



DIGITAL SOLUTIONS

B E N E F I T

**Modello di organizzazione, gestione e controllo
ex Decreto Legislativo 231/2001**

PARTE GENERALE

SOMMARIO

DEFINIZIONI	4
CAPITOLO 1	8
IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DEGLI ENTI	8
1.1. Il Decreto e la normativa di riferimento.....	8
1.2. I Reati c.d. presupposto.....	8
1.3. L'apparato sanzionatorio previsto dal Decreto.	21
1.4. L'adozione del Modello quale possibile esimente dalla responsabilità amministrativa.	23
CAPITOLO 2	25
ADOZIONE DEL MODELLO DA PARTE DI DIGITAL SOLUTIONS	25
2.1. Adozione e aggiornamento del Modello e nomina dell'Organismo di Vigilanza.....	25
2.2. Le Linee Guida Confindustria e i " <i>Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza</i> ".	25
2.3. Le caratteristiche del Modello.....	27
2.4. Funzione e scopo del Modello.	28
2.5. Identificazione delle Aree a Rischio e delle Attività Sensibili: attività preliminare.	28
2.6. <i>As is e gap analysis</i>	29
2.7. Predisposizione del Modello.	29
2.7.1. Principi generali cui si ispira il Modello.	30
2.7.2. La procedura di adozione, modifica ed integrazione del Modello.	31
2.8. Destinatari del Modello.....	31
CAPITOLO 3	33
IL GRUPPO, LA SOCIETÀ ED ARCHITETTURA DEL SISTEMA NORMATIVO INTERNO	33
3.1. Il Gruppo PFM.	33
3.2. La Società.....	34
3.3. La <i>Corporate Governance</i> di Digital Solutions.....	35
3.4. Regole generali.....	37
3.4.1. Il sistema in linea generale.....	37
3.4.2. Il sistema di deleghe e procure.....	37
3.5. Il sistema di controlli interni e gestione dei rischi.	39
3.6. Descrizione delle Attività Sensibili e piano dei controlli.....	39
CAPITOLO 4	41
L'ORGANISMO DI VIGILANZA	41
4.1. Identificazione dell'Organismo di Vigilanza.	41
4.2. Durata in carica.	43
4.3. Funzione e poteri dell'Organismo di Vigilanza.	44
4.4. Poteri dell'Organismo di Vigilanza.	46
4.5. Regole di convocazione e di funzionamento.....	47
4.6. Flussi informativi dell'OdV verso gli Organi Sociali.	48
4.7. Flussi informativi nei confronti dell'Organismo di Vigilanza.	49
4.8. Modalità delle segnalazioni.....	50
4.9. Obblighi di riservatezza.	51
4.10. Gestione delle segnalazioni da parte dell'Organismo di Vigilanza.	52
4.11. <i>Whistleblowing</i> : la tutela del dipendente e/o del collaboratore che segnala illeciti.	53
CAPITOLO 5	54
LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO	54
5.1. Formazione ed informazione dei Dipendenti.....	54
5.1.1. La comunicazione iniziale.....	54
5.1.2. La formazione.	54
5.2. Informazione dei Consulenti, <i>Partner</i> e Fornitori.....	54
CAPITOLO 6	55

SISTEMA SANZIONATORIO.....	55
6.1. Funzione del sistema sanzionatorio.....	55
6.2. Dipendenti soggetti al CCNL - Sistema sanzionatorio.	55
6.3. Misure nei confronti dei dirigenti.	57
6.4. Misure nei confronti degli amministratori.	57
6.5. Misure nei confronti dei membri dell’OdV.....	57
6.6. Misure nei confronti dei Consulenti, <i>Partner</i> e Fornitori.	58
CAPITOLO 7.....	59
VERIFICHE SULL’ADEGUATEZZA DEL MODELLO.	59

Definizioni.

Oltre ai termini definiti altrove nel Modello (come *infra* definito), i seguenti termini con la lettera iniziale maiuscola avranno il significato indicato qui di seguito, se non altrimenti indicato, sia che vengano utilizzati nella forma singolare o plurale e viceversa.

- i) “**ANAC**”: indica l’Autorità Nazionale Anticorruzione.
- ii) “**Amministratore Delegato**”: indica l’amministratore delegato nominato da Digital Solutions.
- iii) “**Area a Rischio**”: indica l’area in cui sono identificabili le attività e/o operazioni di Digital Solutions nel cui ambito sussiste il rischio di commissione dei Reati.
- iv) “**ASPP**” o “**Addetti al Servizio di Prevenzione e Protezione**”: indicano i soggetti in possesso della capacità e dei requisiti professionali di cui all’articolo 32 del Testo Unico Sicurezza designati per l’espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.
- v) “**Assemblea**”: indica l’assemblea dei soci di Digital Solutions.
- vi) “**Attività Sensibili**”: indica le attività e/o operazioni di Digital Solutions nel cui ambito sussiste il rischio di commissione dei Reati.
- vii) “**BS – OHSAS 18001**” o “**British Standard**”: indicano il *British Standard* OHSAS 18001:2007, a cui la Società si è ispirata per la predisposizione della Parte Speciale.
- viii) “**Capogruppo**”: indica PFM Sintesi S.r.l. Società *Benefit*, con sede legale in Milano (MI), via Enrico Toti n. 4, codice fiscale, partita IVA e numero di iscrizione al Registro delle Imprese di Milano Monza-Brianza Lodi 08042690969.
- ix) “**CCNL**”: indica il Contratto Collettivo Nazionale di Lavoro (contratto per i per i dipendenti da aziende del Terziario della Distribuzione e dei Servizi) attualmente in vigore ed applicato da Digital Solutions.
- x) “**Codice Etico**”: indica il codice etico adottato da Digital Solutions.
- xi) “**Consiglio di Amministrazione**”: indica il consiglio di amministrazione di Digital Solutions.
- xii) “**Consulenti**”: indica coloro che agiscono in nome e/o per conto di DS sulla base di un mandato ovvero coloro che collaborano con la Società in forza di un contratto di collaborazione di qualsiasi natura.
- xiii) “**D.Lgs. 74/2000**” indica il decreto legislativo 10 marzo 2000, n. 74 e successive modificazioni e integrazioni, recante la “*Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto*”.
- xiv) “**Datore di Lavoro**”: indica il soggetto titolare del rapporto di lavoro con il Lavoratore o, comunque, il soggetto che, secondo il tipo e l’assetto dell’organizzazione nel cui ambito il Lavoratore presta la propria attività, ha la responsabilità, in virtù di apposita delega, dell’organizzazione stessa o del singolo settore in quanto esercita i poteri decisionali e di spesa.

