

**MODELLO DI  
ORGANIZZAZIONE, GESTIONE E CONTROLLO  
ex D. Lgs. 8 giugno 2001 n. 231  
e  
PIANO TRIENNALE DELLA PREVENZIONE DELLA CORRUZIONE  
ANNI 2025 - 2027**

Approvato dal CDA in data 03 marzo 2025

Sommario

**SEZIONE I**

**PARTE GENERALE: MODELLO DI ORGANIZZAZIONE E GESTIONE EX D. LGSN.231/2001**

**SEZIONE I – PARTE GENERALE - MODELLO DI ORGANIZZAZIONE E GESTIONE EX D. LGS. N. 231/2001** - 7 -

**1. IL QUADRO NORMATIVO DI RIFERIMENTO: IL D. LGS. N. 231/2001 E LA SUA EVOLUZIONE** - 8 -

**1.1. IL SUPERAMENTO DEL PRINCIPIO “*SOCIETAS DELINQUERE NON POTEST*” E LA PORTATA DELLA NUOVA RESPONSABILITÀ AMMINISTRATIVA DA REATO** - 8 -

**1.2. LE SANZIONI PREVISTE DAL D. LGS. N. 231/2001** - 10 -

**1.3. L’ADOZIONE E L’ATTUAZIONE DI UN MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO** - 11 -

**2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI DIFESA SERVIZI** - 12 -

**2.1. DIFESA SERVIZI S.P.A. E LA SUA MISSION** - 12 -

**2.2. LE COMPONENTI DEL MODELLO DI DIFESA SERVIZI S.P.A.** - 13 -

**3. IL MODELLO DI GOVERNANCE ED IL SISTEMA ORGANIZZATIVO DI DIFESA SERVIZI** - 13 -

**3.1. IL MODELLO DI GOVERNANCE DI DIFESA SERVIZI** - 13 -

**3.2. L’ASSETTO ORGANIZZATIVO DI DIFESA SERVIZI** - 15 -

**3.2.1. LE AREE AZIENDALI** - 15 -

**3.2.2. DEFINIZIONE DELL’ORGANIGRAMMA AZIENDALE E DEI COMPITI** - 16 -

**4. IL SISTEMA DI INCARICHI IN DIFESA SERVIZI** - 16 -

**4.1. I PRINCIPI GENERALI** - 16 -

**4.2. IL SISTEMA DI DELEGHE E PROCURE** - 17 -

**4.3. LA STRUTTURA DEL SISTEMA DI INCARICHI IN DIFESA SERVIZI** - 17 -

**5. PROCEDURE MANUALI ED INFORMATICHE** - 17 -

**6. IL CONTROLLO DI GESTIONE ED I FLUSSI FINANZIARI** - 18 -

**6.1. FASE DI PROGRAMMAZIONE E DI DEFINIZIONE DEL BUDGET** - 18 -

**6.2. FASE CONSUNTIVA ED ANALISI DEGLI SCOSTAMENTI** - 19 -

**7. L’ORGANISMO DI VIGILANZA DI DIFESA SERVIZI** - 19 -

**7.1. LA COMPOSIZIONE DELL’ORGANISMO ED I SUOI REQUISITI** - 19 -

**7.2. I COMPITI ED I POTERI DELL’ORGANISMO DI VIGILANZA** - 19 -

**7.3. I FLUSSI INFORMATIVI CHE INTERESSANO L’ORGANISMO DI VIGILANZA** - 20 -

**7.4. WHISTLEBLOWING** - 21 -

**7.4.1. OBBLIGHI DI RISERVATEZZA E TUTELA DEL SEGNALENTE** - 22 -

<b>8. IL CODICE ETICO DI DIFESA SERVIZI</b>	<b>- 23 -</b>
<b>8.1. ELABORAZIONE ED APPROVAZIONE DEL CODICE ETICO</b>	<b>- 23 -</b>
<b>8.2. FINALITÀ, STRUTTURA E DESTINATARI DEL CODICE ETICO</b>	<b>- 24 -</b>
<b>8.3. I PRINCIPI GENERALI CHE REGOLANO L'ATTIVITÀ DELLA SOCIETÀ</b>	<b>- 24 -</b>
<b>8.4. PRINCIPI E NORME DI COMPORTAMENTO</b>	<b>- 25 -</b>
<b>8.4.1. PRINCIPI E NORME DI COMPORTAMENTO PER I COMPONENTI DEGLI ORGANI SOCIALI</b>	<b>- 25 -</b>
<b>8.4.2. PRINCIPI E NORME DI COMPORTAMENTO PER IL PERSONALE</b>	<b>- 25 -</b>
<b>8.4.3. PRINCIPI E NORME DI COMPORTAMENTO PER I TERZI DESTINATARI</b>	<b>- 27 -</b>
<b>8.5. OBBLIGHI DI COMUNICAZIONE ALL'ORGANISMO DI VIGILANZA</b>	<b>- 27 -</b>
<b>8.6. LE MODALITÀ DI ATTUAZIONE ED IL CONTROLLO SUL RISPETTO DEL CODICE ETICO</b>	<b>- 28 -</b>
<b>9. IL SISTEMA DISCIPLINARE DI DIFESA SERVIZI</b>	<b>- 28 -</b>
<b>9.1. L'ELABORAZIONE E L'ADOZIONE DEL SISTEMA DISCIPLINARE</b>	<b>- 28 -</b>
<b>9.2. LE CONDOTTE RILEVANTI PER IL SISTEMA DISCIPLINARE</b>	<b>- 29 -</b>
<b>11. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI CONNESSI. L'AGGIORNAMENTO DEL MODELLO</b>	<b>- 30 -</b>
<b>10.1. L'INFORMAZIONE SUL MODELLO E SUI PROTOCOLLI CONNESSI</b>	<b>- 30 -</b>
<b>10.2. LA FORMAZIONE SUL MODELLO E SUI PROTOCOLLI CONNESSI</b>	<b>- 30 -</b>
<b>10.3. COMUNICAZIONE DEGLI AGGIORNAMENTI DEL MODELLO E DEL CODICE ETICO</b>	<b>- 30 -</b>
<b>SEZIONE II – PARTE SPECIALE MODELLO DI ORGANIZZAZIONE E GESTIONE EX D. LGS. N. 231/2001</b>	<b>- 31 -</b>
<b>1. MAPPATURA E VALUTAZIONE DEI RISCHI</b>	<b>- 32 -</b>
<b>1.1. LE NOZIONI DI PUBBLICA AMMINISTRAZIONE, PUBBLICO UFFICIALE ED INCARICATO DI PUBBLICO SERVIZIO E I REATI PREVISTI DAL D. LGS. N. 231/2001 (CD. REATI-PRESUPPOSTO).</b>	<b>- 33 -</b>
<b>1.1.2. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24 BIS, D. LGS. N. 231/2001)</b>	<b>- 39 -</b>
<b>1.1.3. DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24 TER, D. LGS. N. 231/2001)</b>	<b>- 40 -</b>
<b>1.1.4. REATI SOCIETARI (ART. 25 TER, D. LGS. N. 231/2001)</b>	<b>- 41 -</b>
<b>1.1.5. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO (ART. 25 SEPTIES, D. LGS. N. 231/2001)</b>	<b>- 42 -</b>
<b>1.1.6. RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (ART. 25 OCTIES, D. LGS. N. 231/2001)</b>	<b>- 42 -</b>
<b>1.1.7. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (ART. 25 OCTIES.1, D. LGS. N. 231/2001)</b>	<b>- 42 -</b>
<b>1.1.8. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25 NOVIES, D. LGS. N. 231/2001)</b>	<b>- 43 -</b>
<b>1.1.9. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25 DECIES, D. LGS. N. 231/2001)</b>	<b>- 43 -</b>
<b>1.1.10. REATI AMBIENTALI (ART. 25 UNDECIES, D. LGS. N. 231/2001)</b>	<b>- 43 -</b>
<b>1.1.11. REATI TRIBUTARI (ART. 25-QUINQUESDECIES, D. LGS. N. 231/2001)</b>	<b>- 45 -</b>
<b>1.1.12. DELITTI CONTRO IL PATRIMONIO CULTURALE (ART. 25 SEPTIESDECIES, D. LGS. N. 231/2001)</b>	<b>- 45 -</b>
<b>1.1.13. RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHIEGGIO DI BENI CULTURALI E PAESAGGISTICI (ART. 25 DUODEVICIES, D. LGS. N. 231/2001)</b>	<b>- 46 -</b>

<b>1.2. AREE POTENZIALMENTE “A RISCHIO”. ATTIVITÀ “SENSIBILI”. REATI PROSPETTABILI</b>	<b>- 46 -</b>
<b>1.3. I PRINCIPI GENERALI DI COMPORTAMENTO</b>	<b>- 46 -</b>
<b>1.4. I COMPITI DELL’ORGANISMO DI VIGILANZA</b>	<b>- 48 -</b>

**SEZIONE III – PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE** - 49 -

**1. IL QUADRO NORMATIVO DI RIFERIMENTO IN MATERIA DI PREVENZIONE DELLA CORRUZIONE E TRASPARENZA AI SENSI DELLA LEGGE 190/2012 E LA NOZIONE DI CORRUZIONE** - 50 -

**2. NOZIONE DI “CORRUZIONE”** - 51 -

**3. IL PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE (PTPC)** - 52 -

<b>3.1. OGGETTO, FINALITÀ E DESTINATARI</b>	<b>- 53 -</b>
<b>3.2. I SOGGETTI RESPONSABILI E GLI ATTORI COINVOLTI</b>	<b>- 54 -</b>
<b>3.2.1. IL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE (RPC)</b>	<b>- 54 -</b>
<b>3.2.2. AMBITO SOGGETTIVO</b>	<b>- 55 -</b>
<b>3.2.3. I REFERENTI DEL RPC</b>	<b>- 56 -</b>
<b>3.2.4. I DIPENDENTI DELLA SOCIETÀ</b>	<b>- 56 -</b>
<b>3.2.5. I COLLABORATORI E CONSULENTI A QUALSIASI TITOLO DELLA SOCIETÀ</b>	<b>- 56 -</b>
<b>3.3. INDIVIDUAZIONE E GESTIONE DEI RISCHI DI CORRUZIONE</b>	<b>- 56 -</b>
<b>3.3.1. MAPPATURA E VALUTAZIONE DELLE AREE DEL RISCHIO</b>	<b>- 57 -</b>
<b>3.4. SISTEMA DI CONTROLLI</b>	<b>- 57 -</b>
<b>3.5. INCONFERIBILITÀ SPECIFICHE PER GLI INCARICHI DI AMMINISTRATORE E PER GLI INCARICHI DIRIGENZIALI</b>	<b>- 57 -</b>
<b>3.6. INCOMPATIBILITÀ SPECIFICHE PER GLI INCARICHI DI AMMINISTRATORE E PER GLI INCARICHI DIRIGENZIALI</b>	<b>- 58 -</b>
<b>3.7. ROTAZIONE DEGLI INCARICHI</b>	<b>- 58 -</b>
<b>3.8. MONITORAGGIO</b>	<b>- 59 -</b>
<b>3.9. TUTELA DEL DIPENDENTE PUBBLICO CHE SEGNA LA GLI ILLECITI (<i>WHISTLEBLOWING</i>)</b>	<b>- 60 -</b>
<b>3.10. FORMAZIONE DEL PERSONALE</b>	<b>- 61 -</b>
<b>3.11. MONITORAGGIO DEI RAPPORTI TRA AMMINISTRAZIONE E I SOGGETTI CHE CON LA STESSA STIPULANO CONTRATTI O CHE SONO INTERESSATI A PROCEDIMENTI DI AUTORIZZAZIONE, CONCESSIONE, O EROGAZIONE</b>	<b>- 62 -</b>
<b>3.12. ATTIVITÀ SUCCESSIVA ALLA CESSAZIONE DEL RAPPORTO DI SERVIZIO/LAVORO</b>	<b>- 62 -</b>

**4. IL PIANO TRIENNALE PER LA TRASPARENZA E L’INTEGRITÀ (PTTI)** - 63 -

<b>4.1. SOGGETTI RESPONSABILI</b>	<b>- 63 -</b>
<b>4.1.1. QUALITÀ DELLE INFORMAZIONI E CRITERI GENERALI</b>	<b>- 63 -</b>
<b>4.2. CONTROLLO E MONITORAGGIO</b>	<b>- 64 -</b>
<b>4.3. TEMPI DI ATTUAZIONE DEGLI OBIETTIVI</b>	<b>- 64 -</b>
<b>4.4. ACCESSO CIVICO</b>	<b>- 64 -</b>
<b>4.4.1 L’ACCESSO CIVICO “SEMPLICE”</b>	<b>- 64 -</b>
<b>4.4.2 L’ACCESSO CIVICO GENERALIZZATO, PROCEDIMENTALE O DOCUMENTALE</b>	<b>- 64 -</b>

**5. ADEGUAMENTI** - 65 -

**ALLEGATI:**

1. Organigramma aziendale

2. Codice etico
3. Schede di individuazione delle aree di rischio. Individuazione delle aree strumentali e ruoli aziendali coinvolti
4. Schede dei rischi PTPC
5. Programma triennale per la trasparenza e l'integrità (PTTI)

## PREMESSA

Con la legge 6 novembre 2012, n. 190, pubblicata sulla Gazzetta ufficiale n. 265 del 13 novembre 2012 ed entrata in vigore il 28 novembre 2012, sono state approvate le "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione".

In ottemperanza a quanto previsto dalla Legge ed in coerenza con le disposizioni contenute nel Piano Nazionale Anticorruzione DIFESA SERVIZI S.P.A., con il presente Piano per la Prevenzione della Corruzione, intende aggiornare, per il triennio 2025/2027, il sistema di controllo, di prevenzione e di contrasto della corruzione e l'illegalità integrato con gli altri elementi già adottati dell'Azienda, tra cui il Codice Etico ed il Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01.

Il Piano di Prevenzione della Corruzione ha l'obiettivo di rafforzare e razionalizzare il corpo degli interventi organizzativi e di controllo, attuati dalla DIFESA SERVIZI S.P.A. al fine di identificare le strategie per la prevenzione, il contrasto della corruzione a livello aziendale e si configura come parte del Modello ex D. Lgs. 231/01 adottato dalla Società. DIFESA SERVIZI in quanto totalmente partecipata dal Ministero della Difesa in regime *in house* ha recepito il D. Lgs. 231/2001 mediante l'adozione del Modello di Organizzazione e Gestione (MOGC).

Il presente Piano di Prevenzione della corruzione è stato elaborato sulla base di uno scenario in trasformazione che trae origine dalle innovazioni normative che, a far data dal 2016, hanno attribuito nuove competenze all'Autorità Nazionale Anti Corruzione (ANAC), sia nel settore dei contratti pubblici, che nell'ambito della trasparenza e dell'anticorruzione, con particolare riferimento al decreto legislativo 18 aprile 2016, n. 50, recante il "*Il nuovo Codice dei contratti pubblici*" e del decreto legislativo 25 maggio 2016, n. 97, recante "*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*".

Conformemente alle indicazioni fornite dall'ANAC nel 2023, la Società si dota di un Piano Triennale per la Prevenzione della Corruzione (PTPC) per il triennio 2025/2027, in forza del D. Lgs. 33/2013 dettato in applicazione della delega conferita con la citata Legge 190/2012.

Al Documento sono allegati, costituendone parte integrante, adottati dall'Organo Amministrativo:

- il Modello di Organizzazione e Gestione (MOGC);
- il Programma Triennale per la Trasparenza e l'Integrità (PTTI), diretto ad assicurare l'accesso alle informazioni relative all'attività svolta dall'Azienda, volto ad incrementare il controllo sociale ed a concorrere alla realizzazione di una "Società Trasparente", garante di un adeguato livello di trasparenza, legalità e sviluppo della cultura dell'integrità.

Con il presente documento, comprensivo del PTPC, del PTTI, del MOGC e del Codice Etico, DIFESA SERVIZI intende, quindi, contrastare il fenomeno corruttivo attraverso l'adozione di misure a carattere organizzativo e misure di trasparenza e integrità.

**SEZIONE I – PARTE GENERALE -  
MODELLO DI ORGANIZZAZIONE E  
GESTIONE EX D. LGS. N. 231/2001**

## **1. IL QUADRO NORMATIVO DI RIFERIMENTO: IL D. LGS. N. 231/2001 E LA SUA EVOLUZIONE**

Questa Società aveva già predisposto un piano triennale di prevenzione della corruzione per gli anni 2015/2017, 2016/2018, 2017/2019, 2018/2020, 2019/2021, 2021/2023, 2022/2024, 2023/2025, 2024/2026 ed è provveduto ad adeguare il modello 231/2001 con le Linee Guida emanate dall'A.N.A.C. nel 2023 e ad integrarlo con il Piano Triennale approvato.

### **1.1. Il superamento del principio “societas delinquere non potest” e la portata della nuova responsabilità amministrativa da reato**

Il Legislatore italiano, in esecuzione della delega di cui alla Legge n. 300 del 29 settembre 2000, in data 8 giugno 2001 ha emanato il D. Lgs. n. 231/2001 (d'ora in poi, per brevità, anche il ‘Decreto’) “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”, per adeguare la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune Convenzioni Internazionali in precedenza sottoscritte dallo Stato Italiano.

Il Legislatore Delegato, dunque, ponendo fine ad un acceso dibattito dottrinale, ha superato il principio secondo cui “societas delinquere non potest”, introducendo a carico degli enti (gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica), un regime di responsabilità amministrativa (invero, dal punto di vista pratico, assimilabile ad una vera e propria responsabilità penale) nell'ipotesi in cui alcune specifiche fattispecie di reato, come specificato all'art. 5 del Decreto, vengano commesse, nell'interesse o a vantaggio degli enti stessi, da:

- i) soggetti che rivestano funzioni di rappresentanza, amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitino, anche di fatto, la gestione e il controllo dello stesso (si tratta dei c.d. soggetti in posizioni apicale);
- ii) soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto i) (i c.d. soggetti in posizione subordinata).

Non tutti i reati commessi dai soggetti sopra indicati implicano una responsabilità amministrativa riconducibile all'Ente, atteso che sono state individuate come rilevanti solo specifiche tipologie di reati. Quanto alla tipologia dei reati destinati a comportare il suddetto regime di responsabilità amministrativa, il Decreto – nel suo testo originario – si riferiva ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione. Successivamente il legislatore è intervenuto con diversi provvedimenti normativi che hanno ampliato il catalogo dei Reati Presupposto.

Ad oggi, le categorie di Reati Presupposto risultano essere le seguenti:

Si elencano di seguito le categorie di reato attualmente ricomprese nell'ambito di applicazione del D. Lgs. 231/2001:

1. Reati contro la Pubblica Amministrazione, modificati dalla L. n. 190/2012, dalla L. n. 161/2017, dalla L. 3/2019, dal D. Lgs. n. 75/2020, dalla L. n. 137/2023, dalla L. 112/2024 e dalla L. 114/2024 (artt. 24 e 25);
2. Delitti informatici e trattamento illecito di dati, introdotti dalla Legge 48/2008, modificati dal D.Lgs. n. 7 e 8/2016 e dal D.L. 105/2019 (art. 24-bis);
3. Delitti di criminalità organizzata, introdotti dalla Legge 94/2009 e modificati dalla L. 69/2015 (art. 24 ter);
4. Reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, aggiunti dal D. L. n. 350/2001, convertiti con modificazioni dalla L. n. 409/2001, dalla L. n. 99/2009 e dal D. Lgs. 125/2016 (art. 25-bis);
5. Delitti contro l'industria e il commercio, introdotti dalla Legge 99/2009 (art. 25-bis 1);
6. Reati societari, introdotti dal D. Lgs. 61/2002 e modificati dalla Legge 190/2012, dalla Legge 69/2015, dal D. Lgs. 38/2017 e dal D. Lgs. n. 19/2023 (art. 25-ter);

7. Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali, introdotti dalla Legge 7/2003 (art. 25 quater);
8. Pratiche di mutilazione degli organi genitali femminili, introdotti dalla Legge 7/2006 (art. 25–quater. 1);
9. Delitti contro la personalità individuale, introdotti dalla Legge 228/2003 e modificati con la Legge 199/2016 (art. 25 quinquies);
10. Reati di abuso di mercato, introdotti dalla Legge 62/2005 e modificati dal D.Lgs. 107/2018 (art. 25-sexies);
11. Reati transnazionali, introdotti dalla Legge 146/2006;
12. Reati di omicidio colposo e lesioni gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, introdotti dalla Legge 123/2007 da ultimo modificati con la L. n. 3/2018 (art. 25-septies);
13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, introdotti dal D. Lgs. 231/2007, con la Legge 186/2014, e modificati dal D.Lgs. n. 195/2021 (art. 25-octies);
14. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, introdotti dal D. Lgs. 184/2021 e modificati dalla L. n. 137/2023 (Art. 25-octies 1);
15. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti, introdotto dal D.Lgs. 184/2021 (Art. 25-octies 1 comma 2 del Decreto);
16. Delitti in materia di violazione del diritto d'autore, introdotti dalla Legge 99/2009 e modificati dalla L. n. 93/2023 (art. 25-novies);
17. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, introdotto dalla Legge 116/2009 (art. 25-decies);
18. Reati ambientali, introdotti dal D. Lgs. 121/2011, modificati dalla Legge 68/2015, dal D.Lgs. n. 21/2018 e dalla L. n. 137/2023 (art. 25-undecies);
19. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, introdotti nel Decreto dal D. Lgs. 109/2012, modificati dalla L. n. 161/2017 e dal D.L. n. 20/2023 (art. 25-duodecies).
20. Razzismo e xenofobia, introdotti nel Decreto dalla Legge n. 167 del 20 novembre 2017, art. 5 comma 2, e modificati dal D.Lgs. n. 21/2018 (art. 25 terdecies);
21. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, introdotti nel Decreto dalla L. n. 39/2019 (art. 25 quaterdecies);
22. Reati tributari, introdotti dalla Legge n. 157 del 19 dicembre 2019 e modificati con il D. Lgs. n. 75 del 14 luglio 2020 (art. 25-quinquiesdecies);
23. Contrabbando, introdotti dal D. Lgs. n. 75 del 14 luglio 2020 e modificato dal D.Lgs. 141/2024 (art. 25-sexiesdecies);
24. Delitti contro il patrimonio culturale, introdotti dalla Legge 9 marzo 2022 n. 22 e modificato dalla L. n. 6/2024 (artt. 25 duodecies e art. 25 septiesdecies).

L'elenco dei reati sopra indicati è suscettibile di modifiche ed integrazioni da parte del legislatore. Da qui l'esigenza di una costante verifica sull'adeguatezza di quel sistema di regole che costituisce – come

si dirà – il Modello di Organizzazione, Gestione e Controllo, previsto dal Decreto e funzionale alla prevenzione dei reati.

## **1.2. Le sanzioni previste dal D. Lgs. n. 231/2001**

Nell'ipotesi in cui i soggetti di cui all'art. 5 del Decreto commettano uno dei reati previsti dagli artt. 24 e ss. del Decreto o di quelli previsti dalla normativa speciale richiamata, l'Ente potrà subire l'irrogazione di pesanti sanzioni.

Ai sensi dell'art. 9, le sanzioni, denominate amministrative, si distinguono in:

- I. sanzioni pecuniarie;
- II. sanzioni interdittive;
- III. confisca;
- IV. pubblicazione della sentenza.

Dal punto di vista generale è opportuno precisare che l'accertamento della responsabilità dell'Ente, nonché la determinazione dell'*an* e del *quantum* della sanzione, sono attribuiti al Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa.

L'Ente è ritenuto responsabile dei reati individuati dagli artt. 24 e ss. anche se questi siano stati realizzati nelle forme del tentativo. In tali casi, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà.

L'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

### **I. Le sanzioni pecuniarie**

Le sanzioni pecuniarie trovano regolamentazione negli artt. 10, 11 e 12 del Decreto e si applicano in tutti i casi in cui sia riconosciuta la responsabilità dell'Ente. Le sanzioni pecuniarie vengono applicate per "quote", in numero non inferiore a 100 e non superiore a mille, mentre l'importo di ciascuna quota va da un minimo di € 258,23 ad un massimo di € 1.549,37. Il Giudice determina il numero di quote sulla base degli indici individuati dal I comma dell'art. 11, mentre l'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente coinvolto.

