' vietato qualsiasi uso dei sistemi informatici per scopi incompatibili con quello per il quale essi sono concessi in uso agli utenti. In particolare è vietato:*
  - ✓ *l'uso ludico dei sistemi informatici;*
  - ✓ *operare il download, il caricamento o l'installazione di software (musicali, film, foto, programmi, ecc...) non autorizzati e, comunque, in violazione del diritto d'autore;*
  - ✓ *utilizzare supporti rimovibili (es. chiavetta USB) non controllati preventivamente e comunque in modo esclusivo per attività attinenti alle mansioni lavorative;*
  - ✓ *rendere in qualsiasi modo noto a terzi non autorizzati, o comunque consentire a questi la conoscenza di dati, informazioni, formule, descrizioni di processi, documenti, materiale di qualsiasi natura, coperto da riservatezza o la cui conoscenza da parte di soggetti terzi potrebbe recare danno alla società;*

- ✓ *produrre, detenere, diffondere, in qualsiasi forma e modo, materiale pornografico, pedopornografico, di propaganda od istigazione a fini terroristici, ovvero offensivo dell'onore o dignità di terzi;*
- ✓ *violare registri ed archivi informatici della società e/o falsificare dati, informazioni o documenti informativi di qualsiasi specie;*
- ✓ *comunicare a terzi, cedere, trasmettere rendere noto o mettere a disposizione, in qualsiasi forma o modo, e a qualunque titolo, password di accesso a sistemi informatici della società o di terzi dei quali i destinatari della procedura siano in possesso in ragione dell'attività svolta;*
- ✓ *porre in essere una delle condotte previste dall'art. 24bis d. lgs. 231/2001 ovvero anche altra condotta strumentale alle medesime.*
- *L'accesso a sistemi informatici di soggetti esterni alla Società (a titolo d'esempio la P.A.) è limitato ai soli utenti a ciò espressamente autorizzati attraverso l'attribuzione di specifici codici di accesso. Costoro sono tenuti a mantenere strettamente riservate, non divulgare e conservare al sicuro ed al riparo da atti di impossessamento o appropriazione le chiavi di accesso ai predetti sistemi;*
- *Nei casi di cessazione dei rapporti con la società, ovvero di cambio di mansioni dell'utente, le password e gli user-ID relativi ai sistemi informatici della società sono revocati; la società si fa inoltre carico di avvisare gli enti esterni dei quali l'utente sia in possesso di password e User-Id per conto della Società.*

La verifica del rispetto delle regole sopra elencate è delegata ad un consulente, che effettuerà controlli periodici producendo un apposito report per l'Organismo di Vigilanza.

#### **4.2 Principi generali di comportamento**

I Principi generali di controllo possono essere sintetizzati come segue:

- *Segregazione delle attività:* si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla. In nessun caso il rilascio di codici di accesso o modifica di profili utente potrà essere operata senza specifica richiesta / autorizzazione.
- *Esistenza di procedure/norme/circolari:* devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- *Poteri autorizzativi e di firma:* i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo,

ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società.

- *Tracciabilità*: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata tramite strumenti informatici (firewall e software di tracciatura). Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate, rispettando gli obblighi di legge di conservazione dei Log (Provvedimento del Garante della Privacy del 27/11/2008).
- *Formazione*: verranno programmati periodicamente corsi di formazione sulla sicurezza informatica e sull'utilizzo dei sistemi informatici in favore dei Dipendenti, diversificati in ragione delle rispettive mansioni. Saranno promossi corsi di formazione attraverso cui verranno sensibilizzati i valori etici e morali nell'uso di sistemi informatici riepilogati nel presente documento.

### 4.3 Le procedure specifiche generalmente applicabili

L'utilizzo e la gestione di sistemi informatici e del Patrimonio informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi della Società. Tra i sistemi informativi utilizzati dalla Società vi sono anche hardware e software finalizzati agli adempimenti per la Pubblica Amministrazione che prevedono il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi.