- xv) “**Delegato Sicurezza**”: indica il dirigente *ex* articolo 18 del Testo Unico Sicurezza ai quali il Datore di Lavoro può delegare, ai sensi dell’articolo 16 del medesimo Testo Unico Sicurezza, funzioni di responsabilità relative alla salute e sicurezza sul lavoro eventualmente nominati all’interno della Società.
- xvi) “**Destinatari**”: indica tutti coloro ai quali si rivolge il Modello, compresi gli Organi Sociali, i Dipendenti, i Consulenti, i Fornitori e i *Partner*.
- xvii) “**Digital Solutions**” o “**DS**” o “**Società**”: indicano Digital Solutions S.r.l. Società *Benefit*, con sede legale in Milano (MI) - Via Enrico Toti n. 4, capitale sociale Euro 300.000,00 i.v., codice fiscale, partita IVA e numero iscrizione al Registro delle Imprese di Milano Monza-Brianza Lodi 12985480156, iscritta al numero REA: MI-1606714, soggetta all’attività di direzione e coordinamento di PFM Sintesi S.r.l. Società *Benefit*.
- xviii) “**Dipendenti**”: indica tutti i dipendenti di Digital Solutions (compresi eventuali dirigenti).
- xix) “**D.Lgs. 231/2001**” o “**Decreto**”: indica il decreto legislativo 8 giugno 2001, numero 231, e successive modifiche ed integrazioni.
- xx) “**DUVRI**” o “**Documento Unico di Valutazione dei Rischi per le Interferenze**”: indicano il documento redatto dal Datore di Lavoro committente contenente una valutazione dei rischi e le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze.
- xxi) “**DVR**” o “**Documento di Valutazione dei Rischi**”: indicano il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l’attività lavorativa ed i criteri per la suddetta valutazione, l’indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito di tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l’individuazione delle procedure per l’attuazione delle misure da realizzare nonché dei ruoli dell’organizzazione aziendale che vi debbono provvedere, l’indicazione dei nominativi di RSPP, RLS e del Medico Competente che ha partecipato alla valutazione del rischio, nonché l’individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento.
- xxii) “**Enti**”: indicano le persone giuridiche, le società e le associazioni anche prive di personalità giuridica la cui responsabilità amministrativa è prevista dal Decreto.
- xxiii) “**Fornitori**”: indicano i fornitori di beni e servizi della Società, professionali e no, inclusi quelli di natura finanziaria.
- xxiv) “**Gruppo 231**”: indicano le società del Gruppo PFM che hanno adottato (o che adotteranno) un proprio modello di organizzazione, gestione e controllo ai sensi del Decreto.
- xxv) “**Gruppo PFM**”: indica il gruppo di società a cui appartiene anche DS.
- xxvi) “**Lavoratore**”: indica la persona che, indipendentemente dalla tipologia contrattuale, svolge un’attività lavorativa nell’ambito dell’organizzazione della Società con o senza retribuzione anche al fine di intraprendere un mestiere.

- xxvii) “**Linee Guida Confindustria**”: indica le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex Decreto approvate da Confindustria in data 7 marzo 2002 e successivi aggiornamenti.
- xxviii) “**Linee Guida Uni-Inail**”: indica le linee guida elaborate dall’UNI e dall’INAIL per la costituzione volontaria da parte delle imprese di un sistema di gestione della salute e sicurezza sul lavoro del 28 settembre 2001.
- xxix) “**Medico Competente**”: indica il medico in possesso di uno dei titoli e dei requisiti formali e professionali indicati nel Testo Unico Sicurezza, che collabora con il Datore di Lavoro della Società ai fini della valutazione dei rischi e dell’esecuzione della Sorveglianza Sanitaria e dell’adempimento di tutti gli altri compiti di cui al Testo Unico Sicurezza.
- xxx) “**Modello**”: indica il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001 e adottato dalla Società, comprensivo, tra l’altro, di Parte Generale, Parte Speciale e le relative procedure.
- xxxi) “**Normativa Privacy**”: indica tutta la normativa in materia di protezione dei dati personali, comprensiva del decreto legislativo 30 giugno 2003, numero 196, e successive modifiche e integrazioni, del Regolamento UE n. 679/2016 (c.d. “GDPR”), del decreto legislativo 18 maggio 2018, numero 51, e successive modificazioni e integrazioni.
- xxxii) “**Organi Sociali**”: indica l’Assemblea e il Consiglio di Amministrazione di Digital Solutions.
- xxxiii) “**Organismo di Vigilanza**” o “**OdV**”: indicano l’organismo interno preposto alla vigilanza sul funzionamento e sull’osservanza del Modello e al relativo aggiornamento.
- xxxiv) “**P.A.**” o “**Pubblica Amministrazione**”: indicano la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio.
- xxxv) “**Parte Generale**”: indica la parte generale del Modello adottato da DS;
- xxxvi) “**Parte Speciale**”: indica la parte speciale del Modello adottato da DS;
- xxxvii) “**Partner**”: indica le controparti contrattuali di Digital Solutions, sia persone fisiche sia persone giuridiche, con cui la Società addivenga ad una qualunque forma di rapporto di collaborazione contrattualmente regolato (ad esempio, associazione temporanea d’impresa - ATI, *joint venture*, consorzi, eccetera), ove destinati a cooperare con la Società nell’ambito delle Attività Sensibili.
- xxxviii) “**Preposto**”: indica il soggetto e/o i soggetti individuato/i dal Datore di Lavoro, ai sensi dell’articolo 18 del Testo Unico Sicurezza, per l’effettuazione delle attività di vigilanza di cui all’articolo 19 del D.Lgs. 81/2008 in materia di salute e sicurezza dei Lavoratori.
- xxxix) “**Presidente**”: indica il presidente del Consiglio di Amministrazione.
- xl) “**Principi**”: indica i “*Principi consolidati per la redazione dei modelli organizzativi e l’attività dell’organismo di vigilanza e prospettive di revisione del D.lgs. 8 giugno 2001, n. 231*” elaborati di concerto dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, dall’Associazione Bancaria Italiana, dal Consiglio Nazionale Forense e da Confindustria.