### **II. Le sanzioni interdittive**

Le sanzioni interdittive, individuate dal comma II dell'art. 9 del Decreto si applicano, in aggiunta alle sanzioni pecuniarie, soltanto se espressamente previste per il reato per cui l'ente viene condannato e solo nel caso in cui ricorra almeno una delle seguenti condizioni:

- l'ente ha tratto dal reato un profitto rilevante e il reato è stato commesso da un soggetto apicale, o da un soggetto subordinato qualora la commissione del reato sia stata resa possibile da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Quand'anche ricorrano una o entrambe le precedenti condizioni, le sanzioni interdittive non si applicano se sussiste anche solo una delle seguenti circostanze:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità;
- prima della dichiarazione di apertura del dibattimento di primo grado, concorrono tutte le seguenti condizioni:
  - ✓ l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
  - ✓ l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di un Modello;
  - ✓ l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Le sanzioni interdittive previste dal Decreto sono:

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

Come per le sanzioni pecuniarie, il tipo e la durata delle sanzioni interdittive sono determinati dal Giudice penale che conosce del processo per i reati commessi dalle persone fisiche, tenendo conto dei fattori meglio specificati dall'art. 14 del Decreto. In ogni caso, le sanzioni interdittive hanno una durata minima di tre mesi e massima di due anni.

Inoltre, le sanzioni interdittive possono essere applicate all'Ente sia all'esito del giudizio e, quindi, accertata la colpevolezza dello stesso, sia in via cautelare, ovvero quando vi siano:

- gravi indizi per ritenere la sussistenza della responsabilità dell'Ente per un illecito amministrativo dipendente da reato;
- fondati e specifici elementi che facciano ritenere l'esistenza del concreto pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

### III. La confisca

La confisca del prezzo o del profitto del reato è una sanzione obbligatoria che consegue alla eventuale sentenza di condanna (art. 19).

### IV. La pubblicazione della sentenza

La pubblicazione della sentenza è una sanzione eventuale e presuppone l'applicazione di una sanzione interdittiva (art. 18).

Per completezza, infine, deve osservarsi che l'Autorità Giudiziaria può, altresì, disporre:

- a) il sequestro preventivo delle cose di cui è consentita la confisca (art. 53);
- b) il sequestro conservativo dei beni mobili e immobili della società qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54).

### **1.3. L'adozione e l'attuazione di un Modello di Organizzazione, Gestione e Controllo quale esimente della responsabilità amministrativa da reato**

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto, forme specifiche di esonero della responsabilità amministrativa dell'Ente.

In particolare, l'art. 6, comma 1, prescrive che, nell'ipotesi in cui i fatti di reato siano ascrivibili a soggetti in posizione apicale, l'Ente non è ritenuto responsabile se prova che:

- a) ha adottato ed attuato, prima della commissione del fatto, un Modello di Gestione, Organizzazione e Controllo (di seguito, per brevità, anche solo "Modello") idoneo a prevenire reati della specie di quello verificatosi;
- b) ha nominato un Organismo, indipendente e con poteri autonomi, che vigili sul funzionamento e l'osservanza del Modello e ne curi l'aggiornamento (Organismo di Vigilanza; di seguito, anche 'O.d.V.');
- c) il reato è stato commesso eludendo fraudolentemente le misure previste nel Modello;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui al precedente punto b).

Il contenuto del Modello è individuato dallo stesso art. 6, il quale, al comma 2, prevede che la società debba:

- individuare le attività nel cui ambito possono essere commessi i reati;

- prevedere specifici protocolli volti 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 prevenire i reati;
- prevedere obblighi di informazione nei confronti dell'O.d.V.;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello.

Nel caso dei soggetti in posizione subordinata, l'adozione e l'efficace attuazione del Modello importa che l'Ente sarà chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza (combinato di cui ai commi 1 e 2 dell'art. 7). I successivi commi 3 e 4 introducono due principi che sono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'Ente per entrambe le ipotesi di reato di cui all'art. 5, lettere a) e b) (soggetti apicali o in posizione subordinata). Segnatamente, è ivi previsto che:

- il Modello deve prevedere misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge ed a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione; assume rilevanza, altresì, l'esistenza di un idoneo sistema disciplinare (condizione, invero, già prevista dalla lett. e), sub art. 6, comma 2).

Sotto un profilo formale, pertanto, l'adozione ed efficace attuazione di un Modello non costituisce un obbligo, ma unicamente una facoltà per gli Enti, i quali ben potrebbero decidere di non conformarsi al disposto del Decreto senza incorrere, per ciò solo, in alcuna sanzione.

A ben vedere, tuttavia, l'adozione ed efficace attuazione di un Modello idoneo è, per gli Enti, un presupposto irrinunciabile per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, tenere in precipuo conto che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'Ente di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze che, al momento della sua creazione, non era possibile individuare.

Si evidenzia, inoltre, come DIFESA SERVIZI abbia provveduto a nominare un Responsabile per la trasparenza e la corruzione ai sensi della Legge n. 190 del 6 novembre 2012 e del D. Lgs. n. 33 del 13 marzo 2013.

È stata altresì inserita nel presente documento e collocata in una sezione apposita del modello la versione aggiornata del PTPC.

## **2. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI DIFESA SERVIZI**

### **2.1. DIFESA SERVIZI S.P.A. e la sua *mission***

DIFESA SERVIZI è stata costituita ai sensi dell'art. 535 del D. Lgs. n. 66 del 15 marzo 2010, come modificato dall'art. 1, comma 380, della legge 23 dicembre 2014, n. 190 (legge di stabilità 2015).

La Società è interamente controllata dal Ministero della Difesa che ne determina gli indirizzi strategici. La sede sociale è attualmente ubicata a Roma, in Via Flaminia, 335.

La missione della Società è quella di valorizzare, nel rispetto dei principi fissati dallo Statuto, approvato con Decreto del Ministro della Difesa, di concerto con il Ministro dell'Economia e delle Finanze, in data 28 gennaio 2022, beni mobili, immobili ed immateriali del Ministero della Difesa.

DIFESA SERVIZI instaura e sviluppa rapporti di collaborazione con le Amministrazioni statali, regionali e provinciali, nonché con gli altri Enti Pubblici anche locali e con le Aziende private.

Nello svolgimento della propria attività aziendale, in ragione della peculiarità dei beni oggetto della sua gestione, nonché dell'importanza dei compiti ad essa demandati, DIFESA SERVIZI mantiene una costante attenzione alle attese della collettività e degli interlocutori.

DIFESA SERVIZI dedica grande considerazione agli aspetti etici dell'impresa e adotta le migliori tecniche disponibili per la mitigazione degli impatti derivanti dalle proprie attività.

La *mission* aziendale è garantita da un sistema di *governance* adeguato alla dimensione e struttura aziendale (sul punto si veda infra, capitolo 4).

In tale contesto, DIFESA SERVIZI ha ritenuto di ottemperare alle disposizioni di cui al Decreto in modo da implementare un sistema strutturato ed idoneo a prevenire il rischio del verificarsi di ogni forma di irregolarità nello svolgimento dell'attività d'impresa, così da limitare il pericolo di commissione dei reati e garantire la correttezza e la trasparenza della propria attività.

## **2.2. Le componenti del Modello di DIFESA SERVIZI S.P.A.**

Il Documento è costituito da una Parte Generale e da una Parte Speciale.

Nella Parte Generale, dopo aver effettuato una breve ma necessaria illustrazione della *ratio* e dei principi del Decreto, oltre ad una sintetica ricognizione delle previsioni di cui al documento "Disciplina e compiti dell'O.d.V." dedicato alla regolamentazione dell'O.d.V., sono compendiate i protocolli sottoindicati (di seguito, i 'Protocolli'), che compongono il Modello di DIFESA SERVIZI:

- il sistema organizzativo;
- il sistema di procure e deleghe;
- le procedure manuali ed informatiche;
- il sistema di controllo di gestione;
- il Codice Etico;
- il Sistema Disciplinare;
- la comunicazione e la formazione al personale sul Modello.

La Parte Speciale ha l'obiettivo di illustrare i criteri e di regolamentare ruoli, responsabilità e norme comportamentali cui i destinatari, devono attenersi nella gestione delle attività a rischio connesse con le fattispecie individuate dal D. Lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività. Sono tenuti all'osservanza delle medesime norme comportamentali, degli stessi principi e delle regole di seguito definite i Consulenti, i Collaboratori ed i Fornitori che esplicano, per conto di DIFESA SERVIZI, attività aventi ad oggetto rapporti ed adempimenti verso la Pubblica Amministrazione.

Nell'ambito della Parte Speciale, sono stati indicati, seguendo anche l'approccio metodologico in precedenza illustrato:

- i) le aree ritenute "a rischio reato" e le attività sensibili;
- ii) le funzioni e/o i servizi societari che operano nell'ambito delle aree a rischio reato o delle attività sensibili;
- iii) i reati astrattamente perpetrabili;
- iv) le aree ritenute "strumentali", nonché i soggetti che in esse agiscono;
- v) i principi di comportamento da rispettare al fine di ridurre il rischio di commissione dei reati;
- vi) i compiti spettanti all'O.d.V. al fine di prevenire il pericolo di commissione dei reati.

## **3. IL MODELLO DI *GOVERNANCE* ED IL SISTEMA ORGANIZZATIVO DI DIFESA SERVIZI**

Il modello di *governance* di DIFESA SERVIZI e, in generale, tutto il suo sistema organizzativo, è strutturato in modo da assicurare alla Società l'attuazione delle strategie ed il raggiungimento degli obiettivi.

La struttura di DIFESA SERVIZI, infatti, è stata creata tenendo conto della necessità di dotare la Società di una organizzazione tale da garantirle un adeguato livello di efficienza ed efficacia operativa.

### **3.1. Il modello di *governance* di DIFESA SERVIZI**

Alla luce della peculiarità della propria struttura organizzativa e delle attività svolte, DIFESA SERVIZI ha privilegiato il c.d. sistema tradizionale.

Il sistema di *governance* di DIFESA SERVIZI risulta, pertanto, attualmente così articolato:

Assemblea: L'Assemblea (Socio Unico) è competente a deliberare, in sede ordinaria e straordinaria, sulle materie alla stessa riservate dalla legge (art. 535 del D. Lgs. 15-3-2010 n. 66 "Codice dell'ordinamento militare") e dallo Statuto.

**L'Assemblea del 22 maggio 2023 ha deliberato di determinare il limite, oltre il quale è prevista la Sua autorizzazione per consentire al Consiglio di Amministrazione di porre in essere le relative operazioni, sia attive sia passive, nella misura di € 5.000.000,00 (cinquemilioni).**

Consiglio di Amministrazione: Il Consiglio di Amministrazione è investito dei più ampi poteri per l'amministrazione della Società e per l'attuazione ed il raggiungimento dello scopo sociale, nei limiti di quanto consentito dalla legge e dallo Statuto. Al Consiglio di Amministrazione risulta, quindi, tra l'altro, conferito il potere di individuare le strategie aziendali e verificare i relativi risultati.

La suddetta **Assemblea del 22 maggio 2023** ha deliberato che, fermo restando *ex* art. 2381 co. 3 Codice Civile il potere del Consiglio di avocare a sé le operazioni rientranti nella delega dell'Amministratore Delegato, è necessaria l'approvazione del C.d.A. per operazioni di valore superiore a:

- € 500.000,00 per acquisti di beni strumentali e contratti passivi;
- € 2.000.000,00 per contratti attivi.

Il Consiglio di Amministrazione della DIFESA SERVIZI è composto, a mente dello Statuto, da 5 consiglieri.

Amministratore delegato: L'Amministratore Delegato esercita per le materie delegate la rappresentanza legale della Società, sostanziale e processuale, attiva e passiva, ed in tale ambito esercita anche la gestione ordinaria, ferme restando le prerogative riservate al Consiglio.

**In particolare, il Consiglio di Amministrazione del 15 maggio 2023 ha attribuito**, ai sensi degli artt. 19 e 21 dello Statuto, all'Amministratore Delegato le seguenti deleghe a firma singola:

- a) predisporre la struttura organizzativa della Società da sottoporre, previa delibera del Consiglio di amministrazione, all'approvazione dell'Assemblea;
- b) curare che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura ed alle dimensioni della Società;
- c) gestire e coordinare la struttura interna della Società, sia di linea che di *staff*;
- d) assumere, con preventivo assenso del Ministro della difesa, sospendere e licenziare personale esterno, nonché fissarne il trattamento economico ed eventuali successive variazioni;
- e) sottoscrivere con le articolazioni della Difesa le convenzioni per l'attuazione del contratto di servizio, previste dall'art. 5, comma 3 dello Statuto;
- f) costituire, modificare ed estinguere negozi giuridici attivi, quali atti e contratti fonte di ricavo per la Società, entro il limite di € 2.000.000,00 (due milioni) per ciascun atto-contratto;
- g) accendere rapporti bancari e postali attivi, con esclusione di quelli passivi, ed operare sui medesimi entro i limiti degli importi disponibili ivi compreso, a titolo esemplificativo e non esaustivo:
  - i. richiedere e ritirare libretti di moduli di assegni da emettere a valere sui conti corrente e dare il benestare agli estratti conto relativi ai conti corrente medesimi;
  - ii. effettuare versamenti sui conti corrente;
  - iii. effettuare prelievi sui conti corrente;
  - iv. emettere ordini di pagamento, mandati di pagamento, cambiali, assegni e bonifici a favore di terzi sui conti corrente;
  - v. girare per l'incasso, sui conti corrente, assegni bancari e altri titoli all'ordine;
  - vi. rilasciare quietanze di pagamento ed accettazioni cambiali in favore di terzi;
  - vii. emettere e sottoscrivere ordini di bonifico per effettuare trasferimenti di denaro (giroconti) tra i conti corrente;

- h) costituire, modificare ed estinguere negozi giuridici passivi, quali atti e contratti fonte di costo o di acquisto di beni strumentali, materiali ed immateriali, per la Società, entro il limite di € 500.000,00 (cinquecentomila) per ciascun atto-contratto;
- i) predisporre entro l'anno precedente i budget annuali della Società da sottoporre per la loro discussione ed approvazione al Consiglio di amministrazione;
- j) instaurare, proseguire e resistere in ogni tipo di giudizio, in tutte le sedi e presso tutte le autorità e corti consentite dalla legge;
- k) definire i termini di eventuali transazioni e conciliazioni giudiziali e stragiudiziali, entro il limite di € 500.000,00 (cinquecentomila) per singola transazione o conciliazione, in sede ordinaria, speciale ed amministrativa, nonché presentare atti, ricorsi, querele, esposti e denunce alle autorità competenti;
- l) delegare, al fine di agevolare la gestione operativa, singoli dirigenti della Società, addetti a particolari funzioni per il compimento di particolari atti;
- m) nominare procuratori speciali per il compimento di determinati atti rientranti nei suoi poteri o in quelli espressamente conferitigli dal Consiglio di amministrazione ovvero dall'Assemblea;
- n) dare attuazione a tutte le deliberazioni del Consiglio di amministrazione compiendo altresì tutti gli atti, nonché tutte le operazioni ad esse collegate.

L'Amministratore Delegato, inoltre, ai sensi dell'art. 21 comma 2 dello Statuto, riferisce al Consiglio di Amministrazione ed al Collegio Sindacale almeno ogni tre mesi sul generale andamento della gestione e sulla sua prevedibile evoluzione, nonché sulle operazioni di maggior rilievo, per le loro dimensioni o caratteristiche, effettuate dalla Società.

Collegio Sindacale: Il Collegio Sindacale è composto da 3 membri effettivi e 2 supplenti scelti tra gli iscritti nel registro dei revisori contabili istituito presso il Ministero della Giustizia. Al Collegio Sindacale sono affidati i compiti previsti dalla legge e dallo statuto.

I Sindaci durano in carica per 3 esercizi e sono rieleggibili una sola volta.

Magistrato della Corte dei Conti: Un magistrato della Corte dei Conti, nominato dal Presidente della Corte medesima, svolge le funzioni di delegato al controllo sulla gestione finanziaria ed assiste alle sedute degli organi di amministrazione e del Collegio sindacale della Società.

Inoltre, tenuto conto della possibilità offerta dal decreto del Ministro della difesa del 27 febbraio 2019, il Consiglio di amministrazione ha proposto di esercitare la facoltà ivi disciplinata, mediante l'affidamento all'OIV della Difesa del compito di svolgere il controllo strategico e di sottoporre la decisione alla successiva deliberazione del Socio, che ha approvato.

## **3.2. L'assetto organizzativo di DIFESA SERVIZI**

### **3.2.1. Le Aree Aziendali**

La struttura organizzativa della Società è orientata a garantire, da un lato, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, dall'altro, la massima efficienza possibile. La struttura organizzativa aziendale è improntata ad una precisa definizione delle competenze e delle connesse responsabilità.

In particolare, in seguito alla delibera dell'Assemblea del 20 settembre 2023, è stato adottato un nuovo modello organizzativo suddiviso in Livelli e Aree/Unità organizzative.

Oltre al Livello *Corporate*, composto dal Consiglio di Amministrazione, dal Presidente e dall'Amministratore delegato, la struttura è così articolata:

- Livello consultivo composto da:
  - Comitato Tecnico Scientifico;
  - Comitato dei Referenti di Forza Armata;
- Livello di *Staff* e supporto composto da:

- Direzione Affari Legali, Qualità e Rapporto Industriali;
  - Direzione Risorse Umane e Innovazione Tecnologica;
  - Direzione Amministrazione, Finanza e Controllo;
  - Direzione Relazioni Istituzionali e Sviluppo;
  - Area Comunicazione;
  - Segreteria del CDA e del Presidente.
- Livello Operativo, retto da un Direttore Generale, ed articolato in:
- Divisione Brand e Media;
  - Divisione Innovazione e Tecnologie;
  - Divisione Patrimonio;
  - Divisione Cultura e Professioni;
  - Direzione Gare, Contratti e Centrale di Committenza;

A tutte le Articolazioni è conferito il potere di compiere gli atti attinenti alle proprie competenze e necessari per il raggiungimento degli obiettivi assegnati.

### **3.2.2. Definizione dell'organigramma aziendale e dei compiti**

Al fine di rendere immediatamente chiaro il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale, DIFESA SERVIZI ha messo a punto un prospetto sintetico nel quale è schematizzata l'intera struttura organizzativa della Società (Organigramma in Allegato 1).

Nell'Organigramma, in particolare, sono specificate:

- le aree in cui si suddivide l'attività aziendale;
- le linee di dipendenza gerarchica;
- i soggetti che operano nelle singole aree ed il relativo ruolo organizzativo.

La Società, come anticipato, si è dotata anche di un dettagliato Regolamento organizzativo (Funzionigramma), ove sono rappresentate le Strutture organizzative. Per ogni Articolazione è riportata la *mission* specifica, che sintetizza le finalità della stessa. Per le unità organizzative sono riportate le principali aree di responsabilità.

Tali documenti, che specificano precisamente la struttura organizzativa ed i compiti del personale sono oggetto di costante e puntuale aggiornamento in funzione dei cambiamenti effettivamente intervenuti nella struttura organizzativa.

I documenti di sintesi indicati sono oggetto di ufficiale comunicazione a tutto il personale della Società, anche attraverso la loro pubblicazione sulla rete intranet aziendale.

## **4. IL SISTEMA DI INCARICHI IN DIFESA SERVIZI**

### **4.1. I principi generali**

Così come richiesto dalla *best practice* aziendale, il Consiglio di Amministrazione di DIFESA SERVIZI è l'organo preposto a conferire ed approvare formalmente gli incarichi ed i connessi poteri di firma, assegnati in coerenza con le responsabilità organizzative e gestionali definite e prevedendo una puntuale indicazione delle soglie di approvazione delle spese.

Il livello di autonomia ed il potere di rappresentanza attribuiti ai vari titolari di incarichi e procure all'interno della Società devono sempre essere individuati e fissati in stretta coerenza con il livello gerarchico del destinatario dell'incarico o della procura o in relazione a specifiche attività.

I poteri così conferiti devono essere periodicamente aggiornati in funzione dei cambiamenti organizzativi intervenuti nella struttura della Società.

#### **4.2. Il sistema di deleghe e procure**

Ai fini di una corretta ed efficiente gestione dell'attività aziendale, è definito un sistema di deleghe e procure volte a:

- gestire i riporti funzionali;
- disegnare controlli di primo livello verso le operazioni sensibili;
- stabilire regole di operatività secondo i già citati criteri di definizione dei ruoli e di tracciabilità delle operazioni svolte.

Al fine di svolgere un'efficace prevenzione dei Reati, è possibile individuare alcuni requisiti del sistema di deleghe che si ritiene debbano sempre essere assicurati e monitorati nell'ambito dell'operatività di DIFESA SERVIZI S.p.A.:

- a) tutti coloro che, per conto di DIFESA SERVIZI S.p.A., assumono impegni con la P.A. devono essere dotati di delega formale in tal senso;
- b) le deleghe devono rispettare regole di coerenza con la posizione ricoperta dal delegato all'interno di DIFESA SERVIZI S.p.A., evitando potenziali disallineamenti tra l'incarico svolto in ambito societario ed i poteri a lui delegati;
- c) le deleghe devono definire i poteri del delegato ed i riporti gerarchici che questi è tenuto a rispettare;
- d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- e) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

Inoltre:

1. le procure generali devono essere conferite esclusivamente a soggetti dotati di delega interna e devono definire i limiti di spesa, nonché i limiti che il procuratore deve rispettare nell'ambito dell'assunzione dei rischi;
2. le procure possono essere conferite a persone fisiche espressamente individuate nella procura stessa, oppure a persone giuridiche che agiranno a mezzo di propri procuratori investiti, nell'ambito della stessa, di analoghi poteri;
3. deve essere prevista una procedura mirante ad assicurare la gestione ed il costante aggiornamento delle procure, in presenza di attribuzioni, modifiche o revoche.

Al fine di assicurare un efficace controllo sul sistema delle deleghe e procure, tutti gli eventi relativi ad attribuzioni, modifiche, revoche devono essere comunicati all'OdV sulla base di una cadenza temporale definita dall'Organismo stesso. Nell'ambito dei compiti attribuiti all'Organismo è altresì previsto che lo stesso proceda allo svolgimento di verifiche periodiche, anche con il supporto di funzioni competenti, del sistema di deleghe e procure in vigore e della coerenza degli stessi con il potere di gestione del delegato o del procuratore.

#### **4.3. La struttura del sistema di incarichi in Difesa Servizi**

Il sistema di incarichi e procure attualmente in vigore in DIFESA SERVIZI ripercorre fedelmente il quadro che emerge dall'Organigramma e dal Regolamento organizzativo, sovrapponendosi esattamente allo stesso.

In particolare:

- l'Assemblea ha poteri di gestione per importi superiori a € 5.000.000,00;
- il Consiglio di amministrazione ha il potere di porre in essere le operazioni, sia attive sia passive, fino a € 5.000.000,00;
- l'Amministratore Delegato, come detto, ha poteri di gestione e di firma fino a:
  - € 500.000,00 per acquisti di beni strumentali e contratti passivi;
  - € 2.000.000,00 per contratti attivi.

### **5. PROCEDURE MANUALI ED INFORMATICHE**

Nell'ambito del proprio sistema organizzativo, DIFESA SERVIZI ha messo a punto alcune procedure volte a regolamentare gli aspetti salienti delle attività aziendali.

In particolare, le procedure approntate dalla Società, sia manuali sia informatiche, costituiscono le regole da seguire in seno ai processi aziendali interessati, prevedendo anche i controlli da espletare al fine di garantire la correttezza, l'efficacia e l'efficienza delle attività aziendali.

Quanto, specificatamente, alle procedure informatiche può indicarsi, in estrema sintesi, che i principali sistemi di gestione della Direzione Amministrazione, Finanza e Controllo sono supportati da applicativi informatici di alto livello qualitativo. Essi assicurano un elevato livello di standardizzazione e di *compliance*.

In questo contesto, pertanto, la Società mira ad assicurare il rispetto dei seguenti principi:

- favorire il coinvolgimento di più soggetti, onde addivenire ad una adeguata separazione dei compiti mediante la distinzione delle funzioni;
- adottare le misure volte a garantire che ogni operazione, transazione, azione sia verificabile, documentata, coerente e congrua;
- prescrivere l'adozione di misure volte a documentare i controlli espletati rispetto alle operazioni e/o alle azioni effettuate.

Le procedure, oltre ad essere diffuse e pubblicizzate presso le Funzioni interessate attraverso specifica comunicazione e formazione, vengono raccolte e poste a disposizione di tutti i soggetti aziendali sia a mezzo della pubblicazione sulla intranet aziendale sia presso la sede della Società.

A tale sistema si affianca la struttura informatica, tecnologica e procedurale prevista dal GDPR, ufficialmente regolamento n. 2016/679 dell'Unione europea in materia di trattamento dei dati personali e di privacy, promulgato il 25 maggio 2018.