Le procedure interne della società ed i processi aziendali sono guidate da principi di sicurezza organizzativa, comportamentale e tecnologica e da adeguate attività di controllo, per un adeguato presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del patrimonio informativo in coerenza con la normativa vigente.

La sicurezza viene perseguita tramite:

- la protezione dei sistemi e delle informazioni dai potenziali attacchi (secondo la creazione di una cultura aziendale attenta agli aspetti della sicurezza e a una direttrice tecnologica, attraverso l'utilizzo di strumenti atti prevenire e a reagire a fronte delle diverse tipologie di attacchi)
- la garanzia della massima continuità del servizio anche attraverso l'installazione e la gestione di apparecchiature di continuità dell'energia elettrica e alla e l'esecuzione di rapide procedure di ripristino delle immagini di backup dei server aziendali;
- l'installazione e gestione di package antivirus, costantemente aggiornati e dotati di un sistema centralizzato di monitoraggio;
- il controllo degli accessi ai locali del Centro Elaborazione Dati;
- Password di accesso, per profilo aziendale e per dipendente, personalizzate in funzione dei ruoli e dei compiti attribuiti all'utente del sistema informatico;
- gli accessi degli amministratori di sistema sono loggati in specifici report con gestione autonoma del sistema in ottemperanza alla norma del Garante della Privacy;
- l'inventario dei programmi software e delle licenze d'uso per monitorare il rischio reato legato al diritto di autore;
- procedure di back up dei dati atte a ripristinare l'integrità dei dati e dei documenti in base alla strategia di disaster recovery e business continuity;
- la conservazione dei programmi applicativi e dei supporti di back up in luoghi idonei alla loro salvaguardia;
- i sistemi contabili e amministrativi sono dotati di log report che tracciano le attività eseguite, l'utente e la data dell'operazione;

- meccanismi di segregazione delle reti a livello di funzione aziendale, limitando l'utilizzo delle aree di scambio;
- la disponibilità di ambienti di test separati da quelli di produzione;
- esistenza di processi per evitare intrusioni attive o passive a sistemi informatici attraverso la continua verifica dei sistemi di protezione (Log) condotta con una scrupolosa valutazione dei files di Log;
- la verifica della possibilità di accesso ai programmi e alle reti esterne senza l'utilizzo delle password e verifica periodica del livello di sicurezza della rete informatica;
- la verifica delle procedure interne di protezione dei dati trattati dei processi per enti esterni;
- la presenza di ambienti di accesso dall'esterno da parte di soggetti appartenenti all'organizzazione dell'ente (es. VPN);
- comunicatie comunicazioni organizzative nei processi dell'ente di accesso a ambienti informatici e telematici interni;
- l'adozione del sistema delle "deleghe" e del rispetto delle procedure, in particolare per quanto riguarda le decisioni di spesa e la scelta delle controparti;
- la separazione delle mansioni e dei ruoli a tutela della separazione delle informazioni societarie;
- il controllo costante di carattere di flusso informativo della funzionalità ed affidabilità del sistema di sicurezza per l'accesso ai dati della Società;
- valutazione periodica dei fornitori esterni di sistemi informatici (hardware e software);

Consorzio Depurazione del Savonese, attraverso la propria struttura di gestione della rete informatica (amministratore di rete) a sua volta si impegna a:

- Informare adeguatamente i Dipendenti, nonché gli stagisti e gli altri soggetti (come ad esempio i Collaboratori Esterni) eventualmente autorizzati all'utilizzo dei Sistemi Informativi, dell'importanza di:
  - mantenere le proprie Credenziali confidenziali e di non divulgare le stesse a soggetti terzi;
  - utilizzare correttamente i software e banche dati in dotazione;
  - non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;
- Prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore degli stagisti e degli altri soggetti (come ad esempio i Collaboratori Esterni) eventualmente autorizzati all'utilizzo dei Sistemi Informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;