- xli) “**Reati**”: indica i reati ai quali si applica la disciplina prevista dal D.Lgs. 231/2001.
- xlii) “**Responsabile dell’Impatto**”: indica il responsabile dell’impatto nominato dalla Società ai sensi della legge 28 dicembre 2015, n. 208, articolo 1, comma 380.
- xliii) “**RLS**” o “**Rappresentante dei Lavoratori per la Sicurezza**”: indicano il soggetto eletto o designato per rappresentare i Lavoratori in relazione agli aspetti della salute e sicurezza durante il lavoro.
- xliv) “**RSPP**” o “**Responsabile del Servizio di Prevenzione e Protezione**”: indicano il soggetto in possesso delle capacità e dei requisiti professionali indicati nel Testo Unico Sicurezza, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione dai rischi.
- xlv) “**Sorveglianza Sanitaria**”: indica l’insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei Lavoratori in relazione all’ambiente di lavoro, ai fattori di rischio professionale, ed alle modalità di svolgimento dell’attività lavorativa.
- xlvi) “**SPP**” o “**Servizio di Prevenzione e Protezione**”: indicano l’insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all’attività di prevenzione e protezione dai rischi professionali per i Lavoratori.
- xlvii) “**SSL**”: indica la salute e la sicurezza dei Lavoratori.
- xlviii) “**Statuto dei Lavoratori**”, indica la legge 20 maggio 1970, n. 300 e successive modificazioni e integrazioni.
- xlix) “**Testo Unico Doganale**”: indica il decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, e successive modificazioni e integrazioni recante le disposizioni legislative in materia doganale;
- l) “**Testo Unico dell’Immigrazione**”: indica il decreto legislativo 25 luglio 1998, n. 286 e successive modificazioni ed integrazioni, concernenti la disciplina dell’immigrazione e norme sulla condizione dello straniero;
- li) “**Testo Unico Sicurezza**”: indica il decreto legislativo 9 aprile 2008, n. 81, e successive modificazioni e integrazioni, di “*Attuazione dell’articolo 1 della Legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*”;
- lii) “**TUF**”: indica il decreto legislativo 24 febbraio 1998, n. 58 recante il “*Testo unico delle disposizioni in materia di intermediazione finanziaria*” e successive modificazioni ed integrazioni.

CAPITOLO 1.

Il regime di responsabilità amministrativa previsto a carico degli Enti.

1.1. Il Decreto e la normativa di riferimento.

Il decreto legislativo 8 giugno 2001, numero 231, recante la “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*” – pubblicato in Gazzetta Ufficiale numero 140, del 13 giugno 2001, Serie Generale, entrato in vigore in data 4 luglio 2001, in parziale attuazione della delega di cui all’articolo 11 della legge 29 settembre 2000 n. 300, disciplina – introducendola per la prima volta nell’ordinamento giuridico nazionale – la responsabilità amministrativa degli Enti.

Il Decreto ha inteso adeguare l’ordinamento giuridico interno in materia di persone giuridiche ad alcune convenzioni internazionali tra cui:

- i) la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- ii) la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri;
- iii) la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

L’articolo 5 del Decreto sancisce la responsabilità dell’Ente qualora determinati Reati (reati c.d. presupposto) siano stati commessi nel suo interesse o a suo vantaggio:

- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo della stessa (ad esempio, amministratori e direttori generali);
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla lettera precedente (ad esempio, dipendenti non dirigenti).

Pertanto, il Decreto sancisce un’estensione della responsabilità derivante dalla commissione di alcuni illeciti penali, oltre alla persona fisica che ha materialmente commesso il fatto, agli Enti che hanno tratto vantaggio dalla commissione dell’illecito o nel cui interesse l’illecito è stato commesso. Il “vantaggio” e l’“interesse” rappresentano due distinti criteri di imputazione della responsabilità, potendo l’Ente essere responsabile per il sol fatto che l’illecito venga commesso nel suo interesse, a prescindere dal conseguimento o meno di un concreto vantaggio.

La responsabilità prevista dal Decreto si configura anche in relazione ai Reati commessi all’estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il Reato medesimo.

1.2. I Reati c.d. presupposto.

I Reati c.d. presupposto, dal cui compimento è fatta derivare la responsabilità amministrativa dell'Ente, sono quelli espressamente e tassativamente richiamati dal Decreto e successive modifiche e integrazioni.

Ad oggi i Reati c.d. presupposto risultano essere i seguenti.

A. REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE
(articoli 24 e 25 del Decreto):

- i) peculato (articoli 314, comma 1, e 316 del codice penale);
- ii) malversazione di erogazioni pubbliche (articolo 316-*bis* del codice penale);¹
- iii) indebita percezione di erogazioni pubbliche (articolo 316-*ter* del codice penale);²
- iv) concussione (articolo 317 del codice penale)³;
- v) corruzione per l'esercizio della funzione (articolo 318 del codice penale)⁴;
- vi) corruzione per un atto contrario ai doveri di ufficio (articoli 319 e 319-*bis* del codice penale);
- vii) corruzione in atti giudiziari (articolo 319-*ter*, comma 1, del codice penale);
- viii) induzione indebita a dare o promettere utilità (articolo 319-*quater* del codice penale)⁵;
- ix) corruzione di persona incaricata di un pubblico servizio (articolo 320 del codice penale)⁶;
- x) pene per il corruttore (articolo 321 del codice penale);
- xi) istigazione alla corruzione (articolo 322 del codice penale)⁷;
- xii) peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri, abuso di ufficio (articolo 322-*bis* del codice penale);
- xiii) abuso d'ufficio (articolo 323 del codice penale);
- xiv) traffico di influenze illecite (articolo 346-*bis* del codice penale);

¹ Così come modificato dal decreto-legge 25 febbraio 2022, n. 13, recante le “*Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili*” (c.d. Decreto frodi).

² Così come modificato dal decreto-legge 25 febbraio 2022, n. 13, recante le “*Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili*” (c.d. Decreto frodi).