## **6. IL CONTROLLO DI GESTIONE ED I FLUSSI FINANZIARI**

Il sistema di controllo di gestione (di seguito, anche “Controllo di Gestione”) di DIFESA SERVIZI prevede meccanismi di verifica della gestione delle risorse che devono garantire l'efficienza e l'economicità delle attività aziendali, mirando ai seguenti obiettivi:

- definire in maniera chiara, sistematica e conoscibile le risorse (monetarie e non) a disposizione delle singole funzioni aziendali ed il perimetro nell'ambito del quale tali risorse possono essere impiegate, attraverso la programmazione e definizione del *budget*;
- rilevare, con periodici *forecast*, gli eventuali scostamenti rispetto a quanto predefinito in sede di *budget*, analizzarne le cause e riferire i risultati delle valutazioni a consuntivo agli appropriati livelli gerarchici per gli opportuni interventi di adeguamento.

La rilevazione periodica di ogni eventuale scostamento dei dati correnti rispetto alle previsioni di *budget* assicura la rispondenza dei dati effettivi con quelli programmati (ed approvati) ad inizio esercizio.

Qualora, in fase di verifica periodica, emergano significativi scostamenti dal *budget* o anomalie di spesa, la Direzione Amministrazione, Finanza e Controllo provvede ad informare l'O.d.V.

### **6.1. Fase di programmazione e di definizione del *budget***

Il processo di preparazione del *budget* viene effettuato dopo la definizione del piano strategico, prendendo in considerazione orizzonti temporali di definizione dello stesso che siano coerenti con il tipo di attività svolta. La coerenza del *budget* con i piani strategici della società viene garantita dal controllo effettuato da parte del Consiglio di Amministrazione. In tale sede, il Consiglio di Amministrazione, qualora lo ritenga opportuno, può richiedere chiarimenti alle Aree interessate.

Il *budget* annuale è rivisto ed approvato dal Consiglio di Amministrazione; esso è determinato sulla base di obiettivi di *business* “ragionevoli”; nella definizione degli obiettivi da raggiungere sono adeguatamente analizzati e presi in considerazione i risultati degli anni precedenti.

## **6.2. Fase consuntiva ed analisi degli scostamenti**

Periodicamente, con cadenza almeno trimestrale, vengono effettuate delle analisi – i suddetti *forecast* - volte a valutare l'entità degli scostamenti dei dati a consuntivo rispetto a quelli previsti a *budget* e di tale andamento viene informato il Consiglio di Amministrazione.

## **7. L'ORGANISMO DI VIGILANZA DI DIFESA SERVIZI**

### **7.1. La composizione dell'Organismo ed i suoi requisiti**

In conformità a quanto previsto dalle Linee Guida delle Associazioni di riferimento, in ragione della sua dimensione e della sua organizzazione, la Società ha optato per la nomina – da parte del Consiglio di Amministrazione – di un Organismo di Vigilanza collegiale. L'O.d.V., costituito da tre componenti, è composto da personale interno dell'Ente oltre che da un Presidente esterno.

Come è stata consuetudine fino al 2023, il Presidente dell'O.d.V. è stato scelto tra i Vice Capi di Gabinetto, con particolare riferimento all'Ufficiale Generale cui fanno capo – pro tempore – le articolazioni interne all'UG che trattano le materie di competenza di questa Società.

Da ultimo, il Consiglio di Amministrazione della Società, nella seduta del 6 dicembre 2023, ha deliberato di rinnovare la composizione dell'intero Organismo, con decorrenza dal 1 gennaio 2024 e per la durata di un triennio, individuando la carica di Presidente tra professionisti esterni al Dicastero, che operano prevalentemente nello specifico settore.

In conformità a quanto previsto dalle suddette Linee Guida, l'O.d.V. di DIFESA SERVIZI si caratterizza per rispondere ai seguenti requisiti:

- autonomia e indipendenza: tali requisiti si riferiscono all'Organo in quanto tale e caratterizzano la sua azione. A questo proposito, è previsto che l'O.d.V. sia privo di compiti operativi, i quali, facendolo partecipare a decisioni o attività dell'Ente, potrebbero ledere l'obiettività di giudizio;
- professionalità: intesa come insieme di strumenti e tecniche necessari allo svolgimento dell'attività assegnata, sia di carattere ispettivo che consulenziale;
- continuità di azione: per garantire una efficace e costante attuazione del Modello, la struttura dell'O.d.V. è provvista di adeguate risorse ed è dedicata stabilmente all'attività di vigilanza;
- onorabilità ed assenza di conflitti di interessi: da intendersi nei medesimi termini previsti dalla legge con riferimento ad amministratori e membri del Collegio Sindacale.

Il venir meno dei predetti requisiti determina la decadenza dall'incarico. In tal caso il Consiglio di Amministrazione provvede, tempestivamente, alla nomina del sostituto del membro decaduto, nel rispetto del principio e dei requisiti precedentemente descritti.

Il membro dell'ODV è in qualunque momento revocabile per giusta causa e/o per giustificato motivo dal Consiglio di Amministrazione, che deve provvedere tempestivamente alla sua sostituzione.

L'ODV si potrà, se necessario, servire della collaborazione di soggetti esterni qualificati, avvalendosi delle rispettive competenze al fine di assicurare un elevato livello di professionalità e di continuità d'azione.

### **7.2. I compiti ed i poteri dell'Organismo di Vigilanza**

In conformità al disposto di cui all'art. 6, I comma del Decreto, all'Organismo di Vigilanza sono affidati i seguenti compiti e poteri:

- vigilare sull'osservanza del Modello e sull'efficacia dello stesso e verificarne l'adeguatezza e la sua efficacia nel prevenire i comportamenti illeciti;
- promuovere la diffusione, la conoscenza e la comprensione del Modello all'interno della società fornendone le istruzioni, i chiarimenti necessari ed istituendo specifici corsi di formazione se necessari;
- mantenere aggiornato il Modello Organizzativo apportando le eventuali correzioni che si rendessero necessarie per adeguarlo all'evoluzione della legge, o in conseguenza delle modifiche dell'organizzazione interna e dell'attività aziendale;

- effettuare periodicamente verifiche mirate;
- collaborare alla predisposizione ed integrazione dei codici comportamentali interni;
- accedere a tutte le attività svolte dalla Società ed alla relativa documentazione, ove attività rilevanti o potenzialmente rilevanti siano affidate a terzi, l'Organismo deve poter accedere anche alle attività svolte da detti soggetti;
- disporre verifiche straordinarie e/o indagini mirate laddove si evidenzino disfunzioni del Modello o si sia verificata la commissione di reati oggetto delle attività di prevenzione;
- vigilare sul rispetto e l'applicazione del Modello Organizzativo e attivare le procedure per le proposte di eventuali provvedimenti sanzionatori secondo la diversa tipologia prevista;
- identificare e monitorare adeguatamente i rischi di cui al D. Lgs. 231/2001 rispetto ai reali processi aziendali, procedendo ad un costante aggiornamento dell'attività di rilevazione e mappatura dei rischi di reato;
- riferire tempestivamente al Consiglio di Amministrazione qualsiasi violazione del Modello.

La frequenza di convocazione dell'ODV è, di norma, semestrale, salvo specifiche esigenze che richiedano una maggior frequenza, a seguito di rilevanti evoluzioni del quadro normativo, di incidenti, anomalie gestionali o specifiche segnalazioni.

### **7.3. I flussi informativi che interessano l'Organismo di Vigilanza**

Il Decreto enuncia, tra le esigenze che il Modello deve soddisfare, l'istituzione di obblighi informativi nei confronti dell'Organismo di Vigilanza. Detti flussi riguardano tutte le informazioni e i documenti che devono essere portati a conoscenza dell'Organismo di Vigilanza. Devono essere obbligatoriamente e immediatamente trasmesse all'O.d.V. le informazioni:

A) che possono avere attinenza con violazioni, anche potenziali, del Modello, incluse, senza che ciò costituisca limitazione:

- 1) eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna o il Modello;
- 2) eventuali richieste od offerte di doni (eccedenti il valore modico) o di altre utilità provenienti e/o rivolte da/a pubblici ufficiali o incaricati di pubblico servizio;
- 3) eventuali scostamenti significativi dal *budget* o anomalie di spesa emersi in fase di verifica periodica;
- 4) eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- 5) i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini che interessano, anche indirettamente, la Società, i suoi dipendenti o i componenti degli organi sociali;
- 6) le richieste di assistenza legale inoltrate alla società dai dipendenti ai sensi del CCNL, in caso dell'avvio di un procedimento penale a carico degli stessi;
- 7) le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione;

B) relative all'attività della Società, che possono assumere rilevanza quanto all'espletamento da parte dell'O.d.V. dei compiti ad esso assegnati, incluse, senza che ciò costituisca limitazione:

- 1) le notizie relative ai cambiamenti organizzativi;
- 2) gli aggiornamenti del sistema dei poteri e delle deleghe;
- 3) le eventuali comunicazioni della società di revisione riguardanti aspetti che possono indicare una carenza dei controlli interni;
- 4) le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici, ove ricorrenti;
- 5) i prospetti riepilogativi delle gare, pubbliche o a rilevanza pubblica, che la Società ha indetto, nonché i prospetti riepilogativi delle trattative private.

È stato istituito un canale di comunicazione per la consultazione dell'Organismo di Vigilanza, consistente in un indirizzo di posta elettronica dedicato ([odv@difesaservizi.it](mailto:odv@difesaservizi.it)).

Quanto all'attività di *reporting* dell'O.d.V. agli organi societari, in sintesi, si rammenta che l'O.d.V.:

- in ogni momento, in presenza di particolari necessità o in caso di urgenza, relaziona al Consiglio di Amministrazione, il quale assume le determinazioni più opportune;
- relaziona per iscritto, su base annuale, al Consiglio di Amministrazione ed al Collegio Sindacale sull'attività compiuta nel periodo e sull'esito della stessa, fornendo pure una anticipazione sulle linee generali di intervento per l'anno successivo.

L'attività di *reporting* avrà ad oggetto, in particolare:

- l'attività, in genere, svolta dall'O.d.V.;
- eventuali problematiche o criticità che si siano evidenziate nel corso dell'attività di vigilanza;
- i correttivi, necessari o eventuali, da apportare al fine di assicurare l'efficacia e l'effettività del Modello;
- l'accertamento di comportamenti non in linea con il Modello;
- la rilevazione di carenze organizzative o procedurali tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto;
- l'eventuale mancata o carente collaborazione da parte delle funzioni aziendali nell'espletamento dei propri compiti di verifica e/o d'indagine;
- in ogni caso, qualsiasi informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte degli organi deputati.

Gli incontri devono essere verbalizzati e le copie dei verbali devono essere conservate presso gli uffici dell'O.d.V. o della Direzione Affari Legali, Qualità e Relazioni Industriali della Società.

#### **7.4. Whistleblowing**

Il 30 marzo 2023 è entrato in vigore il Decreto Legislativo 10 marzo 2023, n. 24, che recepisce la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019. Il Decreto, pubblicato sulla Gazzetta Ufficiale n. 63 del 15 marzo 2023, introduce una normativa strutturata per garantire la protezione dei *whistleblowers* (segnalanti), ovvero persone che, in ambito lavorativo pubblico o privato, segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che compromettono l'interesse pubblico o l'integrità di un'amministrazione pubblica o di un'organizzazione privata.

La disciplina riconosce tutela non solo ai soggetti che segnalano condotte idonee a configurare reati rilevanti ai sensi del D.Lgs. 231/2001 o violazioni del relativo Modello 231, ma anche a coloro che evidenziano violazioni di norme nazionali o europee nei settori specificamente indicati all'articolo 2 del Decreto.

Il Decreto in esame disciplina nello specifico quanto segue:

##### **1) Definizione dei soggetti legittimati ad effettuare segnalazioni (*whistleblowers*)**

Sono legittimati ad effettuare segnalazioni i seguenti soggetti:

- Dipendenti;
- Collaboratori;
- Fornitori, subfornitori e dipendenti e collaboratori degli stessi;
- Liberi professionisti, consulenti, lavoratori autonomi;
- Volontari e tirocinanti, retribuiti o non retribuiti;
- Azionisti o persone con funzione di amministrazione, direzione, vigilanza, controllo o rappresentanza;
- Ex dipendenti, ex collaboratori o persone che non ricoprono più una delle posizioni indicate in precedenza;

- Soggetti in fase di selezione, di prova o il cui rapporto giuridico con l'ente non sia ancora iniziato.

## 2) Definizione del contenuto della segnalazione *Whistleblowing*

La segnalazione *Whistleblowing* può avere ad oggetto:

- a. violazioni di disposizioni normative nazionali: illeciti amministrativi, contabili, civili o penali; condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231 (reati presupposto a titolo esemplificativo: Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture), o violazioni del Modello 231 della Società;
- b. violazione di disposizioni normative europee: illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; atti od omissioni che ledono gli interessi finanziari dell'Unione; atti od omissioni riguardanti il mercato interno (a titolo esemplificativo: violazioni in materia di concorrenza e di aiuti di Stato); atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

La Società ha adottato un'apposita Procedura aziendale "Modello di Procedura di gestione delle segnalazioni" (cui si rimanda), disciplinante le modalità di gestione delle segnalazioni, al fine di migliorare l'efficacia dello strumento e permettere una gestione più efficace delle segnalazioni, alla quale si rinvia per quanto non previsto nel presente paragrafo.

La suddetta procedura fornisce indicazioni operative circa l'oggetto, il contenuto, i destinatari e le modalità di trasmissione delle segnalazioni ed esplicita le forme di tutela e di garanzia che l'ordinamento riconosce al *whistleblower*.

Con riguardo ai canali interni di segnalazione interna, è stata implementata, una piattaforma di segnalazione online. In particolare, le segnalazioni possono essere formulate accedendo al sito <https://www.difesaservizi.whistleblowing.it>. Le segnalazioni possono essere effettuate tramite questo portale in modo assolutamente anonimo.

Sempre in linea con quanto previsto dal D.lgs. n. 24/2023 e nel rispetto delle misure in esso indicate, è possibile effettuare segnalazioni in forma orale ovvero richiedere un incontro diretto con i soggetti responsabili della gestione della segnalazione.

Per ulteriori dettagli di rimanda alla procedura summenzionata.

### **7.4.1. Obblighi di riservatezza e tutela del segnalante**

I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengono in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello.

I componenti dell'OdV si astengono, altresì, dall'utilizzare informazioni riservate per fini diversi da quelli di cui ai precedenti paragrafi e comunque per scopi non conformi alle funzioni proprie di un organismo di vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

L'inosservanza di tali obblighi costituisce giusta causa di revoca della carica.

In ogni caso – come anticipato – la Società adotta tutte le misure necessarie per garantire che sia assicurato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

In particolare, l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale eventualmente indicata dal medesimo.

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

Da ultimo, si precisa che, nelle ipotesi di segnalazione o denuncia effettuate nelle forme e nei limiti di legge, il perseguimento dell'interesse all'integrità dell'ente, nonché alla prevenzione e alla repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli artt. 326, 622 e 623 c.p. e all'articolo 2105 c.c. (fatto salvo il caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata). Quando notizie e documenti che sono comunicati all'organo deputato a riceverli siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

La Società garantisce l'applicazione di misure di protezione (i.e. tutela della riservatezza, protezione delle ritorsioni, limitazione delle responsabilità, misure di sostegno) previste dalla normativa vigente, a favore dei segnalanti, nonché ai seguenti soggetti:

- facilitatore ovvero la persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere riservata; persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- enti di proprietà della persona segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Il gestore della segnalazione è tenuto a valutare che, al momento della segnalazione, il segnalante avesse fondati motivi per credere che i fatti riportati fossero veri. La tutela cessa nel caso in cui sia confermata l'irrilevanza delle motivazioni del segnalante ed anche in caso di condanna in primo grado per diffamazione o calunnia.

## **8. IL CODICE ETICO DI DIFESA SERVIZI**

### **8.1. Elaborazione ed approvazione del Codice Etico**

DIFESA SERVIZI, avendo ben presente l'importante ruolo ad essa affidato, cura da sempre, e con particolare attenzione, la valorizzazione e la salvaguardia dei profili etici della propria attività d'impresa, avendo individuato quale valore centrale della propria cultura e dei propri comportamenti il concetto di "integrità".

Contestualmente all'approvazione del presente Modello, DIFESA SERVIZI ha determinato di aggiornare "Codice Etico" che costituisce parte integrante del Modello, anche in ottemperanza alle

Linee Guida emanate dall'ANAC, attribuendo particolare importanza ai comportamenti rilevanti ai fini della prevenzione dei reati di corruzione.

Il Codice Etico attualmente vigente costituisce il punto di riferimento per fornire l'indirizzo etico di tutte le attività della Società.

## **8.2. Finalità, struttura e destinatari del Codice Etico**

Il Codice Etico di DIFESA SERVIZI indica i principi generali e le regole comportamentali cui la Società riconosce valore etico positivo ed a cui devono conformarsi tutti i destinatari del Codice stesso. Al fine di garantire una piena effettività delle previsioni del Codice Etico, sono tenuti all'osservanza dei principi etici e delle norme di comportamento ivi indicati, senza alcuna eccezione, gli amministratori e i sindaci (organi sociali), i dipendenti, inclusi i dirigenti (di seguito, per brevità, congiuntamente indicati quali "Personale"), nonché tutti coloro che, pur esterni alla Società, operino, direttamente o indirettamente, stabilmente o temporaneamente, per essa (es., procuratori, agenti, collaboratori a qualsiasi titolo, consulenti, fornitori, *partner* commerciali, o comunque, chiunque operi in nome o per conto della Società, di seguito, "Terzi Destinatari") (tutti i soggetti indicati nel paragrafo saranno complessivamente definiti, nel prosieguo, "Destinatari").

I Destinatari sopra indicati sono tenuti ad osservare e, per quanto di propria competenza, a fare osservare i principi contenuti nel Codice Etico, vincolante per tutti loro.

Il complesso delle regole contenute nel Codice Etico, peraltro, uniformando comportamenti aziendali a *standard* etici particolarmente elevati ed improntati alla massima correttezza e trasparenza, garantisce la possibilità di salvaguardare gli interessi degli *stakeholders*, nonché di preservare l'immagine e la reputazione della Società, assicurando, nel contempo, un approccio etico al mercato, con riguardo alle attività svolte nell'ambito del territorio italiano.

Il corpus del Codice Etico si compone di tre sezioni:

- I. nella prima, sono indicati i principi etici generali che individuano i valori di riferimento nelle attività della Società;
- II. nella seconda, sono indicate le norme comportamentali dettate nei riguardi dei soggetti, ivi inclusi i Terzi Destinatari tenuti al rispetto del presente Codice;
- III. nella terza, sono disciplinati i meccanismi di comunicazione, formazione e monitoraggio del Codice Etico.

Di seguito si riporta una sintesi di principi, norme di comportamento, obblighi di comunicazione, modalità di attuazione e controllo sul rispetto del Codice Etico, fermo restando che, per la completa disciplina di tali aspetti, si rimanda al Codice Etico nella sua interezza che costituisce parte integrante del Modello.

## **8.3. I principi generali che regolano l'attività della Società**

Nella prima sezione del Codice Etico, sono individuati i principi generali che regolano l'attività di DIFESA SERVIZI.

La Società, difatti, ha avvertito l'esigenza di addivenire ad una esaustiva e chiara formalizzazione dei principi cui riconosce valore etico positivo, primario ed assoluto. Tali principi sono, peraltro, in linea con quelli contemplati nella "carta dei valori d'impresa", elaborata dall'Istituto Europeo per il bilancio sociale e rappresentano i valori fondamentali cui i soggetti tenuti al rispetto del Codice Etico devono attenersi nel perseguimento della *mission* aziendale e, in genere, nella conduzione delle attività sociali.

In particolare, i principi etici fondamentali adottati da DIFESA SERVIZI riguardano i seguenti valori:

- Rispetto delle leggi e dei regolamenti;
- Correttezza;
- Imparzialità;
- Onestà;
- Integrità;
- Trasparenza;
- Efficienza;
- Concorrenza leale;

- Tutela degli interessi pubblici;
  - Tutela della *privacy*;
  - Spirito di servizio;
  - Valore delle risorse umane;
  - Tutela della personalità individuale,
- e le aree di attività di seguito elencate:
- Rapporti con la collettività e tutela ambientale;
  - Rapporti con istituzioni pubbliche;
  - Rapporti con associazioni, organizzazioni sindacali e partiti politici;
  - Rapporti con operatori internazionali;
  - Sicurezza e salute.

#### **8.4. Principi e norme di comportamento**

DIFESA SERVIZI ha riservato un'apposita sezione del Codice Etico alle norme ed ai principi di comportamento che devono essere rispettati nell'ambito dell'attività d'impresa, indicando, per ciascuna categoria dei soggetti Destinatari del Modello, le norme ed i principi di comportamento da seguire.

##### **8.4.1. Principi e norme di comportamento per i componenti degli organi sociali**

I componenti degli Organi Sociali, in ragione del loro fondamentale ruolo, sono tenuti a rispettare le previsioni del Codice Etico.

In particolare, nello svolgimento della loro attività, essi devono tenere un comportamento ispirato ad autonomia, indipendenza e correttezza nei rapporti con qualsivoglia interlocutore, sia pubblico sia privato.

Ugualmente, devono tenere un comportamento responsabile e leale nei confronti della Società e astenersi dal compiere atti in presenza di un conflitto di interesse. Devono, inoltre, fare un uso riservato delle informazioni di cui vengono a conoscenza in ragione del loro incarico.

##### **8.4.2. Principi e norme di comportamento per il Personale**

Il Personale deve uniformare la propria condotta, sia nei rapporti interni sia nei confronti degli interlocutori esterni alla Società, alla normativa vigente, ai principi espressi dal Codice Etico ed alle norme di comportamento appositamente indicate, nel rispetto del Modello e delle procedure aziendali vigenti.

In particolare, il Personale è tenuto ad osservare tutte le prescrizioni dettate dal "Codice di comportamento dei dipendenti del Ministero della Difesa", approvato dal Ministro in data 23 marzo 2018.

In via generale, il Personale di DIFESA SERVIZI deve evitare di porre in essere, di dar causa o di collaborare alla realizzazione di comportamenti idonei, anche in via potenziale, ad integrare alcuna delle fattispecie di reato richiamate nel Decreto, e deve collaborare con l'Organismo di Vigilanza nel corso delle attività di verifica e vigilanza da questi espletate, fornendo le informazioni, i dati e le notizie da esso richieste.

Nella sezione relativa al Personale, inoltre, sono illustrate le norme ed i principi comportamentali dettati con precipuo riguardo a particolari questioni ed a specifici settori della vita aziendale i cui tratti salienti sono di seguito esposti.

#### **Conflitto di interessi**

Il Personale deve evitare di porre in essere o agevolare operazioni in conflitto d'interesse anche solo apparente o potenziale - con la Società, nonché attività che possano tendere a interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto delle norme del Codice Etico.

Qualora si trovi in una situazione di conflitto di interessi, anche solo potenziale, il Personale deve astenersi dal compiere qualsiasi operazione/attività e comunicare tale circostanza sia al proprio superiore gerarchico che al Responsabile per la prevenzione della corruzione e trasparenza.

#### Rapporti con la Pubblica Amministrazione

Il Personale di DIFESA SERVIZI che intrattiene, nell'esercizio delle sue funzioni, rapporti con interlocutori istituzionali, deve adottare comportamenti rispettosi sia delle disposizioni legislative vigenti che del Codice Etico, in modo da non compromettere l'integrità e l'immagine della Società.

In qualsiasi trattativa o rapporto con la Pubblica Amministrazione è fatto esplicito divieto a tutti i collaboratori interni ed esterni di influenzare impropriamente le decisioni della controparte, ad esempio mediante offerte, promesse, dazioni di denaro o altra utilità, con la finalità di promuovere o favorire l'interesse della Società, anche a seguito di illecite pressioni.

Allo stesso modo, anche gli esponenti della Società non possono accettare denaro, beni, omaggi o, comunque, utilità da rappresentanti della Pubblica Amministrazione.

#### Redazione della documentazione di gara e commissioni di gara

DIFESA SERVIZI effettua la redazione della documentazione di gara in conformità a quanto previsto dalla normativa vigente in materia, nonché nel pieno rispetto delle disposizioni e dei principi stabiliti nel Codice Etico, nonché delle indicazioni fornite dall'ANAC.

La Società si impegna ad agire nel rispetto dei principi di correttezza, trasparenza e buona fede evitando di porre in essere, in qualsiasi modo, forme di favoritismo.

DIFESA SERVIZI, inoltre, favorisce la massima partecipazione possibile alle procedure di selezione e scelta del contraente.