- Definire nell'ambito del Codice Etico e delle policy di Information Security i comportamenti accettabili per l'utilizzo corretto dei software e delle banche dati;
- L'ente considera noto a tutti i dipendenti, stagisti e consulenti, il documento contenente le regole di utilizzo degli strumenti informatici (User Policy, Politiche utenti dei sistemi informativi) in quanto pubblicata sulla propria rete Intranet, di cui tutti i soggetti abilitati all'uso dei sistemi informatici hanno accesso.
- Informare i dipendenti, nonché gli stagisti e gli altri soggetti (come ad esempio i collaboratori esterni) eventualmente autorizzati all'utilizzo dei sistemi informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- Impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzate per un determinato periodo di tempo, si blocchino automaticamente;
- Limitare gli accessi alle stanze server unicamente al personale autorizzato;
- Proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- Dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- Impedire l'installazione e l'utilizzo di software non approvati da Consorzio Depurazione del Savonese e non correlati con l'attività professionale espletata per la stessa;
- Informare gli utilizzatori dei sistemi informatici che i software per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- Limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di Virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;
- Impedire l'installazione e l'utilizzo, sui sistemi informatici di Consorzio Depurazione del Savonese, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, Virus, etc.) senza alcuna possibilità di controllo da parte di Consorzio Depurazione del Savonese;

- Qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni a Consorzio Depurazione del Savonese, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;
- Prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti, degli stagisti e degli altri soggetti (come ad esempio i collaboratori esterni) eventualmente autorizzati all'utilizzo dei Sistemi Informativi;
- Limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti, degli stagisti e degli altri soggetti (come ad esempio i collaboratori esterni) eventualmente autorizzati all'utilizzo dei sistemi informativi;
- Provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;
- Prevedere, nei rapporti contrattuali con i fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, clausole di manleva volte a tenere indenne la Società da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi;
- Prevedere delle fasi di test dell'operatività delle procedure di sicurezza adottate in azienda.

## 5. I controlli dell'ODV

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le funzioni preposte ai Sistemi Informativi; al riguardo dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento. Pertanto all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di Attività Sensibili.

In relazione ai doveri dei destinatari della Parte Speciale, i controlli dell'OdV consisteranno in:

- verifica che le direttive e procedure che regolamentano le attività nelle aree a rischio siano adeguate e correttamente applicate dai soggetti coinvolti, attraverso apposita reportistica dell'area informatica sui controlli ed esito degli stessi;
- verifica annuale delle relazioni riepilogative sull'analisi dei log report di sistema traccianti gli accessi e le anomalie emerse; tale relazione verrà redatta dall'area informatica, mentre per le eventuali ulteriori verifiche l'OdV potrà essere supportata da consulenti esterni;
- verifica annuale delle relazioni sull'analisi statistica degli interventi manutentivi. Tali relazioni annuali saranno redatte dall'area informatica;
- verifica annuale dell'aggiornamento dell'elenco delle licenze relative agli applicativi e all'infrastruttura tecnologica. Tali relazioni annuali saranno redatte dall'area informatica;
- verifica dell'atto di nomina degli Amministratori di Sistema;
- controllo in merito alle attività di verifica compiute circa il rispetto delle misure minime di sicurezza/privacy (es. controlli periodici di IT audit della società di revisione o verifiche ispettive qualità sul controllo degli accessi e creazione/cancellazione degli account); attraverso apposita reportistica dell'area informatica sui controlli ed esito degli stessi, mentre per le eventuali ulteriori verifiche l'OdV potrà essere supportata da consulenti esterni;
- verifica dei programmi di formazione periodica dell'incaricato in ambito privacy, dell'applicazione del Codice Etico e delle regole presenti nel Modello Organizzativo, attraverso apposita reportistica dell'area personale.

L'Organismo di Vigilanza, viste le specifiche professionalità necessarie per l'esercizio del controllo delle attività informatiche, potrà avvalersi di consulenti esterni

chiamati ad effettuare le verifiche su delega e rendicontare all'Organismo stesso attraverso apposite reportistiche.