³ Così come modificato dalla legge 6 novembre 2012, n. 190, “*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*”, in vigore dal 28 novembre 2012.

⁴ Così come modificato dalla legge 6 novembre 2012, n. 190.

⁵ Reato introdotto dalla legge 6 novembre 2012, n. 190.

⁶ Così come modificato dalla legge 6 novembre 2012, n. 190.

⁷ Così come modificato dalla legge 6 novembre 2012, n. 190.

- xv) turbata libertà degli incanti (articolo 353 del codice penale)⁸;
- xvi) turbata libertà del procedimento di scelta del contraente (articolo 353-*bis* del codice penale)⁹;
- xvii) frode nelle pubbliche forniture (articolo 356 del codice penale);
- xviii) truffa a danno dello Stato o di un altro ente pubblico o dell'Unione Europea o col pretesto di far esonerare taluno dal servizio militare (articolo 640, comma 2, numero 1 del codice penale);
- xix) truffa aggravata per il conseguimento di erogazioni pubbliche (articolo 640-*bis* del codice penale)¹⁰;
- xx) frode informatica (articolo 640-*ter* del codice penale);
- xxi) esposizione di dati o notizie falsi per conseguire indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (articolo 2 della legge 23 dicembre 1986, numero 898).

B. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (articolo 24-*bis* del Decreto):

- i) falsità in un documento informatico pubblico (articolo 491-*bis* del codice penale)¹¹;
- ii) accesso abusivo ad un sistema informatico o telematico (articolo 615-*ter* del codice penale);
- iii) detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (articolo 615-*quater* del codice penale);¹²
- iv) detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (articolo 615-*quinquies* del codice penale);¹³
- v) intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (articolo 617-*quater* del codice penale);
- vi) detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad

⁸ Così come modificato dal decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137.

⁹ Così come modificato dal decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137.

¹⁰ Così come modificato dal decreto-legge 25 febbraio 2022, n. 13, recante le "Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili" (c.d. Decreto frodi).

¹¹ Così modificato dal decreto legislativo 15 gennaio 2016, n. 7.

¹² Così come modificato dall'articolo 19 della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione.

¹³ Così come modificato dall'articolo 19 della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione.

intercettare, impedire o interrompere comunicazioni informatiche o telematiche (articolo 617-*quinquies* del codice penale)¹⁴;

- vii) danneggiamento di informazioni, dati e programmi informatici (articolo 635-*bis* del codice penale);
- viii) danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (articolo 635-*ter* del codice penale);
- ix) danneggiamento di sistemi informatici o telematici (articolo 635-*quater* del codice penale);
- x) danneggiamento di sistemi informatici o telematici di pubblica utilità (articolo 635-*quinquies* del codice penale);
- xi) frode informatica del soggetto che presta servizi di certificazione di firma elettronica (articolo 640-*quinquies* del codice penale);
- xii) delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105 (perimetro di sicurezza nazionale cibernetica)¹⁵.

C. DELITTI DI CRIMINALITÀ ORGANIZZATA (articolo 24-*ter* del Decreto):

- i) associazione per delinquere (articolo 416 del codice penale);
- ii) associazioni di tipo mafioso anche straniere (articolo 416-*bis* del codice penale);
- iii) scambio elettorale politico-mafioso (articolo 416-*ter* del codice penale);
- iv) sequestro di persona a scopo di estorsione (articolo 630 del codice penale);
- v) produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope (articolo 73 del D.P.R. 9 ottobre 1990, n. 309);
- vi) associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (articolo 74 del D.P.R. 9 ottobre 1990, n. 309);
- vii) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma 3, della legge 18 aprile 1975, n. 110 (articolo 407, 2 comma, lettera a), numero 5 del codice di procedura penale).

¹⁴ Così come modificato dall'articolo 19 della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione.

¹⁵ Introdotta dall'articolo 1, comma 1, del decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133.

D. REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO E IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (articolo 25-*bis* del Decreto):

- i) falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (articolo 453 del codice penale);
- ii) alterazione di monete (articolo 454 del codice penale);
- iii) spendita e introduzione nello Stato, senza concerto, di monete falsificate (articolo 455 del codice penale);
- iv) spendita di monete falsificate ricevute in buona fede (articolo 457 del codice penale);
- v) falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (articolo 459 del codice penale);
- vi) contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (articolo 460 del codice penale);
- vii) fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (articolo 461 del codice penale);
- viii) uso di valori di bollo contraffatti o alterati (articolo 464 del codice penale);
- ix) contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (articolo 473 del codice penale);
- x) introduzione nello Stato e commercio di prodotti con segni falsi (articolo 474 del codice penale).

E. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (articolo 25-*bis.1* del Decreto):

- i) turbata libertà dell'industria o del commercio (articolo 513 del codice penale);
- ii) illecita concorrenza con minaccia o violenza (articolo 513-*bis* del codice penale);
- iii) frodi contro le industrie nazionali (articolo 514 del codice penale);
- iv) frode nell'esercizio del commercio (articolo 515 del codice penale);
- v) vendita di sostanze alimentari non genuine come genuine (articolo 516 del codice penale);
- vi) vendita di prodotti industriali con segni mendaci (articolo 517 del codice penale);
- vii) fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (articolo 517-*ter* del codice penale);
- viii) contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti

agroalimentari (articolo 517-*quater* del codice penale).

F. REATI SOCIETARI (articolo 25-*ter* del Decreto):

- i) false comunicazioni sociali (articolo 2621 del codice civile);
- ii) fatti di lieve entità (articolo 2621-*bis* del codice civile);
- iii) false comunicazioni sociali delle società quotate (articolo 2622 del codice civile);
- iv) impedito controllo (articolo 2625 del codice civile);
- v) indebita restituzione dei conferimenti (articolo 2626 del codice civile);
- vi) illegale ripartizione degli utili e delle riserve (articolo 2627 del codice civile);
- vii) illecite operazioni sulle azioni o quote sociali o della società controllante (articolo 2628 del codice civile);
- viii) operazioni in pregiudizio dei creditori (articolo 2629 del codice civile);
- ix) omessa comunicazione del conflitto di interessi (articolo 2629-*bis* del codice civile);
- x) formazione fittizia del capitale (articolo 2632 del codice civile);
- xi) indebita ripartizione dei beni sociali da parte dei liquidatori (articolo 2633 del codice civile);
- xii) corruzione fra privati (articolo 2635 del codice civile)¹⁶;
- xiii) istigazione alla corruzione tra privati (articolo 2635-*bis* del codice civile)¹⁷;
- xiv) illecita influenza sull'assemblea (articolo 2636 del codice civile);
- xv) aggio (articolo 2637 del codice civile);
- xvi) ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (articolo 2638 del codice civile).

G. DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (articolo 25-*quater* del Decreto):

Si tratta di reati previsti dal codice penale aventi finalità terroristiche o eversive nonché di delitti posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo sottoscritta a New York in data 9 dicembre 1999. In particolare:

¹⁶ Introdotta dalla legge 6 novembre 2012, n. 190, in vigore dal 28 novembre 2012.

¹⁷ Introdotta dall'articolo 4 del decreto legislativo 15 marzo 2017, n. 38.

- i) associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (articolo 270-*bis* del codice penale);
- ii) assistenza agli associati (articolo 270-*ter* del codice penale);
- iii) arruolamento con finalità di terrorismo anche internazionale (articolo 270-*quater* del codice penale);
- iv) organizzazione di trasferimenti per finalità di terrorismo (articolo 270-*quater*.1 del codice penale);
- v) addestramento ad attività con finalità di terrorismo anche internazionale (articolo 270-*quinquies* del codice penale);
- vi) condotte con finalità di terrorismo (articolo 270-*sexies* del codice penale);
- vii) attentato per finalità terroristiche o di eversione (articolo 280 del codice penale);
- viii) atto di terrorismo con ordigni micidiali o esplosivi (articolo 280-*bis* del codice penale);
- ix) sequestro di persona a scopo di terrorismo o di eversione (articolo 289-*bis* del codice penale).

H. REATO DI PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (articolo 25-*quater*.1 del Decreto):

- i) pratiche di mutilazione degli organi genitali femminili (articolo 583-*bis* del codice penale).

I. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE (articolo 25-*quinquies* del Decreto):

- i) riduzione o mantenimento in schiavitù o in servitù (articolo 600 del codice penale);
- ii) prostituzione minorile (articolo 600-*bis* del codice penale);
- iii) pornografia minorile (articolo 600-*ter* del codice penale);
- iv) detenzione o di accesso a materiale pornografico (articolo 600-*quater* del codice penale);¹⁸
- v) pornografia virtuale (articolo 600-*quater*.1 del codice penale);
- vi) iniziative turistiche volte allo sfruttamento della prostituzione minorile (articolo 600-*quinquies* del codice penale);
- vii) tratta di persone (articolo 601 del codice penale);

¹⁸ Così come modificato dall'articolo 20, comma 1, lettera a) della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

- viii) acquisto e alienazione di schiavi (articolo 602 del codice penale);
- ix) intermediazione illecita e sfruttamento del lavoro (articolo 603-*bis* del codice penale);
- x) violenza sessuale (articolo 609-*bis* del codice penale);
- xi) atti sessuali con minorenne (articolo 609-*quater* del codice penale);
- xii) corruzione di minorenne (articolo 609-*quinqies* del codice penale);
- xiii) violenza sessuale di gruppo (articolo 609-*octies* del codice penale);
- xiv) adescamento di minorenni (articolo 609-*undecies* del codice penale).¹⁹

J. ABUSI DI MERCATO (articolo 25-*sexies* del Decreto):

i) Reati:

- a) abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (articolo 184 del TUF);²⁰
- b) manipolazione del mercato (articolo 185 del TUF).

ii) Illeciti amministrativi (*ex* articolo 187-*bis* del TUF):

- a) abuso e comunicazione illecita di informazioni privilegiate (articolo 187-*bis* del TUF);
- b) manipolazione del mercato (articolo 187-*ter* del TUF).

K. REATI TRANSNAZIONALI (articolo 10 della legge 16 marzo 2006, n. 146):

- i) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377-*bis* del codice penale);
- ii) favoreggiamento personale (articolo 378 del codice penale);
- iii) associazione per delinquere (articolo 416 del codice penale);
- iv) associazione di tipo mafioso anche straniera (articolo 416-*bis* del codice penale);
- v) associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (articolo 74 del D.P.R. 9 ottobre 1990, n. 309);

¹⁹ Modificato dall'articolo 20, comma 1, lettera a) della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

²⁰ Così come modificato dall'articolo 26, comma 1, lettera c) della legge 23 dicembre 2021, n. 238, entrata in vigore il 1° febbraio 2022, per l'adeguamento alla direttiva n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile.

- vi) associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (articolo 291-*quater* del Testo Unico Doganale);
- vii) disposizioni contro le immigrazioni clandestine (articolo 12 commi 3, 3-*bis*, 3-*ter* e 5 del Testo Unico dell'Immigrazione).

L. REATI DI OMICIDIO COLPOSO O DI LESIONI GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO (articolo 25-*septies* del Decreto):

- i) omicidio colposo (articolo 589 del codice penale);
- ii) lesioni personali colpose (articolo 590 del codice penale).

M. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ AUTORICICLAGGIO (articolo 25-*octies* del Decreto):

- i) ricettazione (articolo 648 del codice penale);²¹
- ii) riciclaggio (articolo 648-*bis* del codice penale);²²
- iii) impiego di denaro, beni o utilità di provenienza illecita (articolo 648-*ter* del codice penale);²³
- iv) auto-riciclaggio (articolo 648-*ter*.1 del codice penale).²⁴

N. DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI (articolo 25-*octies*.1 del Decreto)²⁵:

- i) indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (articolo 493-*ter* del codice penale);
- ii) detenzione e diffusione di apparecchiature, dispositivi, programmi informatico diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (articolo 493-*quater* del codice penale);
- iii) trasferimento fraudolento di valori (articolo 512-*bis* del codice penale)²⁶;
- iv) frode informatica (articolo 640-*ter* del codice penale).

²¹ Così come modificato dal decreto legislativo 8 novembre 2021, n. 195 entrato in vigore in data 15 dicembre 2021, in attuazione della direttiva (UE) 2018/1673 del Parlamento Europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale.

²² Così come modificato dal decreto legislativo 8 novembre 2021, n. 195 (cfr. nota 17).