Tutti coloro che partecipano alle Commissioni di gara devono operare con imparzialità e assumere decisioni con rigore, riservatezza, nel rispetto della normativa vigente e dei principi stabiliti nel presente Codice. I componenti delle Commissioni sono inoltre tenuti a non avere contatti informali con soggetti interessati ad ottenere informazioni sulle procedure di gara in essere.

#### Rapporti con i fornitori

I dipendenti di DIFESA SERVIZI devono improntare il rapporto con i fornitori alla massima trasparenza e correttezza.

In particolare, non devono intraprendere alcuna iniziativa che possa comportare favoritismi.

Il fornitore viene selezionato anche in considerazione della capacità di garantire:

- il rispetto del Codice Etico;
- l'attuazione di sistemi di qualità aziendali adeguati, ove previsto;
- la disponibilità di mezzi e strutture organizzative idonei;
- il rispetto della normativa in materia di lavoro, ivi incluso per ciò che attiene il lavoro minorile, la salute e la sicurezza dei lavoratori.

Per quanto riguarda il pagamento delle prestazioni, la Società rispetta i termini contrattuali e si impegna a non effettuare nessun tipo di favoritismo tra i fornitori. Nel caso in cui non possa essere rispettato il termine legale o convenzionale di adempimento, saranno evase prioritariamente le fatture i cui termini di pagamento risultano scaduti da più tempo ed eventuali deroghe a tale principio dovranno essere espressamente autorizzate e motivate.

#### Rapporti con terzi

DIFESA SERVIZI, anche in ragione della rilevanza pubblicistica della propria attività, presta grande attenzione al rapporto con i terzi contraenti ed, in particolare, con i conduttori degli immobili.

Il Personale, nello svolgimento dell'attività nell'interesse della Società, deve comportarsi in modo trasparente e, quindi, rappresentare una informazione chiara e veritiera, basandosi su valutazioni obiettive al fine di consentire all'interlocutore una scelta consapevole.

I potenziali terzi contraenti, interessati ad *asset* nella disponibilità di DIFESA SERVIZI, sono trattati con il medesimo metro di valutazione, non essendo ammessi favoritismi di nessun genere.

Al Personale è fatto assoluto divieto di ricevere denaro, omaggi, doni o regali da parte dei potenziali terzi contraenti sia qualora si tratti di soggetti privati (Società, Fondazioni, ecc.) sia nel caso si tratti di soggetti pubblici (esponenti di Comuni, Regioni, Società aventi rilevanza pubblicistica).

#### Responsabilità in materia di controlli interni

Ogni persona che fa parte dell'organizzazione di DIFESA SERVIZI è parte integrante del suo sistema di controllo interno ed ha il dovere di contribuire, nell'ambito delle funzioni ed attività svolte, al suo corretto funzionamento.

Inoltre, tutti i dipendenti di DIFESA SERVIZI sono tenuti a segnalare al proprio responsabile le eventuali carenze riscontrate nel sistema dei controlli o eventuali comportamenti negligenti o tenuti in mala fede dei quali fossero venuti a conoscenza.

#### Riservatezza

Il Personale deve trattare con assoluta riservatezza, anche successivamente alla cessazione del rapporto di lavoro, dati, notizie ed informazioni di cui viene in possesso, evitandone la diffusione o l'uso a fini speculativi propri o di terzi. Le informazioni aventi carattere riservato possono essere rese note, nell'ambito della Società, solo nei riguardi di coloro che abbiano effettiva necessità di conoscerle per motivi di lavoro.

#### Diligenza nell'utilizzo dei beni della Società

Il Personale deve proteggere e custodire i valori ed i beni di DIFESA SERVIZI ad esso affidati, e contribuire alla tutela del patrimonio della Società in generale, evitando situazioni che possano incidere negativamente sull'integrità e sicurezza di tale patrimonio.

#### Utilizzo dei sistemi informatici

L'utilizzo dei sistemi informatici, delle banche dati della Società e di internet, deve avvenire nel rispetto delle procedure interne, della normativa vigente e sulla base dei principi di correttezza e onestà.

#### Utilizzo dei social media

I Destinatari devono sempre tenere in considerazione che quanto effettuato attraverso i social network, anche per conto personale, può avere ripercussioni negative sulla Società, anche indirettamente, provocando un danno economico o reputazionale.

Pertanto, nell'utilizzo dei social media è necessario che tutti i Destinatari usino moderazione e buon senso.

### **8.4.3. Principi e norme di comportamento per i Terzi Destinatari**

Oltre che ai componenti degli Organi sociali ed al Personale, il Codice Etico si applica anche ai Terzi Destinatari.

I Terzi Destinatari sono, pertanto, obbligati al rispetto delle disposizioni ivi contenute ed, in particolare, nei limiti delle rispettive competenze e responsabilità, dei principi etici di riferimento e delle norme di comportamento dettate per il Personale di DIFESA SERVIZI.

In assenza dell'impegno espresso a rispettare le norme del Codice Etico, DIFESA SERVIZI non concluderà e/o non proseguirà alcun rapporto con il Terzo Destinatario. A tal fine, è previsto l'inserimento, nelle lettere di incarico e/o negli accordi negoziali, di apposite clausole volte a confermare l'obbligo del Terzo Destinatario di conformarsi pienamente al Codice, nonché a prevedere, in caso di violazione, una diffida al puntuale rispetto dello stesso ovvero l'applicazione di penali o, ancora, la risoluzione del rapporto contrattuale.

### **8.5. Obblighi di comunicazione all'Organismo di Vigilanza**

I Destinatari del Codice Etico devono adempiere a precisi obblighi di informazione nei confronti dell'O.d.V., con particolare riferimento alle possibili violazioni di norme di legge o regolamenti, del Modello, del Codice Etico, delle procedure interne.

In ogni caso, l'O.d.V. assicura che la persona che effettua la comunicazione, qualora identificata o identificabile, non sia oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, assicurandone, quindi, la riservatezza (salvo la ricorrenza di eventuali obblighi di legge che impongano diversamente).

### **8.6. Le modalità di attuazione ed il controllo sul rispetto del Codice Etico**

Il controllo circa l'attuazione ed il rispetto del Modello e, in particolare, del Codice Etico è affidato all'O.d.V., il quale è tenuto, tra l'altro, anche a:

- controllare il rispetto del Modello e del Codice Etico, nell'ottica di ridurre il pericolo della commissione dei reati previsti dal Decreto;
- formulare le proprie osservazioni in merito sia alle problematiche di natura etica che dovessero insorgere nell'ambito delle decisioni aziendali, sia alle presunte violazioni del Codice Etico di cui venga a conoscenza;
- fornire ai soggetti interessati tutti i chiarimenti e le delucidazioni richieste, ivi incluse quelle relative alla legittimità di comportamenti o condotte concrete, ovvero alla corretta interpretazione delle previsioni del Modello o del Codice Etico;
- seguire e coordinare l'aggiornamento del Codice Etico, anche attraverso proprie proposte di adeguamento;
- predisporre ed approvare il piano di comunicazione e formazione etica;
- segnalare agli organi aziendali competenti le eventuali violazioni del Modello e, in particolare, del Codice Etico, suggerendo la sanzione da irrogare nei confronti del soggetto individuato quale responsabile e verificando l'effettiva applicazione delle misure eventualmente irrogate.

## **9. IL SISTEMA DISCIPLINARE DI DIFESA SERVIZI**

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati *ex* D. Lgs. 231/2001 costituisce un elemento essenziale del sistema di controllo preventivo. Tali principi sono inseriti nel Codice etico.

### **9.1. L'elaborazione e l'adozione del Sistema Disciplinare**

Ai sensi degli artt. 6 e 7 del Decreto, il Modello può ritenersi efficacemente attuato, ai fini dell'esclusione di responsabilità della Società, se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate. Simili violazioni ledono infatti il rapporto di fiducia instaurato con l'Ente e devono di conseguenza comportare azioni disciplinari, a prescindere dall'eventuale instaurazione di un giudizio penale nei casi in cui il comportamento costituisca reato. La valutazione disciplinare dei comportamenti effettuata dai datori di lavoro, salvo, naturalmente, il successivo eventuale controllo del giudice del lavoro, non deve, infatti, necessariamente coincidere con la valutazione del giudice in sede penale, data l'autonomia della violazione del codice etico e delle procedure interne rispetto alla violazione di legge che comporta la commissione di un reato. Il datore di lavoro non è tenuto quindi, prima di agire, ad attendere il termine del procedimento penale eventualmente in corso. I principi di tempestività ed immediatezza della sanzione rendono infatti non soltanto non doveroso, ma altresì sconsigliabile ritardare l'irrogazione della sanzione disciplinare in attesa dell'esito del giudizio eventualmente instaurato davanti al giudice penale.

Quanto alla tipologia di sanzioni irrogabili, in via preliminare va precisato che, nel caso di rapporto di lavoro subordinato, qualsiasi provvedimento sanzionatorio deve rispettare le procedure previste dall'art. 7 dello Statuto dei Lavoratori.

Nel caso specifico di DIFESA SERVIZI essendo tutto il personale dipendente tratto dall'Amministrazione della Difesa si applicheranno:

- per i militari, i provvedimenti sanzionatori previsti dal Codice dell'Ordinamento Militare;
- per il personale civile, le disposizioni previste dal D. Lgs. 30 marzo 2001, n. 165 e dal D.P.R. n. 62/2013, modificato dal D.P.R. 81/2023.

DIFESA SERVIZI ha quindi stabilito, sulla scorta del Contratto di Servizio, sottoscritto il 27 agosto 2021 e della convezione sulla gestione del personale, sottoscritta con lo SMD e SGD/DNA il 18 maggio 2022 e attualmente in corso di perfezionamento, di deferire il personale militare e civile ai rispettivi Enti cui sono assegnati per la valutazione degli aspetti disciplinari. In particolare, il procedimento disciplinare di stato verrà svolto dagli organi competenti in caso di violazione dei principi, delle norme e delle misure previste nel Modello e dei relativi Protocolli.

Sono passibili di sanzione anche le violazioni del Modello e dei relativi Protocolli commesse dai soggetti posti in posizione “apicale” - in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione dell’Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero titolari del potere, anche solo di fatto, di gestione o di controllo dell’Ente - sia le violazioni perpetrate dai soggetti sottoposti all’altrui direzione o vigilanza o operanti in nome e/o per conto di DIFESA SERVIZI. Sono previste delle specifiche sanzioni, inoltre, per il Terzi Destinatari.

Qualora la violazione delle norme etiche fosse invece posta in essere da un lavoratore autonomo, fornitore o altro soggetto avente rapporti contrattuali con DIFESA SERVIZI, dovrà prevedersi, quale sanzione, la risoluzione del contratto.

## **9.2. Le condotte rilevanti per il Sistema Disciplinare**

Con riguardo agli amministratori ed ai sindaci, agli altri soggetti in posizione “apicale” ed ai dipendenti della Società, costituiscono condotte sanzionabili:

- 1) il mancato rispetto del Modello, qualora si tratti di violazioni connesse, in qualsiasi modo, alle aree indicate quali “strumentali” o “di supporto” nel Documento di Sintesi del Modello (Parte Speciale) e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4;
- 2) il mancato rispetto del Modello, qualora si tratti di violazioni connesse, in qualsiasi modo, alle aree “a rischio reato” o alle attività “sensibili” indicate nel Documento di Sintesi del Modello (Parte Speciale) e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4;
- 3) il mancato rispetto del Modello, qualora si tratti di violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;
- 4) il mancato rispetto del Modello, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto o, comunque, sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto.

Per ciò che concerne i Terzi Destinatari, costituiscono condotte sanzionabili:

- il mancato rispetto del Codice Etico, qualora la violazione non integri alcuna delle fattispecie di cui alle successive lett. b) e c);
- il mancato rispetto del Codice Etico, qualora si tratti di violazione idonea ad integrare il solo fatto (elemento oggettivo) di uno dei reati previsti nel Decreto;
- il mancato rispetto del Codice Etico, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto o, comunque, sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto.

Con riguardo al Whistleblowing, sono oggetto di sanzione le violazioni delle misure di tutela del dipendente che segnala illeciti del presente Modello nonché le segnalazioni effettuate con dolo o colpa grave che si rivelano infondate. Nello specifico, sono previste sanzioni:

- per coloro che hanno commesso ritorsioni, hanno ostacolato la segnalazione o hanno tentato di ostacolarla ovvero hanno violato l'obbligo di riservatezza di cui all'art. 12 del D.Lgs. 24/2023;
- qualora non siano stati istituiti canali di segnalazione, non siano state adottate procedure per l'effettuazione e la gestione delle segnalazioni (o tali procedure non sono conformi a quanto indicato dagli articoli 4 e 5 del D.Lgs. 24/2023), quando non è stata svolta attività di verifica e analisi della segnalazione ricevuta.

## **11. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI CONNESSI. L'AGGIORNAMENTO DEL MODELLO**

### **10.1. L'informazione sul Modello e sui Protocolli connessi**

La Società promuove la più ampia divulgazione, all'interno e all'esterno della struttura, dei principi e delle previsioni contenuti nel Modello e nei Protocolli ad esso connessi.

Il Modello è comunicato formalmente ad ogni componente degli organi sociali.

Il Modello è, altresì, comunicato formalmente a tutti i soggetti apicali, ai dipendenti della Società nonché ai soggetti che per essa agiscono, mediante consegna di copia integrale, anche su supporto informatico, nonché conservazione in luogo accessibile a tutti.

Della eseguita consegna e del contestuale impegno da parte dei Destinatari al rispetto delle regole ivi previste viene conservata traccia documentale agli atti dell'O.d.V..

Per i Terzi Destinatari, una sintesi dello stesso è resa disponibile sul sito *internet* della Società.

Specifica attenzione è, poi, riservata alla diffusione del Codice Etico, che, oltre ad essere comunicato con le modalità già indicate in generale per il Modello (consegna a tutti, ossia componenti degli organi sociali, altri soggetti apicali e dipendenti, affissione in un luogo aziendale accessibile a tutti verrà messo a disposizione dei soggetti terzi tenuti al rispetto delle relative previsioni, nonché di qualunque altro interlocutore della Società, mediante pubblicazione integrale sul sito *internet* aziendale. In particolare, al fine di formalizzare l'impegno al rispetto dei principi del Codice Etico da parte di terzi aventi rapporti contrattuali con la Società in relazione all'attività loro richiesta, è previsto l'inserimento nel contratto di riferimento di una apposita clausola come in precedenza specificato.

L'O.d.V. pianifica e monitora tutte le ulteriori attività di informazione che dovesse ritenere necessarie o opportune.

### **10.2. La formazione sul Modello e sui Protocolli connessi**

In aggiunta alle attività connesse alla Informazione dei Destinatari, l'O.d.V. ha il compito di promuovere e monitorare la periodica e costante Formazione, ovvero di promuovere e monitorare le iniziative volte a favorire una conoscenza ed una consapevolezza adeguate del Modello e dei Protocolli ad esso connessi, al fine di incrementare la cultura di eticità all'interno della Società.

In particolare, è previsto che i principi del Modello e, in particolare, quelli del Codice Etico, siano illustrati alle risorse aziendali attraverso apposite attività formative (ad es., corsi, seminari, questionari, ecc.), a cui è posto obbligo di partecipazione e le cui modalità di esecuzione da parte delle risorse ritenute maggiormente adeguate sono pianificate dall'O.d.V. mediante approvazione di specifici Piani.

I corsi e le altre iniziative di formazione sui principi del Modello sono, peraltro, differenziati in base al ruolo ed alla responsabilità delle risorse interessate, ovvero mediante la previsione di una formazione più intensa e caratterizzata da un più elevato grado di approfondimento per i soggetti qualificabili come "apicali" alla stregua del Decreto, nonché per quelli operanti nelle aree qualificabili come "a rischio" ai sensi del Modello.

### **10.3. Comunicazione degli aggiornamenti del Modello e del Codice Etico**

L'O.d.V. ha il compito di promuovere il necessario aggiornamento e adeguamento continuo del Modello e dei Protocolli ad esso connessi (ivi incluso il Codice Etico), suggerendo all'organo amministrativo le correzioni e gli adeguamenti necessari o opportuni.

Il Consiglio di Amministrazione è responsabile, unitamente alle funzioni aziendali eventualmente interessate, dell'aggiornamento del Modello e del suo adeguamento in conseguenza di un mutamento degli assetti organizzativi o dei processi operativi, di significative violazioni del Modello stesso, di integrazioni legislative. Gli aggiornamenti ed adeguamenti del Modello, o dei Protocolli ad esso connessi, sono divulgati mediante comunicazioni inviate a mezzo e-mail e, se del caso, attraverso la predisposizione di sessioni informative illustrative degli aggiornamenti e adeguamenti più rilevanti.

**SEZIONE II – PARTE SPECIALE  
MODELLO DI ORGANIZZAZIONE E  
GESTIONE EX D. LGS. N. 231/2001**

## 1. MAPPATURA E VALUTAZIONE DEI RISCHI

L'art 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno dei requisiti del Modello di organizzazione, gestione e controllo, "l'individuazione delle attività nel cui ambito possono essere commessi reati". In riferimento a ciò si è proceduto ad aggiornare l'individuazione delle cd. "aree sensibili" o "a rischio", cioè di quei processi e di quelle attività in cui potrebbe determinarsi il rischio di commissione dei reati richiamati dal D. Lgs. 231/01 e parallelamente si sono identificate le condotte e le attività che potrebbero portare alla realizzazione di fattispecie delittuose ("processi strumentali"). L'obiettivo è quello di valutare ipotesi di reati che possano presentare, per loro natura, un rischio "significativo". È stato utilizzato un criterio di valutazione del rischio di tipo "qualitativo" che considera cinque fasce di misurazione (basso, medio, alto, molto, elevatissimo) e che prevede anche l'individuazione dei rischi di reato "non verosimili" o "non applicabili".

Sono stati valutati "non verosimili" o "non applicabili":

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25 bis)
- Delitti contro l'industria e il commercio (Art. 25 bis.1);
- Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25 quater);
- Pratiche di mutilazione degli organi genitali femminili (Art. 25 quater.1);
- Delitti contro la personalità individuale (Art. 25 quinquies);
- Reati di abuso di mercato (Art. 25 sexies);;
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25 duodecies);
- Razzismo e Xenofobia (Art. 25 terdecies);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25 quaterdecies);
- Contrabbando (Art. 25 sexiesdecies);
- Reati transnazionali (L.146/2006);

Le seguenti macro-categorie di reati, invece, sono state valutate applicabili e verosimili:

- Indebita percezione di erogazioni, truffa in danno dello Stato, ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24);
- Delitti informatici e trattamento illecito di dati (Art. 24 bis);
- Delitti di criminalità organizzata (Art. 24 ter);
- Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25);
- Reati societari (Art. 25 ter);
- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies);
- Ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25 octies);
- Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25 octies.1);
- Delitti in materia di violazione del diritto d'autore (Art. 25 novies);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25 decies);
- Reati ambientali (Art. 25 undecies);
- Reati tributari (Art. 25 quinquiesdecies);
- Delitti contro il patrimonio culturale (Art. 25 septiesdecies);

- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25 duodevices).

### **1.1. Le nozioni di Pubblica Amministrazione, Pubblico Ufficiale ed Incaricato di Pubblico Servizio e i reati previsti dal D. Lgs. n. 231/2001 (cd. Reati-presupposto).**

Preliminare all'analisi dei delitti contro la Pubblica Amministrazione, richiamati dagli artt. 24 e 25 del D. Lgs. n. 231/2001 e ss.mm.ii. (di seguito, per brevità, "Decreto"), è la delimitazione delle nozioni di Pubblica Amministrazione (di seguito, per brevità, "PA"), di Pubblico Ufficiale (di seguito, per brevità, "PU") e di Incaricato di Pubblico Servizio (di seguito, per brevità, "IPS").

Per PA si intende, in estrema sintesi, l'insieme di enti e soggetti pubblici (stato, ministeri, regioni, province, comuni, etc.) e talora privati (organismi di diritto pubblico, concessionari, amministrazioni aggiudicatrici, s.p.a. miste, ecc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica nell'interesse della collettività e, quindi, nell'interesse pubblico. Oggetto della tutela penale nei reati che rilevano in questa sede è il regolare funzionamento, nonché il prestigio degli Enti pubblici ed, in generale, quel "buon andamento" dell'Amministrazione di cui all'art. 97 della Costituzione, ovvero, nel caso dei reati di truffa, il patrimonio pubblico.

La nozione di PU è fornita direttamente dal legislatore, all'art. 357 del cod. pen., il quale indica il "pubblico ufficiale" in "chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa", specificando che "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica Amministrazione e dal suo svolgersi per mezzo dei poteri autoritativi e certificativi".

I "pubblici poteri" qui in rilievo sono il potere legislativo, quello giudiziario e, da ultimo, quelli riconducibili alla "pubblica funzione amministrativa".

Diversamente, l'art. 358 riconosce la qualifica di "incaricato di un pubblico servizio" a tutti "coloro i quali, a qualunque titolo, prestano un pubblico servizio", intendendosi per tale "un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

È, pertanto, un IPS colui il quale svolge una 'pubblica attività', non riconducibile ad alcuno dei "poteri" sopra rammentati e non concernente semplici mansioni d'ordine e/o la prestazione di opera meramente materiale ed, in quanto tali, prive di alcun apporto intellettuale e discrezionale.

Esempi di IPS sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati.

L'effettiva ricorrenza dei sopra indicati requisiti deve essere verificata, caso per caso, in ragione della concreta ed effettiva possibilità di ricondurre l'attività di interesse alle richiamate definizioni, essendo certamente ipotizzabile anche che soggetti appartenenti alla medesima categoria, ma addetti ad espletare differenti funzioni o servizi, possano essere diversamente qualificati proprio in ragione della non coincidenza dell'attività da loro in concreto svolta.

#### **1.1.1. Reati contro la Pubblica Amministrazione (Artt. 24 e 25, D. Lgs. n. 231/2001). Possibili modalità di commissione**

Si riporta di seguito una sintetica descrizione dei reati richiamati negli artt. 24 e 25 del Decreto, nonché una breve esposizione delle possibili modalità di attuazione dei reati, fermo restando che, ai sensi dell'art. 26 del Decreto, la Società potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma del tentativo.

#### Malversazione di erogazioni pubbliche (art. 316-bis codice penale)

Il reato si configura qualora, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità, non si destinano le somme alle finalità previste.

La finalità della previsione incriminatrice è da ravvisare nell'esigenza di tutelare la “destinazione” dei finanziamenti pubblici, ovvero “l'interesse a che le somme erogate per pubbliche finalità dallo Stato, dagli enti pubblici ovvero dagli organismi Europei vengano realmente utilizzate per tali scopi”, contrastando la condotta di chi, ottenuto un finanziamento con vincolo di destinazione alla soddisfazione di un determinato interesse pubblico, non lo impieghi per soddisfare la finalità preordinata.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui l'azienda ottenga correttamente contributi/finanziamenti (etc.) da parte di organismi pubblici italiani o comunitari, partecipando a procedure per l'ottenimento della relativa erogazione, ma non li destini o non li utilizzi alle finalità per cui sono stati erogati.

#### Indebita percezione di erogazioni pubbliche (art. 316-ter codice penale)

Il reato si configura qualora mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, si conseguono indebitamente, per sé o per altri, contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee.

In questa fattispecie, diversamente da quanto accade nel reato di malversazione di erogazioni pubbliche (art. 316 bis cod. pen.), non ha alcuna rilevanza l'uso che viene fatto delle erogazioni, perfezionandosi il reato con il solo ottenimento degli indebiti finanziamenti.

Tale ipotesi di reato assume natura residuale rispetto alla più grave fattispecie di truffa in danno dello Stato/Ente pubblico/Unione europea (ex art. 640, II comma, n. 1 cod. pen.), per la cui sussistenza è necessaria l'induzione in errore mediante artifici o raggiri.

A titolo esemplificativo, il reato potrebbe configurarsi con il semplice utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero l'omissione di informazioni dovute da cui derivi il conseguimento indebito di erogazioni da parte dello Stato o di altri enti pubblici o delle Comunità europee, da cui derivi cioè il conseguimento di erogazioni cui non si ha diritto. Tali erogazioni, poi, possono consistere indifferentemente o nell'ottenimento di una somma di danaro oppure nell'esenzione dal pagamento di una somma altrimenti dovuta (mero risparmio).

#### Turbata libertà degli incanti (art. 353 codice penale)

Il reato si configura qualora, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, si impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche Amministrazioni, ovvero ne allontana gli offerenti.

Per pubblici incanti deve intendersi la procedura attuata dalla P.A. per la stipulazione di contratti con i privati e consistente in una gara aperta tra diversi concorrenti per l'assegnazione del contratto a chi fa l'offerta più vantaggiosa, mentre per licitazione privata si intende la procedura attuata dalla P.A. per la stipulazione di contratti con i privati e consistente in una gara aperta ad un numero ristretto di concorrenti, considerati potenzialmente idonei a fornire la prestazione dovuta, per l'assegnazione del contratto a chi fa l'offerta più vantaggiosa. Presupposto del reato è la pubblicazione del bando, non potendovi essere alcuna consumazione, neanche nella forma tentata, prima di tale momento.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui un rappresentante della società, partecipando ad alcune cene con altri imprenditori, metterebbe a punto delle combine per aggiudicarsi le gare, predisponendo e pianificando il numero e le società che dovrebbero concorrere alla gara di appalto; ciò a prescindere dal danno causato e dal raggiungimento dell'obiettivo, in quanto il turbamento si verifica quando la condotta collusiva influisce soltanto nella regolarità della gara anche senza alterarne i risultati.

Turbata libertà del procedimento di scelta del contraente (art. 353-bis codice penale)

Il reato si configura allorquando con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, si turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso di omessa pubblicità del bando di gara sulla Gazzetta Ufficiale e sui quotidiani a diffusione locale, nonché sul sito istituzionale, allo scopo pratico di limitare la conoscenza e/o conoscibilità del relativo bando ai possibili concorrenti.

Frode nelle pubbliche forniture (art. 356 codice penale)

Il reato si configura nei confronti di chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo art. 355 codice penale, nei confronti dello Stato, degli enti pubblici o di imprese, anche se private, esercenti servizi pubblici o di pubblica necessità.

Per contratto di fornitura non si intende uno specifico tipo di contratto, ma, in generale, ogni strumento contrattuale destinato a fornire alla P.A. beni o servizi. Per quanto concerne l'inadempimento, esso si concreta nella consegna di cosa od opera completamente diversa da quella pattuita, o di cosa od opera affetta da vizi o difetti.

Si richiede anche un comportamento non conforme ai doveri di lealtà e moralità commerciale e di buona fede contrattuale: ed in questo consiste l'elemento frode. È pertanto sufficiente la malafede nell'eseguire il contratto in difformità dei patti, senza necessità di un comportamento tendente a trarre in inganno il committente ed a dissimulare le deficienze della fornitura.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso nella fraudolenta esecuzione di un contratto di somministrazione (art. 1559 c.c.) ovvero di un contratto di appalto (art. 1655 c.c.).

Truffa in danno dello Stato o di altro Ente pubblico o della Comunità Europea (art. 640, comma 2, n. 1 codice penale)

Tale reato si configura qualora, con artifici o raggiri ed in tal modo inducendo taluno in errore, si consegua un ingiusto profitto in danno dello Stato o di altro ente pubblico o l'Unione europea.

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

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

Il "profitto" si ravvisa anche nella mancata diminuzione del patrimonio, per effetto, ad es., del godimento di un bene e, quindi, anche in assenza di un aumento effettivo di ricchezza; può anche non essere di natura patrimoniale, potendo consistere nel soddisfacimento di un interesse di natura morale. A titolo meramente esemplificativo, il reato potrebbe configurarsi nel caso in cui venga evaso il versamento dei contributi previdenziali mediante artifici e raggiri quali, ad es., l'alterazione o contraffazione delle dichiarazioni contributive.

Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis cod. pen.)

Il reato si configura qualora la condotta di truffa sopra descritta sia posta in essere per conseguire indebitamente erogazioni pubbliche.

L'elemento qualificante rispetto al precedente reato è costituito dall'oggetto materiale della frode, in quanto per "erogazione pubblica" si intende ogni attribuzione economica agevolata, erogata da parte dello Stato, di enti pubblici o delle Comunità europee.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si consegua un finanziamento o un contributo pubblico mediante il compimento di artifici e raggiri, come specificati nel punto precedente.

Frode informatica in danno dello Stato o di altro Ente pubblico (art. 640-ter codice penale)

Il reato si configura nel caso in cui, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, si ottenga un ingiusto profitto in danno dello Stato o di altro ente pubblico o dell'Unione europea.

L'alterazione fraudolenta del sistema può essere la conseguenza di un intervento rivolto sia alla componente meccanica dell'elaboratore, sia al *software*.

Sono considerate pertinenti ad un sistema informatico e, quindi, rilevanti ai sensi della norma in questione, le informazioni contenute su supporti materiali, nonché i dati ed i programmi contenuti su supporti esterni all'elaboratore (come dischi e nastri magnetici o ottici), che siano destinati ad essere utilizzati in un sistema informatico.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si alteri il funzionamento di un sistema informatico o telematico o dei dati in esso contenuti al fine di conseguire di modificare la raccolta e la trasmissione di dati relativi alle informazioni richieste dalle Autorità (ad es., Garante della Privacy, Enti previdenziali, ecc.).

Corruzione

a) Corruzione per l'esercizio della funzione (art. 318 codice penale)

Il reato si configura nei confronti del pubblico ufficiale o dell'incaricato di pubblico servizio che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

Ai fini della ricorrenza di tale reato è necessario che la promessa di denaro o di altra utilità siano accettate dal PU o dall'IPS, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 cod. pen. (su cui vedi infra).

Il delitto di corruzione si differenzia da quello di concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio.

b) Corruzione per un atto contrario ai doveri d'ufficio (art. 319 codice penale)

Il reato si configura allorquando un pubblico ufficiale o un incaricato di pubblico servizio, per omettere o ritardare o per aver omesso o ritardato un atto di ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, ricevano, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

È necessario che la promessa di denaro o di altra utilità siano accettate dal PU, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 codice penale.

c) Circostanze aggravanti (art. 319-bis codice penale)

Il reato si configura quando la condotta di corruzione, prevista dall'articolo 319 del codice penale, è posta in essere per il conferimento di pubblici impieghi, licenze, autorizzazioni, concessioni, appalti, o per il pagamento di tributi, sovrime, tasse o per il rilascio di dichiarazioni in materia fiscale, aggravando la gravità del fatto in ragione della natura del vantaggio ottenuto o del danno arrecato all'interesse pubblico.

d) Corruzione in atti giudiziari (art. 319-ter, comma 1, codice penale)

Il reato si configura nel caso in cui i fatti di corruzione di cui agli artt. 318 e 319 siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.

È opportuno evidenziare che nella nozione di PU sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

Il reato è una forma speciale di corruzione e non è necessario che ne derivi effettivamente un danno ad una parte per la consumazione del reato. Infatti il danno (l'ingiusta condanna) è prevista come circostanza aggravante. In ogni caso è necessario che il danno o il favore che consegue alla parte siano ingiusti.

e) Corruzione di persona incaricata di un pubblico servizio (art. 320 cod. pen.)

Le disposizioni previste per il reato di corruzione degli articoli 318 e 319 si applicano non solo al pubblico ufficiale bensì anche all'incaricato di pubblico servizio.

f) Pene per il corruttore (art. 321 cod. pen.)

Il reato si configura quando il soggetto privato, direttamente o indirettamente, offre o promette denaro o altra utilità a un pubblico ufficiale o a un incaricato di pubblico servizio, inducendolo a compiere un atto contrario ai doveri d'ufficio, un atto del suo ufficio o a omettere o ritardare un atto dovuto, rendendosi corresponsabile della corruzione ai sensi delle disposizioni previste dagli articoli 318, 319 e 319-bis del codice penale.

I reati di corruzione indicati sub punti a), b) c) d), e) f), potrebbero essere realizzati mediante l'erogazione di denaro o la promessa di erogazione di denaro al pubblico ufficiale/incaricato di pubblico servizio, la cui provvista derivi da:

- creazione di fondi occulti tramite l'emissione di fatture relative ad operazioni inesistenti;
- rimborsi spese fittizi o per ammontare diverso da quello delle spese effettivamente sostenute anche attraverso consulenti;
- utilizzo delle deleghe di spesa attribuite.

Sotto un diverso profilo, i reati di cui ai punti a), b), c) e d) e) f) potrebbero essere realizzati mediante l'erogazione o la promessa di erogazione al pubblico ufficiale/incaricato di pubblico servizio di una qualsiasi altra utilità o retribuzione, quali in via esemplificativa:

- omaggi e, in genere, regalie;
- dazione/conferimento di beni a condizioni più favorevoli rispetto a quelle di mercato;
- assunzione di personale indicato dal pubblico ufficiale o incaricato di pubblico servizio;
- raggiungimento di accordi/sottoscrizione di lettere di incarico in favore di persone segnalate dal pubblico ufficiale o dall'incaricato di pubblico servizio a condizioni ingiustamente vantaggiose;
- cancellazione immotivata (totale o parziale) di un debito residuo dell'Ente presso cui il pubblico ufficiale/incaricato di pubblico servizio presta il suo servizio o di cui è rappresentante nei confronti della società, ecc.

In particolare, nel caso sub punto d), il fine del reato potrebbe essere quello di ottenere una pronuncia favorevole alla Società nell'ambito di un contenzioso.

Infine, per completezza, deve ricordarsi che, essendo i delitti di corruzione fattispecie a c.d. concorso necessario, ai sensi dell'art. 321 cod. pen., le pene stabilite agli artt. 318, 319, 319 bis, 319 ter e 320 cod. pen. si applicano anche al corruttore e non solo al corrotto.

Concussione (art. 317 cod. pen.)

Il reato si configura allorché un pubblico ufficiale o un incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Con precipuo riguardo a DIFESA SERVIZI, il reato potrebbe essere integrato in tutti i casi in cui un soggetto che agisca nell'interesse della Società rivesta la qualifica di PU e richieda a soggetti terzi,

approfittando della propria qualifica o dei propri poteri, prestazioni non dovute (anche) nell'interesse o a vantaggio della Società.

Induzione indebita a dare o promettere utilità (art. 319-quater cod. pen.)

Il reato si configura nel caso in cui, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Tale fattispecie può configurarsi anche qualora il PU o IPS induca a promettere altre utilità nell'interesse o a vantaggio della Società attraverso conclusione di accordi commerciali.

Istigazione alla corruzione (art. 322 cod. pen.)

Il reato si configura nel caso in cui, nei confronti di un PU o di un IPS, sia formulata l'offerta o la promessa di una somma di denaro o di un'altra utilità non dovuta, qualora l'offerta o la promessa non siano accettate e riguardino, in via alternativa:

- l'esercizio delle sue funzioni o dei suoi poteri
- l'omissione o il ritardo di un suo atto d'ufficio;
- il compimento di un atto contrario ai suoi doveri d'ufficio.

È, inoltre, penalmente sanzionata anche la condotta del PU (o IPS) che sollecita una promessa o dazione di denaro o altra utilità da parte di un privato per le medesime finalità.

È necessario, inoltre, che la promessa di denaro o di altra utilità non siano accettate dal PU, poiché, in caso contrario, deve ritenersi integrata una delle fattispecie di corruzione.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione, fermo restando che, ai fini della configurabilità della fattispecie in esame, è necessario che l'offerta o la promessa non siano accettate.

Traffico di influenze illecite (art. 346-bis codice penale)

Il reato si configura nei confronti di chiunque, sfruttando relazioni esistenti con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, (c.d. mediazione illecita) ovvero per remunerarlo in relazione all'esercizio delle sue funzioni o dei suoi poteri (c.d. remunerazione illecita).

Ai fini di cui al primo comma, per altra mediazione illecita si intende la mediazione per indurre il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito.

La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità economica. Le due condotte hanno una fisionomia che è in parte sovrapponibile: l'elemento oggettivo che vale a distinguerle è costituito dal denaro o dall'utilità data o anche solo promessa. Nella prima, il denaro o l'utilità ha quale destinatario finale il trafficante, che la acquisisce quale corrispettivo delle energie da spendere per mediare, nell'interesse del committente, presso il decisore pubblico. Nella seconda, il denaro o l'utilità ha un destinatario intermedio, il trafficante, ed uno finale, il decisore pubblico, e costituisce il corrispettivo destinato a quest'ultimo per l'esercizio delle sue funzioni o dei suoi poteri funzionalmente mirato al soddisfacimento dell'interesse del committente.

La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio. Le pene sono altresì aumentate se i fatti sono commessi in relazione all'esercizio di attività giudiziarie o per remunerare il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio.

Peculato (art. 314, comma 1, codice penale)

Il reato si configura nei confronti del pubblico ufficiale o dell'incaricato di un pubblico servizio che, avendo per ragione del proprio ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria. Ai fini del D.Lgs. n. 231/2001, tale fattispecie è rilevante quando il fatto offende gli interessi finanziari dell'Unione europea.

Indebita destinazione di denaro o cose mobili (art. art. 314-bis, codice penale)

Il reato si configura quando il pubblico ufficiale o l'incaricato di pubblico servizio, nello svolgimento delle sue funzioni o del suo servizio, destina indebitamente a proprio vantaggio o a vantaggio di terzi somme di denaro o cose mobili di cui abbia la disponibilità in ragione del suo ufficio o servizio, discostandosi dalla finalità istituzionale o dall'uso previsto dalla legge o dai regolamenti, in violazione dei doveri d'imparzialità e correttezza che regolano l'esercizio della funzione pubblica.

Peculato mediante profitto dell'errore altrui (art. 316 codice penale)

Il reato si configura nei confronti del pubblico ufficiale o dell'incaricato di un pubblico servizio che, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità. Ai fini del D.Lgs. n. 231/2001, tale fattispecie è rilevante quando il fatto offende gli interessi finanziari dell'Unione europea.

Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis cod. pen.)

Il reato si configura allorché la medesima condotta prevista per i reati di cui agli articoli 314, 316, da 317 a 320, 322, terzo e quarto comma, venga compiuta da, o nei confronti, di membri degli organi delle Comunità europee o di Stati esteri.

Tali soggetti sono assimilati ai pubblici ufficiali qualora esercitino funzioni corrispondenti, e agli incaricati di pubblico servizio negli altri casi.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione e concussione, fermo restando che, ai fini della configurabilità della fattispecie di istigazione, è necessario che l'offerta o la promessa non siano accettate.

**1.1.2. Delitti informatici e trattamento illecito di dati (Art. 24 bis, D. Lgs. n. 231/2001)**

Falsità in documento informatico pubblico o avente efficacia probatoria (Art. 491-bis codice penale)

Il reato si configura quando un soggetto forma, altera o utilizza un documento informatico pubblico o avente efficacia probatoria, attribuendogli un contenuto falso o modificandone quello autentico, in modo da compromettere la veridicità e l'affidabilità del documento stesso, con rilevanza ai fini giuridici o probatori.

Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter codice penale)

Il reato si configura quando un soggetto accede intenzionalmente a un sistema informatico o telematico protetto da misure di sicurezza, oppure vi si mantiene senza averne diritto, violando le disposizioni normative poste a tutela della riservatezza e dell'integrità dei sistemi e delle informazioni in essi contenute.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (Art. 615-quater codice penale)

Il reato si configura quando un soggetto, senza averne diritto, procura, produce, detiene, diffonde, cede o installa apparecchiature, dispositivi, programmi informatici, codici o altri strumenti specificamente idonei a consentire l'accesso abusivo a un sistema informatico o telematico protetto, violando le disposizioni poste a tutela della sicurezza dei sistemi e delle informazioni.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater codice penale)

Il reato si configura quando un soggetto, fraudolentemente e senza averne diritto, intercetta, impedisce o interrompe comunicazioni informatiche o telematiche tra più soggetti, violando la riservatezza e l'integrità delle comunicazioni protette, con l'intento di trarne vantaggio o arrecare danno.

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies codice penale)

Il reato si configura quando un soggetto, senza autorizzazione, detiene, diffonde, installa o cede apparecchiature, dispositivi o altri mezzi idonei a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, in violazione delle normative che tutelano la riservatezza e l'integrità delle comunicazioni.

Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis codice penale)

Il reato si configura quando un soggetto, senza diritto, danneggia, distrugge, altera o rende inaccessibili informazioni, dati o programmi informatici, compromettendo il corretto funzionamento di sistemi informatici o telematici, con conseguente pregiudizio per l'integrità e l'affidabilità delle informazioni stesse.

Danneggiamento di informazioni, dati e programmi informatici pubblici o di pubblico interesse (Art. 635-ter codice penale)

Il reato si configura quando un soggetto, senza autorizzazione, danneggia, distrugge, altera o rende inaccessibili informazioni, dati o programmi informatici che appartengono a enti pubblici o che rivestono un interesse pubblico, compromettendo l'integrità e l'affidabilità delle risorse informatiche destinate a scopi pubblici o di interesse collettivo.

Danneggiamento di sistemi informatici o telematici (Art. 635-quater codice penale)

Il reato si configura quando un soggetto, senza autorizzazione, danneggia, distrugge o rende inoperante un sistema informatico o telematico, compromettendone il corretto funzionamento e pregiudicando l'accesso o l'uso delle risorse informatiche da parte degli utenti legittimi.

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 635-quater 1 codice penale)

Il reato si configura quando un soggetto, senza autorizzazione, detiene, diffonde o installa apparecchiature, dispositivi o programmi informatici con l'intento di danneggiare, interrompere o compromettere il funzionamento di un sistema informatico o telematico, causando pregiudizio all'integrità e alla disponibilità delle risorse informatiche.

Danneggiamento di sistemi informatici o telematici di pubblico interesse (Art. 635-quinquies codice penale)

Il reato si configura quando un soggetto, senza autorizzazione, danneggia, distrugge o rende inoperante un sistema informatico o telematico di pubblico interesse, compromettendo la disponibilità, l'integrità o il corretto funzionamento delle risorse informatiche destinate a servizi pubblici o di interesse collettivo.

**1.1.3. Delitti di criminalità organizzata (Art. 24 ter, D. Lgs. n. 231/2001)**

Associazione per delinquere (Art. 416 codice penale)

Il reato si configura quando due o più soggetti si associano con l'intento di commettere più reati, anche non determinati, organizzando un'associazione stabile e continuativa per il compimento di atti criminosi, con la consapevolezza e l'accordo di perseguire finalità illecite.

#### **1.1.4. Reati societari (Art. 25 ter, D. Lgs. n. 231/2001)**

##### False comunicazioni sociali (Art. 2621 del codice civile)

Il reato si configura allorché gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore i destinatari sulla predetta situazione. La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

##### Fatti di lieve entità (Art. 2621-bis del codice civile)

Il reato si configura quando, in violazione delle disposizioni sul controllo delle società, un soggetto compie atti illeciti o falsificazioni in documenti societari, ma la condotta è considerata di lieve entità, in relazione all'assenza di danno significativo per la società, i soci o il mercato, e non comporta conseguenze gravi sul patrimonio sociale o sulla gestione.

##### Impedito controllo (Art. 2625 del codice civile)

Il reato si configura quando gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali.

A titolo esemplificativo, il reato potrebbe configurarsi nel caso in cui si occultino dolosamente documenti necessari per svolgere da parte degli organi preposti l'attività di controllo.

##### Corruzione tra privati (Art. 2635 del codice civile)

Il reato si configura quando un soggetto che riveste funzioni direttive o di amministrazione in un'azienda privata, o che è sottoposto alla direzione o vigilanza di tali soggetti, sollecita, accetta o riceve, anche per interposta persona, denaro o altra utilità non dovuta per compiere o omettere atti in violazione dei doveri inerenti al proprio ufficio, o quando un soggetto offre, promette o concede tali benefici con lo stesso scopo.

##### Istigazione alla corruzione tra privati (Art. 2635-bis del codice civile)

Il reato si configura quando un soggetto, con lo scopo di favorire un'azienda rispetto a un'altra, offre o promette denaro o altra utilità non dovuta a dipendenti, dirigenti, amministratori o collaboratori di un'impresa, affinché questi compiano o omettano atti in violazione dei doveri inerenti al proprio ufficio o ai propri obblighi contrattuali, alterando la leale concorrenza tra le imprese.

##### Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (Art. 2638 del codice civile)

Il reato si configura quando un soggetto, consapevolmente, espone fatti non rispondenti al vero o nasconde informazioni dovute, in comunicazioni dirette alle autorità pubbliche di vigilanza, o comunque ostacola l'esercizio delle loro funzioni, compromettendo l'efficacia dei controlli e la trasparenza richiesti dalla legge.

### **1.1.5. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25 septies, D. Lgs. n. 231/2001)**

#### Omicidio colposo (Art. 589 codice penale)

Il reato si configura quando un soggetto, per negligenza, imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline, cagiona la morte di una persona, senza volontà o intenzione di commettere il fatto, ma in violazione dei doveri di diligenza richiesti dalla situazione o dal contesto in cui si è verificato l'evento.

#### Lesioni personali colpose (Art. 590 codice penale)

Il reato si configura quando un soggetto, per negligenza, imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline, cagiona ad altri una lesione personale, determinando un indebolimento permanente di un senso o di un organo, una malattia nel corpo o nella mente, o un'incapacità di attendere alle ordinarie occupazioni per un determinato periodo di tempo.

### **1.1.6. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25 octies, D. Lgs. n. 231/2001)**

#### Ricettazione (Art. 648 codice penale)

Il reato si configura quando un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve, nasconde o comunque utilizza denaro o cose provenienti da un delitto, con la consapevolezza della loro provenienza illecita, contribuendo in tal modo a ostacolare l'identificazione della loro origine delittuosa.

#### Riciclaggio (Art. 648-bis codice penale)

Il reato si configura quando un soggetto sostituisce, trasferisce o compie altre operazioni su denaro, beni o altre utilità provenienti da un delitto, con lo scopo di ostacolare l'identificazione della loro provenienza illecita o di aiutare chi ha commesso il reato a eludere le conseguenze giuridiche delle proprie azioni.

#### Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-ter codice penale)

Il reato si configura quando un soggetto impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da un delitto, con la consapevolezza della loro origine illecita, contribuendo in tal modo a integrare o rendere apparentemente legittime risorse di provenienza delittuosa.

#### Autoriciclaggio (Art. 648-ter.1 codice penale)

Il reato si configura quando un soggetto, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce o compie altre operazioni su denaro, beni o altre utilità provenienti dal reato, con lo scopo di ostacolare l'identificazione della loro provenienza illecita, evitando che le stesse siano riconducibili alla propria attività criminosa.

### **1.1.7. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25 octies.1, D. Lgs. n. 231/2001)**

#### Indebito utilizzo e falsificazione di mezzi di pagamento diversi dai contanti (Art. 493-ter codice penale)

Il reato si configura quando un soggetto utilizza indebitamente o falsifica mezzi di pagamento diversi dai contanti, come carte di credito, carte di debito, assegni o altri strumenti simili, al fine di realizzare pagamenti non autorizzati o per procurarsi un ingiusto profitto, alterando l'autenticità o la validità di tali strumenti di pagamento.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (Art. 493-quater codice penale)

Il reato si configura quando un soggetto detiene, diffonde o cede apparecchiature, dispositivi o programmi informatici progettati per commettere reati relativi a mezzi di pagamento diversi dai contanti, come carte di credito, carte di debito o altri strumenti di pagamento elettronici, al fine di utilizzarli per compiere attività fraudolente o illecite.

Trasferimento fraudolento di valori (Art. 512-bis codice penale)

Il reato si configura quando un soggetto trasferisce, in tutto o in parte, beni o valori, anche sotto forma di denaro, con l'intento di sottrarli alla possibilità di essere aggrediti per soddisfare le obbligazioni nei confronti dei creditori, utilizzando modalità fraudolente che impediscano la loro identificazione o il loro recupero.

Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (Art. 640-ter codice penale)

Il reato si configura quando un soggetto, mediante l'utilizzo di un sistema informatico o telematico, compie una frode a danno di un altro, trasferendo indebitamente denaro, valori monetari o valuta virtuale, con l'aggravante che il trasferimento avvenga attraverso modalità informatiche, con l'intento di procurarsi un ingiusto profitto e causare un danno patrimoniale alla vittima.

**1.1.8. Delitti in materia di violazione del diritto d'autore (Art. 25 novies, D. Lgs. n. 231/2001)**

Reati in materia di software e banche dati (Art. 171-bis legge n. 633/1941)

Il reato si configura quando un soggetto, senza averne diritto, duplica, utilizza, detiene a scopo commerciale o distributivo, oppure comunica al pubblico programmi per elaboratore o banche dati protetti dal diritto d'autore, violando le norme che tutelano la proprietà intellettuale e i diritti esclusivi dell'autore o del titolare dei diritti.