²³ Così come modificato dal decreto legislativo 8 novembre 2021, n. 195 (cfr. nota 17).

²⁴ Così come modificato dal decreto legislativo 8 novembre 2021, n. 195 (cfr. nota 17).

²⁵ Introdotto dall'articolo 3, comma 1, lettera a, del decreto legislativo 8 novembre 2021, n. 184, entrato in vigore dal 14 dicembre 2021, in attuazione della direttiva UE 2019/713 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

²⁶ Così come modificato dal decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137.

O. REATI IN MATERIA DI VIOLAZIONI DEL DIRITTO D'AUTORE (articolo 25-*novies* del Decreto):

- i) protezione del diritto d'autore e di altri diritti connessi al suo esercizio (articolo 171, comma 1, lettera a-*bis*), e comma 3 della legge 22 aprile 1941, n. 633);
- ii) protezione del diritto d'autore e di altri diritti connessi al suo esercizio (articolo 171-*bis* della legge 22 aprile 1941, n. 633);
- iii) protezione del diritto d'autore e di altri diritti connessi al suo esercizio (articolo 171-*ter* della legge 22 aprile 1941, n. 633);
- iv) protezione del diritto d'autore e di altri diritti connessi al suo esercizio articolo 171-*septies* della legge 22 aprile 1941, n. 633);
- v) protezione del diritto d'autore e di altri diritti connessi al suo esercizio articolo 171-*octies* della legge 22 aprile 1941, n. 633);
- vi) protezione del diritto d'autore e di altri diritti connessi al suo esercizio (articolo 174-*quinquies* della legge 22 aprile 1941, n. 633).

P. REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (articolo 25-*decies* del Decreto):

- i) induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 377-*bis* del codice penale).

Q. REATI AMBIENTALI (articolo 25-*undecies* del Decreto):

Si tratta di reati previsti dal codice penale e da leggi speciali. Segnatamente, in relazione alla commissione dei reati previsti dal codice penale:

- i) inquinamento ambientale (articolo 452-*bis*);
- ii) disastro ambientale (articolo 452-*quater*);
- iii) delitti colposi contro l'ambiente (articolo 452-*quinquies*);
- iv) traffico e abbandono di materiale ad alta radioattività (articolo 452-*sexies*);
- v) circostanze aggravanti (articolo 452-*quaterdecies*);
- vi) uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (articolo 727-*bis*)²⁷;
- vii) distruzione o deterioramento di *habitat* all'interno di un sito protetto (articolo 733-

²⁷ Come modificato dall'articolo 1 del decreto legislativo 7 luglio 2011, n. 121.

bis)²⁸;

Con riferimento ai reati previsti dal decreto legislativo 3 aprile 2006, n. 152, “*Norme in materia ambientale – Sanzioni penali*”:

- i) scarichi sul suolo (articolo 103);
- ii) scarichi nel sottosuolo e nelle acque sotterranee (articolo 104);
- iii) scarichi in reti fognarie (articolo 107);
- iv) scarichi di sostanze pericolose (articolo 108);
- v) attività di gestione di rifiuti non autorizzata (articolo 256)²⁹;
- vi) bonifica dei siti (articolo 257);
- vii) violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (articolo 258)³⁰;
- viii) traffico illecito di rifiuti (articolo 259);
- ix) sistema informatico di controllo della tracciabilità dei rifiuti (articolo 260-*bis*, commi 6, 7 e 8);
- x) reati in materia di emissioni (articolo 279, comma 5);
- xi) sanzioni penali in materia di scarichi di acque reflue industriali (articolo 137).

In relazione alla commissione dei reati previsti dalla legge 7 febbraio 1992, n. 150, “*Disciplina dei reati relativi all’applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione, nonché norme per la commercializzazione e la detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l’incolumità pubblica*”:

- i) importazione, esportazione o riesportazione, vendita, detenzione ai fini di vendita, trasporto eccetera in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate nell’allegato A del Regolamento medesimo e successive modificazioni (articolo 1 commi 1 e 2);
- ii) importazione, esportazione o riesportazione di esemplari, sotto qualsiasi regime doganale, senza il prescritto certificato o licenza (eccetera) in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate

²⁸ Come modificato dall’articolo 1 del decreto legislativo 7 luglio 2011, n. 121.

²⁹ Così come modificato dal decreto legislativo 8 novembre 2021, n. 196, in attuazione della direttiva (UE) 2019/904, del Parlamento Europeo e del Consiglio del 5 giugno 2019 sulla riduzione dell’incidenza di determinati prodotti di plastica sull’ambiente.

³⁰ Così come modificato dal decreto-legge 31 maggio 2021, n. 77 (“*Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure*”), convertito con modificazioni dalla legge 29 luglio 2021, n. 108.

negli allegati B e C del Regolamento medesimo e successive modificazioni e salvo che il fatto costituisca più grave reato (articolo 2, commi 1 e 2);

- iii) detenzione di esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica, salvo quanto previsto dalla legge 7 febbraio 1992, n. 150 (articolo 6);
- iv) falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati (reati del codice penale richiamati dall'articolo 3-bis).

In relazione alla commissione dei reati previsti dal decreto legislativo 6 novembre 2007, n. 202, "Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni":

- i) inquinamento colposo (articolo 9);
- ii) inquinamento doloso (articolo 8).

R. DELITTO DI IMPIEGO DI CITTADINI DI STATI TERZI IL CUI SOGGIORNO È IRREGOLARE (articolo 25-duodecies del Decreto):

- i) disposizioni contro le immigrazioni clandestine (articolo 12 del Testo Unico dell'Immigrazione);
- ii) impiego di cittadini di Stati terzi il cui soggiorno è irregolare (articolo 22 del Testo Unico dell'Immigrazione).

S. DELITTI LEGATI AL RAZZISMO E XENOFOBIA (articolo 25-terdecies del Decreto):

- i) propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (articolo 604-bis del codice penale e articolo 3, comma 3-bis, della legge 13 ottobre 1975, n. 654).

T. REATI DI FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (articolo 25-quaterdecies del Decreto):

- i) frode in competizioni sportive (articolo 1 della legge 13 dicembre 1989, n. 401);
- ii) esercizio abusivo di attività di giuoco o scommessa (articolo 4 della legge 13 dicembre 1989, n. 401).