**1.1.9. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25 decies, D. Lgs. n. 231/2001)**

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 377-bis codice penale)

Il reato si configura quando un soggetto induce, minaccia o inganna un altro affinché non renda dichiarazioni all'autorità giudiziaria o renda dichiarazioni false, con l'intento di ostacolare il corso della giustizia, influenzando la veridicità delle informazioni fornite durante un procedimento giudiziario.

**1.1.10. Reati ambientali (Art. 25 undecies, D. Lgs. n. 231/2001)**

Inquinamento ambientale (Art. 452-bis codice penale)

Il reato si configura quando un soggetto, in violazione delle normative ambientali, cagiona un danno significativo e grave all'ambiente mediante l'introduzione, il rilascio o lo smaltimento di sostanze o agenti inquinanti nell'aria, nell'acqua, nel suolo o in altre risorse naturali, alterando l'equilibrio ecologico e arrecando pregiudizio alla salute pubblica o al patrimonio naturale.

Disastro ambientale (Art. 452-quater codice penale)

Il reato si configura quando un soggetto, in violazione delle normative ambientali, causa un disastro ambientale grave mediante l'immissione, il rilascio o lo smaltimento di sostanze inquinanti, in modo da provocare un danno significativo e irreversibile all'ambiente, compromettendo la salute umana, gli ecosistemi e le risorse naturali, con conseguenze devastanti per l'equilibrio ecologico e per la sicurezza pubblica.

Delitti colposi contro l'ambiente (Art. 452-quinquies codice penale)

Il reato si configura quando un soggetto, con negligenza, imprudenza o imperizia, o per inosservanza di leggi, regolamenti o discipline, causa danni all'ambiente attraverso attività che, pur non intenzionali, comportano un impatto negativo sull'ecosistema, sul benessere pubblico o sulle risorse naturali, determinando un pregiudizio per l'ambiente stesso o per la salute della collettività.

Circostanze aggravanti (Art. 452-octies codice penale)

Il reato si configura quando un soggetto, nell'ambito di un reato contro l'ambiente, commette l'illecito in presenza di circostanze aggravanti specifiche, come il rischio di danno grave e irreversibile per l'ambiente, l'abuso di potere o la violazione di obblighi di sicurezza, che determinano un incremento della gravità della condotta e un danno maggiore per l'ecosistema, la salute pubblica o il patrimonio naturale.

Sanzioni penali in materia di scarichi di acque reflue (Art. 137 codice dell'ambiente)

Il reato si configura quando un soggetto effettua uno scarico di acque reflue industriali o urbane senza la prescritta autorizzazione, ovvero in violazione delle prescrizioni contenute nel provvedimento autorizzativo, o quando scarica sostanze pericolose in acque superficiali, sotterranee, o in rete fognaria in assenza delle condizioni stabilite dalla normativa ambientale, arrecando danno o potenziale pregiudizio alla qualità delle risorse idriche e all'ambiente.

Reati in materia di bonifica dei siti (Art. 257 codice dell'ambiente)

Il reato si configura quando un soggetto, obbligato per legge o in forza di un provvedimento dell'autorità competente, omette di effettuare la bonifica di un sito contaminato secondo le modalità e i termini stabiliti, oppure fornisce informazioni false o incomplete circa lo stato di contaminazione del sito, pregiudicando la tutela dell'ambiente e della salute pubblica.

Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (Art. 258 codice dell'ambiente)

Il reato si configura quando un soggetto obbligato omette di effettuare le comunicazioni previste in materia di gestione dei rifiuti, non tiene o aggiorna correttamente i registri obbligatori, oppure non utilizza, compila o conserva i formulari di identificazione dei rifiuti in conformità alle disposizioni normative, ostacolando il tracciamento e il controllo della gestione dei rifiuti.

Traffico illecito di rifiuti (Art. 259 codice dell'ambiente)

Il reato si configura quando un soggetto effettua spedizioni transfrontaliere di rifiuti in violazione delle disposizioni previste dal Regolamento (CE) n. 1013/2006, oppure organizza, trasporta, riceve, smaltisce o recupera rifiuti in modo non conforme alle norme, determinando un pericolo per l'ambiente e la salute pubblica.

False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (Art. 260 bis codice dell'ambiente)

Il reato si configura quando un soggetto fornisce false indicazioni sulla natura, sulla composizione o sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi, inserisce nel SISTRI un certificato di analisi falso o omette o altera in modo fraudolento la copia cartacea della scheda SISTRI - area movimentazione durante il trasporto di rifiuti, compromettendo la tracciabilità e la corretta gestione degli stessi.

### **1.1.11. Reati tributari (Art. 25-quinquiesdecies, D. Lgs. n. 231/2001)**

#### Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2 D.Lgs. n. 74/2000)

Il reato si configura quando un soggetto, al fine di evadere le imposte, emette o utilizza fatture o altri documenti falsi relativi a operazioni inesistenti, in modo da creare artificialmente un credito d'imposta o una deduzione indebita, con l'intento di ingannare l'autorità fiscale e ridurre il carico tributario a proprio favore.

#### Dichiarazione fraudolenta mediante altri artifici (Art. 3 D.Lgs. n. 74/2000)

Il reato si configura quando un soggetto, con artifici o raggiri diversi dall'uso di documenti falsi, omette o fornisce dichiarazioni false o incomplete al fine di ridurre o evitare il pagamento delle imposte, sfruttando mezzi ingannevoli per alterare la realtà economica e fiscale e ottenere un indebito vantaggio tributario.

#### Emissione di fatture o altri documenti per operazioni inesistenti (Art. 8 D.Lgs. n. 74/2000)

Il reato si configura quando un soggetto emette o utilizza fatture o altri documenti relativi a operazioni inesistenti, con l'intento di creare artificialmente un credito d'imposta o di documentare transazioni non reali, al fine di evadere il fisco e ottenere un indebito vantaggio economico.

#### Occultamento o distruzione di documenti contabili (Art. 10 D.Lgs. n. 74/2000)

Il reato si configura quando un soggetto, al fine di ostacolare l'accertamento delle imposte dovute, distrugge, occulta o falsifica documenti contabili o altre scritture obbligatorie previste dalla normativa fiscale, impedendo così il controllo da parte delle autorità competenti e la corretta determinazione delle imposte dovute.

#### Sottrazione fraudolenta al pagamento di imposte (Art. 11 D.Lgs. n. 74/2000)

Il reato si configura quando un soggetto, al fine di sottrarsi fraudolentemente al pagamento delle imposte, trasferisce, nasconde o distrugge beni o risorse patrimoniali, o adotta altre modalità ingannevoli per occultare la propria capacità contributiva, impedendo così l'esecuzione delle azioni necessarie per il recupero delle imposte dovute.

### **1.1.12. Delitti contro il patrimonio culturale (Art. 25 septiesdecies, D. Lgs. n. 231/2001)**

#### Furto di beni culturali (Art. 518-bis codice penale)

Il reato si configura quando un soggetto si appropria senza diritto di beni culturali, come opere d'arte, oggetti storici o archeologici, beni museali o archivistici, sottraendoli dal loro legittimo custode o luogo di conservazione, con l'intento di trarne profitto o di danneggiarli, in violazione delle normative che tutelano il patrimonio culturale.

#### Appropriazione indebita di beni culturali (Art. 518-ter codice penale)

Il reato si configura quando un soggetto, avendo la disponibilità di beni culturali, si appropria indebitamente di essi, sottraendoli al legittimo proprietario o ente detentore, con l'intento di trarne un profitto personale, non rispettando la normativa che protegge e regola la conservazione e il possesso di beni di interesse storico, artistico o archeologico.

#### Falsificazione in scrittura privata relativa a beni culturali (Art. 518-octies codice penale)

Il reato si configura quando un soggetto, al fine di ottenere un vantaggio illecito, falsifica una scrittura privata relativa a beni culturali, alterando in modo fraudolento documenti che attestano la provenienza, la proprietà, il valore o altre informazioni rilevanti su beni di interesse storico, artistico o archeologico, con l'intento di ingannare le autorità o i soggetti coinvolti nel commercio o nella gestione di tali beni.

#### Violazioni in materia di alienazione di beni culturali (Art. 518-novies codice penale)

Il reato si configura quando un soggetto aliena, trasferisce o dispone di beni culturali in violazione delle normative che regolano la tutela e la conservazione del patrimonio culturale, effettuando transazioni non autorizzate o in mancanza dei necessari permessi o procedure, in modo da eludere le leggi che proteggono tali beni di interesse storico, artistico o archeologico.

#### Uscita o esportazione illecite di beni culturali (Art. 518-undecies codice penale)

Il reato si configura quando un soggetto esegue l'uscita o l'esportazione di beni culturali dal territorio nazionale senza le autorizzazioni richieste dalla normativa vigente, eludendo i controlli e le procedure destinate a tutelare il patrimonio culturale, con l'intento di trasferire illegalmente tali beni all'estero.

#### Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (Art. 518-duodecies codice penale)

Il reato si configura quando un soggetto distrugge, disperde, deteriora, deturpa, imbratta o utilizza in modo illecito beni culturali o paesaggistici, danneggiando irreparabilmente il patrimonio storico, artistico o ambientale, con azioni che compromettono la loro integrità, il valore e la funzione di conservazione per le future generazioni.

### **1.1.13. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25 duodevicies, D. Lgs. n. 231/2001)**

#### Riciclaggio di beni culturali (Art. 518-sexies codice penale)

Il reato si configura quando un soggetto sostituisce, trasferisce o compie altre operazioni volte a ostacolare l'identificazione della provenienza illecita di beni culturali, provenienti da delitti, con l'obiettivo di reintrodurli nel circuito economico o culturale come legittimi, eludendo le normative che tutelano il patrimonio culturale e la tracciabilità di tali beni.

#### Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.)

Il reato si configura quando un soggetto, con condotte dolose e violente, causa una distruzione, un saccheggio o un danneggiamento grave e diffuso a beni culturali o paesaggistici, compromettendo in modo significativo il loro valore storico, artistico o ambientale, e arrecando un pregiudizio irreparabile al patrimonio culturale e paesaggistico.

### **1.2. Aree potenzialmente “a rischio”. Attività “sensibili”. Reati prospettabili**

In occasione dell'implementazione dell'attività di *risk mapping* sono state individuate, nell'ambito della struttura organizzativa ed aziendale di DIFESA SERVIZI, delle aree considerate “a rischio”, ovvero dei settori e/o dei processi aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati contro la Pubblica Amministrazione.

Nell'ambito di ciascuna area “a rischio” sono stati, inoltre, individuati i Ruoli Aziendali coinvolti e le relative attività c.d. “sensibili”, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in considerazione della sussistenza di rapporti diretti con gli organismi pubblici e/o i soggetti sopra individuati.

Di seguito è riepilogato il quadro in precedenza esposto.

In allegato 3 sono riportate le schede con l'individuazione e l'analisi delle aree a rischio reato nonché quelle cd. Strumentali ovvero di supporto alle attività che insistono sulle aree a rischio.

### **1.3. I principi generali di comportamento**

I responsabili delle Strutture organizzative ed i collaboratori a qualsiasi titolo impiegati/coINVOLTI nelle aree a rischio e/o in quelle strumentali sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico di DIFESA SERVIZI.

È fatto assoluto divieto di

- porre in essere condotte tali da integrare le fattispecie di reato previste dagli artt. 24 (fino a *ter*) e 25 (*bis-sexiesdecies*) del D. Lgs. 231/2001 e ss.mm.ii.;
- porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- porre in essere o agevolare operazioni in conflitto d'interesse - effettivo o potenziale - con la Società, nonché attività che possano interferire con la capacità di assumere, in modo imparziale, decisioni nel migliore interesse della Società e nel pieno rispetto delle norme del Codice Etico;
- elargire o promettere denaro a pubblici ufficiali o incaricati di pubblico servizio;
- distribuire o promettere omaggi e regali in violazione di quanto previsto dal Codice Etico e dalla prassi aziendale;
- accordare o promettere altri vantaggi, di qualsiasi natura essi siano, in favore di pubblici ufficiali o incaricati di pubblico servizio, così da determinare le conseguenze di cui al punto precedente;
- effettuare prestazioni in favore dei Partner e/o dei consulenti e/o dei fornitori che non trovino adeguata giustificazione nel contesto del rapporto associativo con essi costituito;
- riconoscere compensi in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- effettuare spese di rappresentanza in violazione delle procedure aziendali che disciplinano regole, ruoli, responsabilità e flussi nel processo autorizzativo e di rendicontazione delle spese di attenzione verso terzi;
- esercitare ogni tipo di pressione o comunque di influenzare indebitamente le decisioni della Pubblica Amministrazione in merito al rilascio ed alla gestione di licenze, autorizzazioni, certificazioni;
- detenere o diffondere indebitamente codici o programmi atti al danneggiamento informatico;
- alterare o falsificare documenti informatici di qualsiasi natura o utilizzare indebitamente la firma elettronica;
- offrire, promettere, dare, anche per interposta persona, denaro o altra utilità, che può consistere anche in opportunità di lavoro o commerciali, al funzionario pubblico coinvolto, ai rispettivi familiari o a soggetti in qualunque modo agli stessi collegati;
- accettare la richiesta o sollecitazioni, anche per interposta persona, di denaro o altra utilità, che può consistere anche in opportunità di lavoro o commerciali, dal funzionario pubblico coinvolto, dai rispettivi familiari o da soggetti in qualunque modo agli stessi collegati;
- ricercare o instaurare illecitamente relazioni personali di favore, influenza, ingerenza, idonee a condizionare, direttamente o indirettamente, l'esito del rapporto;
- prevedere deroghe e/o porre in essere deroghe alle condizioni contrattuali economiche e giuridiche standard che siano basate esclusivamente sulla natura di Pubblica Amministrazione, di Pubblico Ufficiale o di Incaricato di Pubblico Servizio del soggetto con cui si contratta;
- utilizzare, anche occasionalmente, la Società, un suo bene o una sua funzione aziendale allo scopo di consentire o agevolare la commissione di uno o più delitti di criminalità organizzata o uno o più reati transnazionali.

Inoltre, ai fini dell'attuazione dei comportamenti di cui sopra:

- occorre garantire il rispetto delle previsioni contenute nel Codice Etico di DIFESA SERVIZI;
- nell'ambito dei rapporti con la Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio deve essere garantito il rispetto dei principi di correttezza, trasparenza e buona fede;
- gli incarichi conferiti ai collaboratori esterni devono essere anch'essi redatti per iscritto, con l'indicazione dei contenuti e delle condizioni economiche pattuite;
- coloro che svolgono una funzione di controllo e supervisione in ordine agli adempimenti connessi all'espletamento delle suddette attività devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'O.d.V. eventuali situazioni di irregolarità;

- è opportuno assicurare la separazione delle attività tra chi esegue, chi autorizza e chi controlla. Tale segregazione è garantita dall'intervento, all'interno di uno stesso macro processo aziendale, di più soggetti al fine di garantire indipendenza e obiettività dei processi. La separazione delle funzioni è attuata anche attraverso l'utilizzo di sistemi informatici che abilitano certe operazioni solo a persone identificate ed autorizzate.

Su qualsiasi operazione realizzata dai soggetti sopra indicati e valutata potenzialmente a rischio di commissione di reati, l'O.d.V. avrà facoltà di effettuare i controlli ritenuti più opportuni, dei quali dovrà essere fornita evidenza scritta.

#### **1.4. I compiti dell'Organismo di Vigilanza**

Pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'O.d.V. nel documento approvato dal Consiglio di Amministrazione e denominato 'Disciplina e compiti dell'O.d.V.', in relazione alla prevenzione dei reati di cui alla presente parte speciale, l'O.d.V., tra l'altro, deve:

- verificare l'osservanza, l'attuazione e l'adeguatezza del Modello rispetto all'esigenza di prevenire la commissione dei reati contro la Pubblica Amministrazione previsti dal D. Lgs. n. 231/2001;
- vigilare sull'effettiva applicazione del Modello e rilevare gli scostamenti comportamentali che dovessero eventualmente emergere dall'analisi dei flussi informativi e dalle segnalazioni ricevute;
- verificare periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore, proponendo modifiche nel caso in cui il potere di gestione non corrisponda ai poteri di rappresentanza conferiti, nonché le procedure aziendali vigenti;
- comunicare eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

L'O.d.V. deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati contro la Pubblica Amministrazione, al Consiglio di Amministrazione ed al Collegio Sindacale, secondo i termini indicati nel documento "Disciplina e Compiti dell'O.d.V."

## **SEZIONE III – PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE**

## **1. IL QUADRO NORMATIVO DI RIFERIMENTO IN MATERIA DI PREVENZIONE DELLA CORRUZIONE E TRASPARENZA AI SENSI DELLA LEGGE 190/2012 E LA NOZIONE DI CORRUZIONE**

Numerose disposizioni della legge n. 190 del 2012 e dei relativi decreti attuativi individuano gli enti di diritto privato partecipati da pubbliche amministrazioni o in controllo pubblico e gli enti pubblici economici quali destinatari di misure di prevenzione della corruzione e di promozione della trasparenza.

Assume particolare rilievo l'art. 1, commi 60 e 61, della legge n. 190 del 2012 secondo cui in sede di intesa in Conferenza unificata Stato, Regioni e autonomie locali sono definiti gli adempimenti per la sollecita attuazione della legge 190 e dei relativi decreti delegati nelle regioni, nelle province autonome e negli enti locali, nonché «negli enti pubblici e nei soggetti di diritto privato sottoposti al loro controllo».

Ai sensi dell'art. 1, co. 17, della legge n. 190 del 2012, anche le società partecipate dalle amministrazioni pubbliche e gli enti di diritto privato in controllo pubblico, in quanto stazioni appaltanti, possono prevedere negli avvisi, nei bandi di gara o nelle lettere di invito che il mancato rispetto delle clausole contenute nei protocolli di legalità o nei patti di integrità costituisca causa di esclusione dalla gara.

Per quanto riguarda la trasparenza, intesa come accessibilità totale delle informazioni pubblicate sui siti *web*, da subito la legge n. 190 del 2012, all'art. 1, co. 34, ne aveva esteso l'applicazione agli enti pubblici economici, come già indicato nella delibera A.N.A.C. n. 50 del 2013 «Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016», e alle società partecipate dalle amministrazioni pubbliche e alle loro controllate, ai sensi dell'art. 2359 del codice civile, «limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea» e con riferimento alle informazioni contenute nei commi da 15 a 33 dell'art. 1 della stessa legge.

Dal quadro normativo sinteticamente tratteggiato emerge con evidenza l'intenzione del legislatore di includere anche le società e gli enti di diritto privato controllati e gli enti pubblici economici fra i soggetti tenuti all'applicazione della normativa in materia di prevenzione della corruzione e di trasparenza, intenzione ulteriormente rafforzata proprio dal fatto che i recenti interventi normativi in materia di trasparenza sono chiaramente indirizzati anche agli enti e alle società in questione.

La *ratio* sottesa alla legge n. 190 del 2012 e ai decreti di attuazione appare, infatti, quella di estendere le misure di prevenzione della corruzione e di trasparenza, e i relativi strumenti di programmazione, a soggetti che, indipendentemente dalla natura giuridica, sono controllati dalle amministrazioni pubbliche, si avvalgono di risorse pubbliche, svolgono funzioni pubbliche o attività di pubblico interesse.

L'Autorità ha sentito l'esigenza di emanare delle Linee guida che, in merito all'individuazione e alla gestione del rischio, tenessero in conto della necessità di coordinare quanto previsto nella legge n. 190 del 2012 per i piani di prevenzione della corruzione con le disposizioni del D. Lgs. n. 231 del 2001, sia in termini di modello di organizzazione e gestione che di controlli e di responsabilità. Esigenze di maggiori adeguamenti sono emerse per l'applicazione alle società ed agli enti controllati e partecipati della normativa sulla trasparenza ai sensi del D. Lgs. n. 33/2013.

In considerazione della peculiare configurazione del rapporto di controllo che le amministrazioni hanno con le società *in house*, queste rientrano nell'ambito delle società controllate cui si applicano le norme di prevenzione della corruzione ai sensi della legge n. 190/2012.

Ciò impone che le società controllate debbano necessariamente rafforzare i presidi anticorruzione già adottati ai sensi del D. Lgs. n. 231/2001 ovvero introdurre apposite misure anticorruzione ai sensi della legge n. 190/2012 ove assente il modello di organizzazione e gestione *ex* 231/2001.

Le misure volte alla prevenzione dei fatti di corruzione *ex* Legge 190/2012 sono elaborate dal RPC in stretto coordinamento con l'Organismo di vigilanza.

## 2. NOZIONE DI “CORRUZIONE”

Il concetto di “corruzione” preso in considerazione dal presente documento va inteso in senso lato, ossia (vedi Circolare nr. 1 del 25.01.2013 del Dipartimento della Funzione Pubblica) come “comprensivo di tutte le varie situazioni in cui, nel corso dell’attività amministrativa, si possa riscontrare l’abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati, configurando situazioni rilevanti più ampie della fattispecie penalistica di cui agli artt. 318, 319 e 319 ter c.p., che arrivano ad includere tutti i delitti contro la pubblica amministrazione disciplinati nel Titolo II, Capo I, del Codice penale e i malfunzionamenti dell’amministrazione a causa dell’uso a fini privati delle funzioni attribuite”, che possono rivestire carattere amministrativo, tecnico o di altro genere e riguardare ogni dipendente quale che sia la qualifica ricoperta.

In questo senso le situazioni rilevanti si possono circoscrivere alla c.d. **corruzione penale**, ovvero l’intera gamma dei delitti contro la pubblica amministrazione disciplinati dal Titolo II, Capo II del codice penale. Si fa riferimento, pertanto, alla fattispecie penalistica disciplinata dagli artt. 318, 319, e 319 ter del codice penale: sono cioè tali da ricomprendere non solo l’intera gamma dei delitti contro la pubblica amministrazione (Titolo II, Capo I, del codice penale).

In particolare, con la L. 190/2012, la normativa di riferimento in tema di anticorruzione si può riassumere in:

- **concussione** (art. 317 c.p.): Il pubblico ufficiale che, abusando delle sue qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro o altra utilità, è punito con la reclusione da quattro da sei a dodici anni;
- **induzione indebita a dare o promettere utilità** (art 319-*quater* c.p.): il pubblico ufficiale o l’incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell’Unione europea e il danno o il profitto sono superiori a euro 100.000;
- **corruzione per l’esercizio della funzione** (art 318 c.p.): pubblico ufficiale che, per l’esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da tre a otto anni;
- **traffico di influenze illecite** (art. 346-*bis* c.p.): chiunque, fuori dei casi di concorso nei reati di cui agli artt. 318, 319 e 319-*ter*, nonché 322 bis, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio o uno degli altri soggetti di cui all’articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica, come prezzo della propria mediazione illecita verso il pubblico ufficiale o l’incaricato di un pubblico servizio o uno degli altri soggetti di cui all’articolo 322-bis ovvero per remunerarlo, in relazione all’esercizio delle sue funzioni o dei suoi poteri ovvero in relazione al compimento di un atto contrario ai doveri di ufficio o all’omissione o al ritardo di un atto del suo ufficio;
- **corruzione amministrativa**, con riferimento ai casi di malfunzionamento dell’amministrazione a causa dell’uso a fini privati delle funzioni attribuite, ovvero le varie situazioni in cui, nel corso dell’attività amministrativa, si riscontri l’abuso da parte di un soggetto del potere affidatogli al fine di ottenere vantaggi privati, quindi le situazioni in cui, a prescindere dalla rilevanza penale, venga in evidenza un malfunzionamento dell’amministrazione a causa dell’uso a fini privati delle funzioni attribuite, ovvero l’inquinamento dell’azione amministrativa, sia nel caso in cui l’azione abbia successo, sia nel caso in cui rimanga a livello di tentativo (Circ. Funzione Pubblica n. 1 del 25 gennaio 2013).

L’elemento qualificante dell’illegalità, quindi, è l’abusività e, più precisamente, la strumentalizzazione dell’ufficio: l’esercizio delle potestà pubblicistiche diretto al conseguimento di un fine diverso o estraneo rispetto a quello previsto da norme giuridiche o dalla natura della funzione.

Illegalità, quindi, non è solo utilizzare le risorse pubbliche per perseguire un fine privato (come avviene nel caso dello sviamento dall’interesse pubblico), ma qualunque deviazione funzionale dallo schema

legale integra, di per sé, un abuso, includendo, quindi anche l'utilizzo di finalità pubbliche per perseguire illegittimamente un fine proprio dell'ente pubblico di riferimento.

Con la nuova disciplina anticorruzione, anche nel settore pubblico (come in quello privato) diventa essenziale prevenire la c.d. irresponsabilità organizzata (o colpa di organizzazione).

Prendendo in prestito una formulazione usata spesso dalla Corte dei conti, si ha colpa di organizzazione in presenza di un'organizzazione predisposta confusamente, gestita in modo inefficiente, non responsabile e non responsabilizzata.

### **3. IL PIANO TRIENNALE DI PREVENZIONE DELLA CORRUZIONE (PTPC)**

Attraverso le disposizioni della L. 190/2012 e il D. Lgs. 33 del 2013 e sue successive modifiche e integrazioni, il legislatore ha inteso perseguire i seguenti obiettivi principali:

- ridurre le opportunità che si manifestino casi di corruzione;
- aumentare la capacità di scoprire casi di corruzione;
- creare un contesto sfavorevole alla corruzione.

Nell'assetto normativo delineato la strategia di contrasto alla corruzione si articola su due livelli:

- quello nazionale, basato sul Piano Nazionale Anticorruzione (PNA), aggiornato con Delibera ANAC n. 7 del 17 gennaio 2023 e successivamente con Delibera ANAC n. 605 del 19 dicembre 2023;
- quello “decentrato”, a livello di singola amministrazione pubblica, attraverso la predisposizione del Piano Triennale per la Prevenzione della Corruzione (PTPC).

Il PTPC rappresenta lo strumento attraverso il quale l'amministrazione sistematizza e descrive il processo finalizzato a formulare una strategia di prevenzione del fenomeno corruttivo. Il Piano definisce un programma di attività e azioni operative derivanti da una preliminare fase di analisi che, in sintesi, consiste nell'esaminare l'organizzazione, le sue regole e le sue prassi di funzionamento in termini di “possibile esposizione” al fenomeno corruttivo. Il PTPC è un programma di attività, con indicazione delle aree di rischio e dei loro rischi specifici, delle misure da implementare per la prevenzione in relazione al livello di pericolosità dei rischi specifici, dei responsabili per l'applicazione di ciascuna misura e dei tempi.

Il PTPC non è un documento di studio o di indagine, ma uno strumento per l'individuazione di misure concrete, da realizzare con certezza e da vigilare quanto ad effettiva applicazione e quanto ad efficacia preventiva della corruzione.

Al fine di realizzare un'efficace strategia di prevenzione del rischio di corruzione, i PTPC debbono essere coordinati rispetto al contenuto di tutti gli altri strumenti di programmazione presenti nell'amministrazione quali i modelli di organizzazione e gestione (MOG) del D. Lgs. n. 231 del 2001 e debbono essere strutturati come documenti di programmazione, con l'indicazione di obiettivi, indicatori, misure, responsabili, tempistica e risorse.

Il Piano anticorruzione, quindi, gioca il ruolo di strumento di “organizzazione dell'organizzazione”, è uno strumento che una compagine pubblica adotta per evitare, all'interno della propria struttura, si realizzino determinati atti illeciti aventi rilevanza penale.

Come precisato nel PNA, al fine di pianificare le strategie di prevenzione della corruzione, l'amministrazione deve esaminare attentamente la propria organizzazione, le sue regole e le prassi di funzionamento per valutarne la possibile esposizione al fenomeno corruttivo.

Per la predisposizione del PTPC è, pertanto, necessaria una propedeutica ed attenta ricostruzione dei processi organizzativi dell'Ente e l'individuazione delle c.d. aree di rischio.

L'individuazione delle aree di rischio consente, infatti, di identificare con precisione le “attività” dell'Ente in relazione alle quali emerge la necessità di prevedere misure di prevenzione e di stabilire la graduazione degli interventi da adottare attraverso le previsioni del PTPC.

Come è noto, la L. 190/2012 (art. 1, comma 16) ha già individuato specifiche aree di rischio, “obbligatorie”, riguardanti, a titolo esemplificativo e non esaustivo, i processi finalizzati a:

- acquisizione e progressione del personale;

- affidamento di lavori, servizi e forniture nonché all'affidamento di ogni altro tipo di commessa o vantaggio pubblici disciplinato dal Decreto Legislativo 31 marzo 2023, n. 36.;
- adozione di provvedimenti ampliativi della sfera giuridica dei destinatari **privi** di effetto economico diretto ed immediato per il destinatario;
- adozione di provvedimenti ampliativi della sfera giuridica dei destinatari **con** effetto economico diretto ed immediato per il destinatario.

Ciascuna amministrazione è, dunque, tenuta ad analizzare con attenzione tali aree di rischio (e le rispettive sotto-aree); è, inoltre, raccomandata l'inclusione nel PTPC di ulteriori aree di rischio, in considerazione delle specifiche caratteristiche dell'attività svolta dal singolo ente e delle peculiarità del contesto di riferimento.

Come indicato nel citato PNA il processo di gestione del rischio finalizzato all'adozione del presente PTPC si compone delle seguenti fasi:

- 1) la mappatura dei processi attuati dall'amministrazione;
- 2) la valutazione del rischio per ciascun processo;
- 3) il trattamento del rischio.

Il PNA prevede, inoltre, che, indipendentemente dall'analisi svolta, ciascun PTPC preveda una serie di misure di prevenzione "obbligatorie" e di carattere trasversale. Tali misure fanno riferimento a:

- ✓ formazione in tema di anticorruzione;
- ✓ codice di comportamento assorbito dal Codice Etico (Allegato2);
- ✓ trasparenza;
- ✓ altre misure obbligatorie:
- ✓ rotazione del personale;
- ✓ obbligo di astensione in caso di conflitto di interesse;
- ✓ disciplina degli incarichi d'ufficio e delle attività non consentite ai dipendenti pubblici;
- ✓ direttive per l'attribuzione di incarichi dirigenziali;
- ✓ definizione di modalità di verifica del rispetto del divieto di svolgere attività incompatibili a seguito della cessazione del rapporto (c.d. *Pantouflage* e *Revolving doors*);
- ✓ direttive per effettuare controlli su precedenti penali (delitti contro la PA) ai fini dell'attribuzione degli incarichi (formazione di commissioni, ecc.) e della assegnazione ad uffici;
- ✓ adozione di misure per la tutela del dipendente che segnala gli illeciti (*whistleblower*);
- ✓ predisposizione di protocolli di legalità negli affidamenti;
- ✓ azioni di sensibilizzazione e rapporto con la società civile.

### **3.1. Oggetto, Finalità e Destinatari**

Il PTPC rappresenta quindi lo strumento attraverso il quale la Società descrive la propria strategia di prevenzione della corruzione, identificando i potenziali rischi ai quali è maggiormente esposta e individuando le azioni che intende attivare per prevenire eventuali casi di corruzione.

Attraverso il PTPC si intende attivare azioni efficaci e coerenti tra loro, idonee a ridurre significativamente il rischio che si possano generare comportamenti corrotti e, al contempo, mira a favorire una condotta del proprio personale ispirata ai principi etici di integrità, legalità, lealtà, correttezza e trasparenza, in netta contrapposizione al fenomeno della corruzione.

La strategia di prevenzione della corruzione è finalizzata a:

1. creare un contesto sfavorevole al fenomeno della corruzione;
2. aumentare le capacità della Società di far emergere eventuali casi di corruzione e malcostume;
3. ridurre le opportunità e gli incentivi all'adozione di comportamenti illeciti.

Per raggiungere tale obiettivo, si intende creare un sistema strutturato di prevenzione basato sulla gestione del rischio di corruzione, attraverso l'utilizzo di tecniche proprie del *risk management* e l'attuazione di misure a partire da quelle indicate nel PNA.

Il PTPC è un documento di natura programmatica che descrive sia le misure di prevenzione intraprese sia quelle da intraprendere, coordinando tra loro i diversi interventi proposti.

Il Piano, oggetto di aggiornamento annuale, si configura come un processo ciclico in cui le strategie e gli strumenti vengono progressivamente affinati, modificati e aggiornati in relazione ai *feedback* ottenuti a seguito della loro applicazione.

Il PTPC è diretto a tutto il personale della Società che, a seguito della pubblicazione, dovrà provvedere alla sua osservanza e, per quanto di propria competenza, alla sua esecuzione. La diffusione del PTPC e del Codice Etico a tutto il personale sarà curata dalla Direzione Risorse Umane e Innovazione Tecnologica, responsabile della gestione del personale, con particolare attenzione al nuovo personale che sarà assegnato alla Società. Inoltre, sono destinatari del Piano tutti i collaboratori, anche occasionali nonché ogni soggetto che, a qualsiasi titolo, collabori con imprese fornitrici di beni e servizi o che realizzino opere in favore della Società. Per questi ultimi soggetti, la diffusione del PTPC e del Codice Etico verrà curata anche dalla Direzione Gare, Contratti e Centrale di Committenza.

### **3.2. I soggetti responsabili e gli attori coinvolti**

#### **3.2.1. Il Responsabile della Prevenzione della Corruzione (RPC)**

Le società *in house* ed in generale le società controllate sono tenute a nominare un Responsabile per la prevenzione della corruzione. Al RPC sono riconosciuti poteri di vigilanza sull'attuazione effettiva delle misure, nonché di proposta delle integrazioni e delle modifiche delle stesse ritenute più opportune.

In aderenza a quanto previsto dalle norme e dalle Linee guida ANAC, il Responsabile della prevenzione della corruzione è stato nominato dal Consiglio di Amministrazione nella seduta del 23 gennaio 2024. La legge, infatti, prevede che ciascuna amministrazione nomini un unico responsabile della prevenzione della corruzione e, ove possibile, cerchi di assicurare la coincidenza con il titolare dell'incarico di Responsabile della trasparenza.

Il RPC è tenuto a:

- elaborare la proposta di PTPC, da sottoporre all'organo di indirizzo ai fini della sua approvazione (articolo 1 comma 8, L. 190/2012);
- definire appropriate procedure per la selezione e la formazione del personale destinato a operare in settori particolarmente esposti alla corruzione (articolo 1 comma 8, L. 190/2012);
- verificare l'efficace attuazione del piano e la sua idoneità (articolo 1 comma 10, lett. a), L. 190/2012);
- proporre modifiche al Piano in caso di accertamenti di significative violazioni o di mutamenti dell'organizzazione (articolo 1 comma 10, lett. a) L. 190/2012);
- verificare, d'intesa con il dirigente competente, l'effettiva rotazione degli incarichi nelle Aree preposte allo svolgimento delle attività nel cui ambito è più elevato il rischio che siano commessi reati di corruzione (articolo 1, comma 10 lettera b) L. 190/2012);
- individuare il personale da inserire nei percorsi di formazione sui temi dell'etica e della legalità (articolo 1 comma 10, lett. c) L. 190/2012);
- coordinare le azioni in risposta alla valutazione del rischio di corruzione.

Con l'atto di nomina al RPCT sono assegnati idonei e congrui poteri di vigilanza sull'attuazione effettiva delle misure previste nel PTPC. A tal fine sono garantiti al RPCT i seguenti poteri:

- collaborare con le strutture aziendali competenti alla redazione delle procedure aziendali che abbiano impatto in materia di anticorruzione e trasparenza;
- effettuare controlli sulle procedure e sui processi aziendali che abbiano impatto in materia di anticorruzione e trasparenza, proponendo le modifiche ritenute necessarie e, nel caso di mancata attuazione, segnalare il tutto al Consiglio di Amministrazione;
- interfacciarsi con ciascun Referente aziendale, ai fini dell'eventuale attivazione delle azioni necessarie per il miglior espletamento dei propri compiti – disporre della libertà di accesso senza limitazioni alle informazioni aziendali rilevanti per le proprie attività di indagine, analisi e controllo;
- richiedere informazioni, rilevanti per le attività di competenza, a qualunque funzione aziendale, che è tenuta a rispondere.

Il RPCT può, inoltre:

- segnalare al CdA e/o all'AD e/o all'OdV e/o al Collegio sindacale e/o agli altri Organi/strutture di controllo le disfunzioni inerenti l'attuazione delle misure in materia di prevenzione della corruzione e della trasparenza;
- indicare agli organi competenti, in base a quanto definito nel Sistema disciplinare della Società, i nominativi dei dipendenti che non hanno attuato correttamente le misure in materia di prevenzione della corruzione e di trasparenza per l'eventuale attivazione del procedimento disciplinare.

### **3.2.2. Ambito soggettivo**

#### Gli Amministratori

Ai sensi dell'art. 1 co. 2 lett. l) D. Lgs.39/2013 sono definiti Amministratori coloro che ricoprono "gli incarichi di Presidente con deleghe gestionali dirette, Amministratore Delegato e assimilabili, di altro organo di indirizzo dell'attività dell'ente comunque denominato". Rispettano queste caratteristiche l'Amministratore Delegato ed il Presidente di Difesa Servizi.

Essi dispongono di competenze rilevanti nel processo di individuazione delle misure di prevenzione della corruzione ed, infatti, hanno l'onere di nominare il RPC ed adottano il PTPC.

Inoltre durante il C.d.A. di approvazione del PTPC dovrà essere presente il RPC al fine di illustrare adeguatamente i contenuti e le implicazioni attuative.

#### Il Direttore Generale

Il nuovo organigramma societario prevede un Direttore Generale e le relative funzioni sono attribuite al Dott. Luca Andreoli, che svolge anche le funzioni di Amministratore Delegato.

La procedura ha visto la finalizzazione, da ultimo in sede di rinnovo dell'incarico, in occasione del Consiglio di Amministrazione tenutosi in data 22 maggio 2023.

La figura, posta formalmente alle dipendenze dell'Amministratore Delegato, coordina e sovrintende le Divisioni/Direzione di line, anche avvalendosi della collaborazione delle Direzioni/Aree del livello di staff e supporto.

Ove nel corso dell'anno, si venisse a modificare la configurazione suddetta, così come nel caso di qualsiasi altra modifica significativa della struttura societaria, si provvederà ad aggiornare il presente PTPC nelle parti che a vario titolo potrebbero esserne interessate.

#### I Capi Divisione e i Capi di Direzione Autonoma

Ancorché la norma individui nei dirigenti le figure principi cui il RPC dovrebbe fare riferimento per l'applicazione del PTPC, per la particolare struttura organizzativa di DIFESA SERVIZI, le figure di riferimento di livello elevato si identificano con i Capi Divisione e i Capi di Direzione Autonoma (con riferimento a quelle Direzioni non inserite nelle Divisioni). Attualmente tali Divisioni e Direzioni sono rette da personale militare che, nello specifico, è chiamato a:

- concorrere alla definizione di misure idonee a prevenire e contrastare i fenomeni di corruzione e a controllarne il rispetto da parte dei dipendenti cui sono preposti;
- fornire le informazioni richieste dal soggetto competente per l'individuazione delle attività nell'ambito delle quali è più elevato il rischio corruzione e formulare specifiche proposte volte alla prevenzione del rischio medesimo;
- provvedere al monitoraggio delle attività nell'ambito delle quali è più elevato il rischio corruzione svolte nelle Aree a cui sono preposti, disponendo, con provvedimento motivato, la rotazione del personale nei casi di avvio di procedimenti penali o disciplinari per condotte di natura corruttiva;
- vigilare sull'applicazione del Codice Etico e verificarne le ipotesi di violazione, ai fini dei conseguenti procedimenti disciplinari;
- individuare il personale da inserire nei programmi di formazione;

- svolgere attività informativa nei confronti del RPC, relazionando con cadenza semestrale sullo stato di attuazione del PTPC.

### **3.2.3. I referenti del RPC**

La legge prevede la possibilità di individuare dei *referenti* per la corruzione che operano nelle strutture e articolazioni dell'ente.

In particolare i referenti per la prevenzione della corruzione sono chiamati a:

- svolgere attività informativa nei confronti del RPC e Responsabile della Trasparenza, affinché questi abbia elementi e riscontri sull'intera organizzazione e attività svolta dai responsabili assegnati alle Articolazioni di riferimento;
- monitorare l'attuazione delle misure obbligatorie e ulteriori per la prevenzione della corruzione, nell'ambito delle strutture di riferimento;
- monitorare il corretto adempimento degli obblighi normativi in materia di trasparenza, a cura delle strutture di competenza;
- coadiuvare il RPC nel monitoraggio del rispetto delle previsioni del piano da parte delle strutture e dei responsabili di afferenza;
- informare tempestivamente il RPC di ogni segnalazione di ritardo procedimentale;
- facilitare i flussi informativi tra le diverse strutture;
- segnalare al RPC ogni esigenza di modifica del piano, in caso di accertate significative violazioni delle prescrizioni ovvero di avvenuti mutamenti del contesto di riferimento.

La rete dei referenti risponde, periodicamente tramite la produzione di *report*, note ed elaborati, direttamente al RPC. I referenti possono essere convocati singolarmente o collegialmente dal RPC in merito all'attuazione del PTPC e delle azioni finalizzate alla prevenzione del rischio di corruzione.

Per quanto detto precedentemente, la Società si è dotata di una rete di referenti individuata nelle figure dei responsabili di:

- Divisione Patrimonio;
- Divisione Brand e Media;
- Divisione Innovazione e Tecnologie;
- Divisione Cultura e Professioni;
- Direzione Affari Legali, Qualità e Rapporto Industriali;
- Direzione Risorse Umane e Innovazione Tecnologica;
- Direzione Relazioni Istituzionali e Sviluppo;
- Direzione Amministrazione, Finanza e Controllo;
- Direzione Gare, Contratti e Centrale di Committenza;
- Area Comunicazione;
- Area Compliance, Risk Mgmt. e Societario;
- Segreteria del Presidente e del CdA.

### **3.2.4. I dipendenti della Società**

I dipendenti osservano le misure contenute nel PTPC e sono chiamati a segnalare le situazioni di illecito ai propri responsabili ed i casi di personale conflitto di interessi.

### **3.2.5. I collaboratori e consulenti a qualsiasi titolo della Società**

Questi osservano, per quanto compatibili, le misure contenute nel PTPC e gli obblighi di condotta previsti dal Codice Etico e segnalano le situazioni di illecito.

## **3.3. Individuazione e gestione dei rischi di corruzione**

In coerenza con quanto previsto dall'art. 1, co. 9, della legge n. 190/2012 e dall'art. 6, co. 2, del D. Lgs. n. 231/2001, è stata effettuata un'analisi del contesto e della realtà organizzativa della Società per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare fatti corruttivi.

Il processo di gestione del rischio, ossia l'insieme delle attività coordinate per guidare e tenere sotto controllo l'azienda con riferimento al rischio di corruzione, è stato condotto in osservanza della metodologia generale indicata dal PNA.

Pertanto, sono state seguite le fasi operative di seguito elencate:

- a) mappatura e valutazione delle aree del rischio;
- b) valutazione del rischio per ciascun processo;
- c) trattamento del rischio.

### **3.3.1. Mappatura e valutazione delle aree del rischio**

In accordo a quanto previsto dal PNA, la valutazione del rischio ha considerato alcuni settori/aree, in particolare:

- A) Area acquisizione e progressione del personale:
  1. reclutamento;
  2. progressioni di carriera;
  3. conferimento di incarichi di collaborazione e consulenza;
- B) Area affidamento di lavori, servizi e forniture:
  1. definizione dell'oggetto dell'affidamento;
  2. individuazione dello strumento/istituto per l'affidamento;
  3. selezione del contraente;
  4. verifica dell'aggiudicazione e stipula del contratto;
  5. esecuzione del contratto;
  6. verifica dell'eventuale anomalia delle offerte;
  7. procedure negoziate;
  8. affidamenti diretti;
  9. revoca del bando;
  10. redazione del cronoprogramma;
  11. varianti in corso di esecuzione del contratto;
  12. subappalto;
  13. utilizzo di rimedi di risoluzione delle controversie alternativi a quelli giurisdizionali durante la fase di esecuzione del contratto;
- C) Area provvedimenti ampliativi della sfera giuridica dei destinatari **privi** di effetto economico diretto ed immediato per il destinatario;
- D) Area provvedimenti ampliativi della sfera giuridica dei destinatari **con** effetto economico diretto ed immediato per il destinatario.

Nelle schede in allegato 4 sono riportati i rischi per ogni processo analizzato e le azioni che si sono individuate per prevenire e fronteggiare il rischio ponderale.

### **3.4. Sistema di controlli**

La definizione di un sistema di gestione del rischio si completa con la valutazione del sistema di controllo interno previsto dal modello di organizzazione e gestione del rischio sulla base del D. Lgs. n. 231 del 2001. Si rimanda per tale ragione alla parte speciale del modello e agli allegati. In quest'ottica vi è un costante coordinamento tra i controlli ai sensi del D. Lgs. 231/2001 e quelli per la prevenzione di rischi di corruzione di cui alla L.190/2012.

### **3.5. Inconferibilità specifiche per gli incarichi di amministratore e per gli incarichi dirigenziali**

La materia delle incompatibilità e delle inconferibilità degli incarichi è disciplinata dal D. Lgs. n. 39/2013. In particolare in capo a coloro che rivestono incarichi di Amministratore, come definiti dall'art. 1, co. 2, lett. l), del D. Lgs. n. 39/2013 - e cioè "gli incarichi di Presidente con deleghe gestionali dirette, Amministratore Delegato e assimilabili, di altro organo di indirizzo dell'attività dell'ente comunque denominato" - e a coloro cui sono conferiti incarichi dirigenziali, sono previste le seguenti cause ostative:

- art. 3, co. 1, lett. d), relativamente alle “inconferibilità di incarichi in caso di condanna per reati contro la pubblica amministrazione”;
  - art. 6, sulle “inconferibilità di incarichi a componenti di organo politico di livello nazionale”;
  - art. 7, sulla “inconferibilità di incarichi a componenti di organo politico di livello regionale e locale”.
- Per i dirigenti, si applica l’art.3, comma 1, lett. c), relativo alle cause di inconferibilità a seguito di condanne per reati contro la pubblica amministrazione.

In DIFESA SERVIZI, quale società *in house*, la nomina degli amministratori è effettuata dal Ministro della Difesa il quale verifica che:

- a. negli atti di attribuzione degli incarichi o negli interpelli siano inserite espressamente le condizioni ostative al conferimento dell’incarico;
- b. i soggetti interessati rendano la dichiarazione di insussistenza delle cause di inconferibilità all’atto del conferimento dell’incarico.

### **3.6. Incompatibilità specifiche per gli incarichi di amministratore e per gli incarichi dirigenziali**

Il C.d.A. verifica l’insussistenza di eventuali situazioni di incompatibilità nei confronti dei titolari degli incarichi di amministratore, come definiti dall’art. 1, co. 2, lett. l) del D. Lgs. n. 39/2013, sopra illustrato, e nei confronti di coloro che rivestono incarichi dirigenziali.

Le situazioni di incompatibilità per gli amministratori sono quelle indicate, in particolare, dalle seguenti disposizioni del D. Lgs. n. 39/2013:

- art. 9, riguardante le “incompatibilità tra incarichi e cariche in enti di diritto privato regolati o finanziati, nonché tra gli stessi incarichi e le attività professionali” e, in particolare, il co. 2;
- art. 11, relativo a “incompatibilità tra incarichi amministrativi di vertice e di amministratore di ente pubblico e cariche di componenti degli organi di indirizzo nelle amministrazioni statali, regionali e locali”, ed in particolare i co. 2 e 3;
- art. 13, recante “incompatibilità tra incarichi di amministratore di ente di diritto privato in controllo pubblico e cariche di componenti degli organi di indirizzo politico nelle amministrazioni statali, regionali e locali”.

A tali fini, la Società, attraverso la Direzione Risorse Umane e Innovazione Tecnologica, verifica che:

- a. siano inserite espressamente le cause di incompatibilità negli atti di attribuzione degli incarichi o negli interpelli per l’attribuzione degli stessi;
- b. i soggetti interessati rendano la dichiarazione di insussistenza delle cause di incompatibilità all’atto del conferimento dell’incarico e nel corso del rapporto.

### **3.7. Rotazione degli incarichi**

Quanto stabilito nel PNA attribuisce al Consiglio di Amministrazione, l’adozione di adeguati sistemi di rotazione del personale apicale addetto alle aree a rischio, con l’accortezza di mantenere la continuità e la coerenza degli indirizzi e le necessarie competenze delle strutture.

La struttura societaria prevede una naturale turnazione e rotazione del personale in tutte le sue componenti, in quanto, così come previsto dalla Statuto societario e dal Contratto di servizio all’art. 6 comma 5, la durata di ogni assegnazione triennale, rinnovabile per triennio.

Laddove comunque allo scadere dei primi tre anni non ci sia cambiamento degli incarichi, si utilizza quale altra misura efficace, in combinazione o alternativa alla rotazione, la distinzione delle competenze attribuendo a soggetti diversi i compiti di:

- a) svolgere istruttorie e accertamenti;
- b) adottare decisioni;
- c) effettuare verifiche.

Qualora tuttavia si renda necessario svolgere una rotazione degli incarichi al fine di eliminare un potenziale rischio corruzione individuato o segnalato al RPC, questo lo proporrà al Consiglio di Amministrazione per la necessaria delibera.