U. REATI TRIBUTARI (articolo 25-quinquiesdecies del Decreto):

- i) dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (articoli 2 e 2 bis del D.Lgs. 74/2000, cui si riferiscono anche i successivi rimandi);

- ii) dichiarazione fraudolenta mediante altri artifici (articolo 3);
- iii) dichiarazione infedele (articolo 4);
- iv) omessa dichiarazione (articolo 5);
- v) emissione di fatture o altri documenti per operazioni inesistenti (articolo 8);
- vi) occultamento o distruzione di documenti contabili (articolo 10);
- vii) indebita compensazione (articolo 10-*quater*);
- viii) sottrazione fraudolenta al pagamento delle imposte (articolo 11).

V. CONTRABBANDO (articolo 25-*sexiesdecies* del Decreto):

Si tratta dei reati previsti dal Testo Unico Doganale:

- i) contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (articolo 282);
- ii) contrabbando nel movimento delle merci nei laghi di confine (articolo 283);
- iii) contrabbando nel movimento marittimo delle merci (articolo 284);
- iv) contrabbando nel movimento delle merci per via aerea (articolo 285);
- v) contrabbando nelle zone extra-doganali (articolo 286);
- vi) contrabbando per indebito uso di merci importate con agevolazioni doganali (articolo 287);
- vii) contrabbando nei depositi doganali (articolo 288);
- viii) contrabbando nel cabotaggio e nella circolazione (articolo 289);
- ix) contrabbando nell'esportazione di merci ammesse a restituzione di diritti (articolo 290);
- x) contrabbando nell'importazione od esportazione temporanea (articolo 291);
- xi) contrabbando di tabacchi lavorati esteri e circostanze aggravanti (articoli 291-*bis* e 291-*ter*);
- xii) associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (articolo 291-*quater*);
- xiii) altri casi di contrabbando (articolo 292).

W. DELITTI CONTRO IL PATRIMONIO CULTURALE (articolo 25-*septiesdecies* del Decreto)³¹:

- i) furto di beni culturali (articolo 518-*bis* del codice penale);
- ii) appropriazione indebita di beni culturali (articolo 518-*ter* del codice penale);
- iii) ricettazione di beni culturali (articolo 518-*quater* del codice penale);
- iv) falsificazione in scrittura privata relativa a beni culturali (articolo 518-*octies* del codice penale);
- v) violazioni in materia di alienazione di beni culturali (articolo 518-*novies* del codice penale);
- vi) importazione illecita di beni culturali (articolo 518-*decies* del codice penale);
- vii) uscita o esportazione illecite di beni culturali (articolo 518-*undecies* del codice penale);
- viii) distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (articolo 518-*duodecies* del codice penale);
- ix) contraffazione di opere d'arte (articolo 518-*quaterdecies* del codice penale).

X. RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI (articolo 25-*duodevicies* del Decreto)³²:

- i) riciclaggio di beni culturali (articolo 518-*sexies* del codice penale);
- ii) devastazione e saccheggio di beni culturali e paesaggistici (articolo 518-*terdecies* del codice penale).

1.3. L'apparato sanzionatorio previsto dal Decreto.

Sotto il profilo sanzionatorio, per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

Le sanzioni previste dal Decreto a carico degli Enti, quindi, sono:

- i) sanzioni pecuniarie;
- ii) sanzioni interdittive;
- iii) confisca del prezzo o del profitto del reato;

³¹ Introdotta dalla legge 9 marzo 2022, n. 22 (“*Disposizioni in materia di reati contro il patrimonio culturale*”).

³² Introdotta dalla legge 9 marzo 2022, n. 22 (“*Disposizioni in materia di reati contro il patrimonio culturale*”).

iv) pubblicazione della sentenza di condanna.

Le **sanzioni pecuniarie** si applicano ogniqualvolta venga accertata la responsabilità degli Enti e sono determinate dal giudice penale attraverso un sistema basato su “quote”. Il giudice penale, nell’ambito di un minimo e di un massimo di quote indicate dal legislatore per ciascun Reato, nonché del valore da attribuire ad esse, stabilisce l’ammontare delle sanzioni pecuniarie da irrogare all’Ente.

Le **sanzioni interdittive** possono trovare applicazione per alcune tipologie di Reato e per le ipotesi di maggior gravità. Si traducono nell’interdizione dall’esercizio dell’attività aziendale; nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell’illecito; nel divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio); nell’esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell’eventuale revoca di quelli concessi; nel divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l’Ente, prima della dichiarazione di apertura del dibattimento di primo grado, abbia:

- i) risarcito il danno o lo abbia riparato;
- ii) eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
- iii) messo a disposizione dell’autorità giudiziaria, per la confisca, il profitto del reato;
- iv) eliminato le carenze organizzative che hanno determinato il reato, adottando modelli organizzativi idonei a prevenire la commissione di nuovi Reati.

La durata delle sanzioni interdittive non può essere inferiore ai 3 (tre) mesi, né eccedere i 2 (due) anni.

L’applicazione di esse è prevista solo per alcuni dei Reati specificamente indicati nel Decreto.

Condizione per la comminazione delle sanzioni interdittive è il ricorrere di uno dei seguenti presupposti: (i) che l’Ente abbia tratto dal Reato un profitto di rilevante entità e, al contempo, che il Reato sia stato commesso da un soggetto in posizione apicale o, se commesso da soggetti sottoposti, che la commissione del Reato sia stata agevolata da carenze del modello organizzativo; ovvero, in alternativa, (ii) che vi sia stata reiterazione del Reato.

Nella scelta della sanzione interdittiva applicabile il giudice deve attenersi agli stessi criteri già indicati più sopra per le misure pecuniarie. In particolare, è richiesto che la sanzione interdittiva abbia il carattere della specificità, ossia abbia ad oggetto la specifica attività alla quale si riferisce l’illecito dell’Ente. Fra le varie misure interdittive, quella della sospensione dall’esercizio dell’attività non può esser comminata se non quando l’irrogazione di ogni altra sanzione risulti inadeguata. È anche possibile che più sanzioni interdittive vengano applicate congiuntamente. Nei casi in cui sussistono i presupposti per comminare una sanzione interdittiva che comporta l’interruzione dell’attività dell’Ente, se l’Ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può comportare un grave pregiudizio per la collettività, ovvero se l’interruzione dell’attività, date le dimensioni dell’Ente e le condizioni economiche del territorio sul quale si trova, può avere rilevanti ripercussioni sull’occupazione, è previsto che il giudice possa, in luogo della sanzione interdittiva, disporre che l’attività dell’Ente

continui sotto la guida di un commissario per un periodo pari alla durata della sanzione che sarebbe stata inflitta.