Si rappresenta che nel corso dell’anno 2024 non si sono ricevute segnalazioni né si è riscontrata la necessità di dover proporre all’organo amministrativo la rotazione di personale per motivi riconducibili

a fenomeni corruttivi, attesa anche una fisiologica turnazione per avvicendamento negli incarichi in ambito Forza Armata che ha interessato alcune figure chiave nell'organigramma societario.

### **3.8. Monitoraggio**

In coerenza con quanto previsto dal D. Lgs. 231/2001, gli Amministratori e i Responsabili delle Articolazioni interne sono tenuti a fornire al RPC, in qualsiasi momento lo richieda i *report* relativi allo stato di attuazione del PTPC, al fine di consentire di predisporre la relazione da inoltrare all'organo di indirizzo politico.

La relazione trasmessa dai referenti deve contenere, tenendo conto delle attività svolte nell'esercizio delle proprie funzioni, i seguenti elementi:

- gli eventuali mutamenti nell'organizzazione o nell'attività della propria articolazione che richiedano una modifica del PTPC;
- l'eventuale accertamento di significative violazioni delle prescrizioni del Piano tali da richiedere una modifica;
- gli esiti del monitoraggio sui rapporti tra la Società e i soggetti che con la stessa stipulano contratti o che sono interessati a procedimenti di concessione o di erogazione di vantaggi economici di qualunque genere;
- il personale da inserire nei programmi di formazione in quanto chiamato ad operare nelle aree nelle quali è più elevato il rischio di corruzione;
- i dati o le notizie di incompatibilità ai sensi del D. Lgs. 39/2013;
- qualunque altra informazione ritenuta utile per il pieno conseguimento delle finalità del presente PTPC.

Il RPC può tenere conto di segnalazioni non anonime provenienti da eventuali portatori di interesse, sufficientemente circostanziate, che evidenzino situazioni di anomalia e configurino la possibilità di un rischio probabile di corruzione.

Al fine di facilitare le segnalazioni al RPC si procederà ad attivare gli opportuni canali di comunicazione dedicati e, precisamente, una apposita casella di posta elettronica (rpct@difesaservizi.it). Le segnalazioni possono, altresì, essere inoltrate per iscritto, anche in forma anonima, all'indirizzo: Responsabile Prevenzione della Corruzione, DIFESA SERVIZI S.p.a., Via Flaminia, 335, 00196, Roma.

Il RPC entro il 31 gennaio di ogni anno pubblica sul sito [www.difesaservizi.it](http://www.difesaservizi.it) una relazione recante i risultati dell'attività svolta.

Di seguito si elencano le tipologie dei dati pubblicati sul sito web della Società ed i Responsabili, ossia i Capi Divisioni/Direzioni competenti per gli aggiornamenti:

TIPOLOGIE DI DATI	RESPONSABILE/CAPO
Organigramma (monitoraggio ad ogni variazione)	Direzione Risorse Umane e Innovazione Tecnologica
Gare e contratti (monitoraggio mensile)	Direzione Gare, Contratti e Centrale di Committenza;
Consulenti ed esperti (monitoraggio semestrale)	tutti i Responsabili delle Strutture
Pubblicazione retribuzione dei dirigenti (monitoraggio ai rinnovi contrattuali)	Direzione Risorse Umane e Innovazione Tecnologica
Pubblicazione Curricula*, retribuzioni, compensi ed indennità di coloro che rivestono incarichi di indirizzo politico- amministrativo (monitoraggio annuale)	Direzione Risorse Umane e Innovazione Tecnologica
Richieste di autorizzazione ad assumere (monitoraggio annuale)	Direzione Risorse Umane e Innovazione Tecnologica
Tassi di presenza ed assenza del personale (monitoraggio mensile)	Direzione Risorse Umane e Innovazione Tecnologica

Ammontare dei premi collegati alla performance dei dirigenti (monitoraggio annuale)	Direzione Risorse Umane e Innovazione Tecnologica Direzione Amministrazione, Finanza e Controllo;
Codice Etico (monitoraggio in caso di una nuova adozione / modifica)	Direzione Risorse Umane e Innovazione Tecnologica
Elenco delle caselle di posta elettronica certificata attive (monitoraggio annuale)	Direzione Risorse Umane e Innovazione Tecnologica
Piano triennale per la trasparenza e l'integrità (monitoraggio alle scadenze Programmate)	Responsabile della Trasparenza
Bilancio di previsione (monitoraggio annuale)	Direzione Amministrazione, Finanza e Controllo
Conto finanziario (monitoraggio annuale)	Direzione Amministrazione, Finanza e Controllo;
Attività di controllo di dichiarazioni sostitutive in luogo di autorizzazioni (monitoraggio semestrale)	tutti i Responsabili delle Strutture

### **3.9. Tutela del dipendente pubblico che segnala gli illeciti (*whistleblowing*)**

Il *whistleblowing* è stato introdotto in Italia con una legislazione specifica a fine 2017, con la legge n. 179. Questa normativa regolamentava in modo completo l'istituto per la pubblica amministrazione, mentre introduceva alcune disposizioni anche per le organizzazioni del settore privato dotate di un modello organizzativo di gestione e controllo ex. D.Lgs. n. 231/2001.

La legge n. 179/2017 è stata superata dalla legge di trasposizione della Direttiva Europea in materia di *whistleblowing* (n. 1937/2019). La nuova legge, il Decreto Legislativo n. 24/2023, è l'attuazione della Direttiva UE n. 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. La nuova normativa prevede oneri in capo alle organizzazioni pubbliche e private, in particolare: tutti gli enti pubblici devono prevedere procedure interne per la gestione delle segnalazioni; lo stesso obbligo è in carico ai soggetti del settore privato che hanno un modello organizzativo ex D.Lgs. n. 231/2001 e a tutte le organizzazioni private con almeno 50 dipendenti.

La fondamentale innovazione prevede che il dipendente, il facilitatore, la persona coinvolta e la persona comunque menzionata nella segnalazione, nonché il contenuto della segnalazione e della relativa documentazione che, nell'interesse dell'integrità della pubblica amministrazione, sono oggetto di segnalazione all'Organismo interno di Vigilanza (OdV), come stabilito dal Consiglio di Amministrazione della Società, oppure ai sensi dell'articolo 1, comma 7, della legge 6 novembre 2012, n. 190 al Responsabile della prevenzione della corruzione e della trasparenza, ovvero all'Autorità nazionale anticorruzione (ANAC), o denuncia all'autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui si è venuti a conoscenza in ragione del proprio rapporto di lavoro, rimangano nell'anonimato. Il segnalatore e il facilitatore non possono essere sanzionati, demansionati, licenziati, trasferiti, o sottoposti ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione. L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante e del facilitatore è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere. L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.

La Legge stabilisce la tutela dell'identità del segnalante e del facilitatore, infatti non può essere rivelata. Nell'ambito del procedimento penale, l'identità del segnalante e del facilitatore è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. Nell'ambito del

procedimento dinanzi alla Corte dei conti, l'identità del segnalante e del facilitatore non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identità del segnalante e del facilitatore non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante e del facilitatore sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante e del facilitatore alla rivelazione della sua identità.

La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.

L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni. Le Linee guida ANAC prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e del facilitatore e per il contenuto delle segnalazioni e della relativa documentazione. L'ANAC può applicare una sanzione amministrativa pecuniaria qualora venga accertata: nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità; l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi; il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione. È a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli. Il segnalante e il facilitatore che siano licenziati a motivo della segnalazione sono reintegrati nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23.

Le tutele non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante e del facilitatore per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la loro responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave».

A tal fine, l'Organismo interno di Vigilanza (OdV), come stabilito dal Consiglio di Amministrazione della Società, vigilerà affinché nessuna di tali azioni venga posta in essere a danno dei segnalanti, interessando in caso contrario l'autorità disciplinare competente.

L'Organismo interno di Vigilanza (OdV), alla ricezione della segnalazione, intraprende le iniziative necessarie e valuta eventualmente di trasmette con tempestività la segnalazione al RPC. È possibile inviare segnalazioni attraverso la piattaforma digitale on-line (<https://whistleblowing.difesaservizi.it>), al sito web societario, attestata direttamente all'invio delle segnalazioni all'Organismo interno di Vigilanza (OdV).

Indipendentemente dalla modalità di scelta per la trasmissione della segnalazione, una volta pervenuta, sarà protocollata e trattata con modalità e soluzioni tecnico-informatiche che ne garantiscano la riservatezza anche per la successiva conservazione.

Durante il corrente anno saranno attivate iniziative di formazione per diffondere la conoscenza del nuovo sistema di segnalazione al fine di garantirne un corretto utilizzo. A tal riguardo, si riportano i links delle pagine predisposte al sito web societario, per ogni approfondimento e per la procedura di gestione delle segnalazioni: <https://www.difesaservizi.it/whistleblowing>; <https://www.difesaservizi.it/societa-trasparente/programma-per-la-trasparenza-e-integrita>.

### **3.10. Formazione del personale**

L'acquisizione da parte dei Responsabili delle Divisioni/Direzioni, e di tutti coloro che occupano posizioni di responsabilità con competenze specifiche in materia di prevenzione della corruzione, risulta fondamentale nel più ampio quadro della funzione che essi rivestono nel processo di gestione dei rischi. La formazione dovrà essere somministrata con contenuti e modalità differenti a seconda dei

destinatari. La struttura dei moduli formativi destinati ai Responsabili dovrà prevedere lo svolgimento di incontri di breve durata, in modo tale da minimizzare l'impatto sull'organizzazione del lavoro. Dovrà essere valutata anche l'opportunità di organizzare la formazione, a seconda della tematica e dei destinatari, con modalità *in house* al fine di orientare gli interventi sulla base di esperienze concrete dell'Amministrazione, contenendo al contempo i costi organizzativi.

Come già avvenuto negli anni precedenti, il RPC, al fine di essere costantemente aggiornato sulla normativa di settore, parteciperà agli specifici corsi organizzati dalla Scuola Nazionale dell'Amministrazione (SNA).

Si ritiene necessario, inoltre, adottare quale procedura *standard*, il rilascio di una Dichiarazione di presa d'atto, da parte di tutti i dipendenti, del Piano Triennale di Prevenzione della Corruzione, oltre che del Codice Etico. Tale attività sarà curata dalla Direzione Risorse Umane e Innovazione Tecnologica, responsabile della gestione del personale, con particolare attenzione al nuovo personale che sarà assegnato alla Società.

### **3.11. Monitoraggio dei rapporti tra amministrazione e i soggetti che con la stessa stipulano contratti o che sono interessati a procedimenti di autorizzazione, concessione, o erogazione**

In considerazione della particolare attività svolta dalla Società, si ritiene che possa essere sufficiente una attività di formazione del personale per dare conoscenza allo stesso dell'obbligo di astensione, delle conseguenze scaturenti dalla sua violazione e dei comportamenti da seguire in caso di conflitto di interessi.

### **3.12. Attività successiva alla cessazione del rapporto di servizio/lavoro**

Tra le misure di prevenzione della corruzione, particolare rilievo assume il divieto di *pantouflage*. In particolare, tale misura agisce sulla fase successiva alla cessazione del rapporto di servizio/lavoro/consulenza con una pubblica amministrazione. Si tratta di un'ipotesi di incompatibilità successiva che si affianca e si aggiunge ai meccanismi di "inconferibilità", ossia i divieti temporanei di accesso ad una carica o ad un incarico, e di "incompatibilità", ossia il divieto di cumulo di più cariche o incarichi, previsti dal D. Lgs. 8 aprile 2013, n. 39 "Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico". Tali misure hanno il comune fine di neutralizzare possibili conflitti di interesse nello svolgimento delle funzioni e di incarichi attribuiti a un dipendente pubblico al fine di salvaguardare l'imparzialità dell'azione amministrativa. La disciplina del *pantouflage* è contenuta agli artt. 53, co. 16-ter del d.lgs. n. 165/2001, articolo 21 del d.lgs. n. 39/2013 e, in descrizione, nelle Linee guida n. 1 adottate dall'ANAC con Delibera n. 493 del 25 settembre 2024.

L'ambito di applicazione del divieto di *pantouflage*, inserito all'interno del menzionato d.lgs. n. 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", è stato esteso, successivamente, per effetto dell'art. 21 del d.lgs. 8 aprile 2013, n. 39 "Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge n. 190 del 2012".

Detta disposizione stabilisce che - ai soli fini dell'applicazione del divieto di *pantouflage* di cui all'art. 53, co. 16-ter d.lgs. n. 165/2001 - sono considerati dipendenti delle pubbliche amministrazioni anche i soggetti titolari di uno degli incarichi del d.lgs. n. 39/2013, ivi compresi i soggetti esterni con i quali l'amministrazione, l'ente pubblico o l'ente di diritto privato in controllo pubblico stabilisce un rapporto di lavoro, subordinato o autonomo.

Pertanto, il divieto si applica non solo ai dipendenti delle pubbliche amministrazioni di cui all'art. 1, co. 2 del d.lgs. n. 165/2001, bensì anche a coloro che svolgono un incarico in enti pubblici e in enti di diritto privato in controllo pubblico, definizioni quest'ultime da rinvenirsi all'art. 1, co. 2, rispettivamente lett. b) e c) del d.lgs. n. 39/2013 citato.

Ai fini dell'applicazione del divieto di *pantouflage*, Difesa Servizi ha previsto che:

- nei bandi di gara o negli atti prodromici agli affidamenti, anche mediante procedura negoziata, sia inserita la condizione soggettiva di non aver concluso contratti di lavoro subordinato o autonomo

e comunque di non aver attribuito incarichi ad ex dipendenti che hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni nei loro confronti per il triennio successivo alla cessazione del rapporto;

- sia disposta l'esclusione dalle procedure di affidamento nei confronti dei soggetti per i quali sia emersa la situazione di cui al punto precedente.

## **4. IL PIANO TRIENNALE PER LA TRASPARENZA E L'INTEGRITÀ (PTTI)**

La società con l'adozione del PTTI, intende dare attuazione al principio della trasparenza dell'attività amministrativa, intesa come accessibilità alle informazioni sull'organizzazione e sull'operato della struttura, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

La trasparenza, nel rispetto delle disposizioni in materia di segreto d'ufficio e di protezione dei dati personali, rappresenta uno strumento essenziale per garantire il rispetto dei principi di imparzialità, di uguaglianza, di responsabilità, di efficacia, di efficienza e del buon andamento.

Il PTTI è funzionale a tre scopi:

1. sottoporre ad un controllo diffuso ogni fase del ciclo di gestione per consentirne il miglioramento;
2. assicurare la conoscenza dei servizi resi, delle loro caratteristiche qualitative e quantitative;
3. prevenire fenomeni corruttivi e promuovere l'integrità dell'operato.

### **4.1. Soggetti responsabili**

Il principale soggetto interessato, per nomina, alla formazione e attuazione del PTTI è il Responsabile della Trasparenza che, come già anticipato, per DIFESA SERVIZI coincide con la figura del Responsabile della prevenzione della corruzione.

A completa similitudine di quanto già illustrato in tema di corruzione, ciascun Capo Divisioni/Direzioni è responsabile del puntuale e costante aggiornamento dei dati e documenti che a qualsiasi titolo sono di competenza delle Divisioni/Direzioni a cui fanno capo.

Tali Referenti sono tenuti ad assolvere agli adempimenti dettati dalla normativa inerente la trasparenza e di tale attività dovranno informare il Responsabile della Trasparenza della Società.

Ogni Referente raccoglie i dati, ne aggiorna il contenuto e li trasmette al Responsabile che ne dispone la pubblicazione direttamente sul sito internet societario, in accordo con quanto richiesto dal Decreto n. 33/2013, di cui si riporta in allegato 5 il Programma Triennale per la Trasparenza e l'Integrità (PTTI) che contiene la "Tabella riepilogativa degli adempimenti" da soddisfare a termini di norma.

#### **4.1.1. Qualità delle informazioni e criteri generali**

I Referenti devono curare la qualità della pubblicazione affinché si possa accedere in modo agevole alle informazioni e si possa comprenderne il contenuto.

In particolare, i dati e i documenti devono essere pubblicati in aderenza alle seguenti caratteristiche:

- completi ed accurati: i dati devono corrispondere al fenomeno che si intende descrivere e, nel caso di dati tratti da documenti, devono essere pubblicati in modo esatto e senza omissioni;
- comprensibili: il contenuto dei dati deve essere esplicitato in modo chiaro ed evidente e pertanto, occorre:
  - a. evitare la frammentazione, cioè la pubblicazione di stesse tipologie di dati in punti diversi del sito, che impedisce e complica l'effettuazione di calcoli e comparazioni;
  - b. selezionare e elaborare i dati di natura tecnica (ad es. bilanci e dati finanziari) in modo che il significato sia chiaro ed accessibile anche per chi è privo di conoscenze specialistiche;
- aggiornati: ogni dato deve essere aggiornato tempestivamente, ove ricorra l'ipotesi;
- tempestivi: la pubblicazione deve avvenire in tempi tali da garantire l'utile fruizione da parte dell'utente;

– in formato aperto: le informazioni e i documenti devono essere pubblicati in formato aperto e raggiungibili direttamente dalla pagina dove le informazioni sono riportate.

Resta inteso sempre il necessario rispetto delle disposizioni in materia di protezione dei dati personali, sia nella fase di predisposizione degli atti sia nella fase della loro divulgazione e pubblicazione.

#### **4.2. Controllo e monitoraggio**

Alla corretta attuazione del PTII concorrono sia il Responsabile per la trasparenza della Società sia i referenti del Ministero della Difesa. In particolare il Responsabile Trasparenza per DIFESA SERVIZI svolge il controllo sull'attuazione del PTII e delle iniziative connesse, riferendo all'Amministratore Delegato su eventuali inadempimenti e ritardi.

A tal fine il Responsabile per la Trasparenza evidenzia e informa delle eventuali criticità i Responsabili, i quali dovranno provvedere a sanare le inadempienze entro e non oltre 30 giorni dalla segnalazione.

Decorso infruttuosamente tale termine, il Responsabile per la Trasparenza è tenuto a dare comunicazione all'Amministratore Delegato della mancata attuazione degli obblighi di pubblicazione.

#### **4.3. Tempi di attuazione degli obiettivi**

L'attuazione degli obiettivi previsti per il triennio si svolgerà entro le date previste nel presente programma, come di seguito indicato:

Anno 2025:

- Aggiornamento del Programma per la Trasparenza entro il 31 gennaio 2025;
- Realizzazione della Giornata della Trasparenza entro il 2025.

Anno 2026:

- Aggiornamento del Programma per la Trasparenza entro il 31 gennaio 2026;
- Realizzazione della Giornata della Trasparenza entro il 2026.

Anno 2027:

- Aggiornamento del Programma per la Trasparenza entro il 31 gennaio 2027;
- Realizzazione della Giornata della Trasparenza entro il 2027.

#### **4.4. Accesso civico**

##### **4.4.1 L'accesso civico "semplice"**

L'accesso civico, cosiddetto "semplice", è il diritto di chiunque di richiedere documenti, informazioni e dati della Società Difesa Servizi S.p.A. oggetto di pubblicazione obbligatoria, ai sensi della normativa vigente, nei casi in cui ne sia stata omessa la pubblicazione sul sito web della Società. Il diritto di accesso civico "semplice" è disciplinato dall'articolo 5 del d.lgs. n. 33/2013, come modificato dal d.lgs. n. 97/2016, e regolamentato dall'ANAC con Delibera n. 1310 del 28 dicembre 2016.

La richiesta di accesso civico "semplice" è gratuita e va presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza, al seguente indirizzo: [rpct@difesaservizi.it](mailto:rpct@difesaservizi.it), compilata nei modi previsti dalle vigenti norme in materia.

In caso di accoglimento, la Società entro 30 giorni procede all'inserimento sul sito web dei dati, delle informazioni o dei documenti richiesti e comunica al richiedente l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto nell'istanza presentata.

##### **4.4.2 L'accesso civico generalizzato, procedimentale o documentale**

Il diritto di accesso civico generalizzato (FOIA), disciplinato dagli articoli 5 e 5 bis del d.lgs. n. 33/2013, come modificato dal d.lgs. 97/2016, sancisce il diritto di chiunque di accedere ai dati e ai documenti, detenuti dalla stessa Società, ulteriori rispetto a quelli per i quali non sussista uno specifico obbligo di pubblicazione, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dal citato articolo 5-bis. L'ANAC ha regolamentato il diritto all'accesso civico generalizzato con Delibera n. 1309 del 28 dicembre 2016.

L'accesso procedimentale o documentale è uno strumento finalizzato a proteggere interessi giuridici particolari di soggetti che sono portatori di un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso. Tale accesso è disciplinato dalla Legge 241/1990 e s.m.i. e dal DPR 184/2006.

Le richieste di accesso civico generalizzato e accesso procedimentale (o documentale ex Legge 241/1990 e s.m.i.) devono essere indirizzate a [protocollo@pec.difesaservizi.it](mailto:protocollo@pec.difesaservizi.it) e dovranno recare nell'oggetto – per una veloce individuazione - la dizione “accesso civico generalizzato” o “accesso procedimentale”, compilate nei modi previsti dalle vigenti norme in materia. Per tali tipologie di Accessi, la trattazione ed il successivo riscontro rientra nella gestione dei flussi documentali e gestionali dell'organizzazione societaria. In particolare, per le richieste di accesso civico generalizzato, la trattazione è attribuita all'ufficio (Divisione/Direzione/Area) che detiene o possiede i dati o i documenti richiesti (rif. Delibera n. 1309 del 28 dicembre 2016 dell'ANAC e Circolare n. 2/2017 “Attuazione delle norme sull'accesso civico generalizzato - c.d. FOIA”, edita dal Dipartimento della Funzione Pubblica del Ministero per la Pubblica Amministrazione). Al riguardo, si specifica che, per l'accesso civico generalizzato, come previsto dalle norme vigenti in materia, Linee guida dell'ANAC e Circolare n. 2/2017 DFP, il RPCT riceve e tratta eventualmente le sole richieste di riesame in caso di diniego totale o parziale dell'accesso generalizzato o di mancata risposta, con delle valutazioni da porre in essere esaminando la fattispecie. Ad esempio, laddove l'accesso generalizzato sia stato negato o differito per motivi attinenti la protezione dei dati personali, il RPCT provvede eventualmente ad interessare anche il Garante per la protezione dei dati personali. Nel caso in cui una domanda di accesso generalizzato sia stata erroneamente inviata al RPCT, quest'ultimo provvede a inoltrare tempestivamente la stessa all'ufficio competente a decidere sulla domanda.

Il Titolare del potere sostitutivo in merito all'accesso civico è l'Amministratore Delegato della Società.

## **5. ADEGUAMENTI**

Il presente PTPC e PTI rappresentano lo strumento attraverso il quale sono individuate le strategie prioritarie per la prevenzione ed il contrasto della corruzione all'interno della Società Difesa Servizi.

Il PTPC non si configura come un'attività compiuta, con un termine di completamento finale, bensì come un insieme di strumenti finalizzati alla prevenzione che vengono via via affinati, modificati o sostituiti in relazione al *feedback* ottenuto dalla loro applicazione.

Pertanto, come già evidenziato in premessa ed attesa la configurazione evolutiva della società, il PTPC non può non integrarsi e richiamare il Modello di Organizzazione ex D. Lgs. 231/2001, così come approvato dal C.d.A.. In particolare, alle previsioni specifiche ivi contemplate, si aggiungono quelle presenti, in un'ottica complementare e globale di prevenzione non solo dei reati contro la P.A., ma di tutte le fattispecie illecite che possono incidere sul corretto andamento e sulla buona amministrazione. Infatti, la disciplina anticorruzione ha apportato profonde innovazioni per le imprese che intendano adeguarsi al sistema di prevenzione D. Lgs. 231/2001; non si tratterà, pertanto, con il presente Piano, semplicemente di introdurre nei modelli e nelle procedure le nuove figure delittuose, di aggiornare la mappatura dei rischi e costruire un adeguato sistema di controllo, quanto piuttosto di conformare l'intero sistema alla legge 190/2012 e dei decreti attuativi.

Ciò richiederà il continuo aggiornamento e la frequente ri-modulazione dei modelli contemplati, alle nuove realtà tramite un processo costante di controllo, ricognizione ed analisi periodica, avendo, infine, riguardo anche all'efficienza dell'attività preventiva con misure che non dovranno tradursi in un aggravio ingiustificato, ovvero in appesantimenti burocratici che lo spirito della legge tende a minimizzare, proprio al fine di scardinare i fenomeni corruttivi.