Le misure interdittive sono, in linea di principio, temporanee. Tuttavia, nel caso in cui una stessa persona giuridica venga condannata per almeno tre volte nei sette anni successivi all'interdizione temporanea dall'attività e se ha tratto dal Reato un profitto di rilevante entità, il Decreto prevede la sanzione dell'interdizione definitiva dall'esercizio dell'attività.

Durante il procedimento penale, su richiesta del pubblico ministero, il giudice può disporre alcune delle misure interdittive descritte sopra in via cautelare. Ciò è possibile in presenza di gravi indizi circa la sussistenza della responsabilità dell'Ente e di fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi altri illeciti della stessa indole di quello per cui si procede. Le misure cautelari non possono avere durata superiore a un anno. Anche in sede cautelare è possibile che in luogo delle sanzioni interdittive si disponga il commissariamento dell'Ente per tutto il tempo della durata della sanzione che sarebbe stata applicata.

La **confisca** consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato: non investe, tuttavia, quella parte del prezzo o del profitto del reato che può restituirsi al danneggiato. La confisca è sempre disposta con la sentenza di condanna.

La **pubblicazione della sentenza** può essere inflitta quando all'Ente è applicata una sanzione interdittiva. La sentenza è pubblicata mediante affissione nel comune ove l'Ente ha la sede principale ed è inoltre pubblicata sul sito *internet* del Ministero della Giustizia.

1.4. L'adozione del Modello quale possibile esimente dalla responsabilità amministrativa.

L'articolo 6 del Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora la società dimostri:

- a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, un modello di organizzazione, gestione e controllo idoneo a prevenire Reati della specie di quello verificatosi;
- b) di aver affidato ad un organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del modello, nonché di curare il suo aggiornamento;
- c) che le persone che hanno commesso il Reato hanno agito eludendo fraudolentemente il suddetto modello;
- d) che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lettera b).

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati ed al rischio di commissione dei Reati – il modello debba rispondere alle seguenti esigenze:

- a) individuare le aree a rischio di commissione dei Reati;

- b) prevedere o fare rinvio a specifici protocolli che regolino la formazione e l'attuazione delle decisioni aziendali in relazione ai reati da prevenire;
- c) individuare le risorse finanziarie idonee ad implementare un sistema di organizzazione tale da prevenire la commissione dei Reati;
- d) prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del modello;
- e) configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

CAPITOLO 2.

Adozione del Modello da parte di Digital Solutions.

2.1. Adozione e aggiornamento del Modello e nomina dell'Organismo di Vigilanza.

Con delibera del Consiglio di Amministrazione del 19 dicembre 2018, Digital Solutions ha adottato un Modello e nominato l'Organismo di Vigilanza, cui è attribuito il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento. La Parte Speciale del Modello è stata aggiornata nel 2020 e l'intero Modello viene nuovamente aggiornato nel 2023.

2.2. Le Linee Guida Confindustria e i “Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza”.

Il Decreto dispone che il Modello può essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento³³ redatti da associazioni rappresentative di categoria.

Nella predisposizione del Modello, Digital Solutions si è ispirata alle Linee Guida Confindustria e ai Principi, quali utili strumenti di orientamento per l'interpretazione e l'analisi delle implicazioni giuridiche ed organizzative derivanti dall'introduzione del Decreto.

I punti fondamentali individuati dalle Linee Guida Confindustria per la costruzione dei modelli possono essere così sintetizzati:

- a) individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- b) predisposizione di un sistema di controllo in grado di prevenire i rischi attraverso l'adozione di apposite procedure. Le componenti più rilevanti del sistema di controllo sono individuate nei seguenti strumenti:
 - i) Codice Etico;
 - ii) sistema organizzativo;
 - iii) procedure aziendali;
 - iv) poteri autorizzativi e di firma;
 - v) sistemi di controllo e gestione;
 - vi) comunicazione al personale e sua formazione.

Le componenti del sistema di controllo devono essere ispirate ai seguenti principi:

- a) verificabilità, tracciabilità, coerenza e congruenza di ogni operazione;

³³ Così come modificati dalla legge 6 novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione”.

- b) documentazione dei controlli;
- c) previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- d) individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
 - i) autonomia;
 - ii) indipendenza;
 - iii) professionalità;
 - iv) continuità di azione;
- e) obblighi di informazione dell'Organismo di Vigilanza.

Resta inteso che la scelta di non adeguare il Modello ad alcune indicazioni di cui alle Linee Guida Confindustria o alla *best practice* applicata non inficia la validità dello stesso. Il singolo Modello, infatti, dovendo essere redatto con riferimento alla realtà concreta della Società, ben può discostarsi dalle indicazioni contenute o rappresentate dagli strumenti operativi di riferimento che, per loro natura, hanno carattere generale.

La predisposizione del Modello è stata preceduta da una serie di attività preparatorie, suddivise in differenti fasi qui di seguito descritte, tutte finalizzate alla costruzione di un sistema di prevenzione e gestione dei rischi in linea e ispirato, oltre che alle norme contenute nel Decreto, anche ai contenuti e suggerimenti dettati dalle Linee Guida Confindustria e alla *best practice* italiana in materia.

In particolare, i Principi propongono una precisa metodologia da adottare per la predisposizione del Modello, che prevede:

- a) una fase preliminare, durante la quale si compirà:
 - i) l'effettuazione di un *check-up* aziendale, volto all'acquisizione di informazioni anche documentali rappresentative e descrittive della struttura, della organizzazione e della concreta gestione dell'Ente (il tutto tenendo traccia tramite compilazione di verbali);
 - ii) la verifica del *risk assessment* in ottica 231, per accertare la presenza ed il funzionamento di opportuni presidi che garantiscono la conformità delle attività (*policy* aziendali, regole formali, principi di comportamento e azioni di controllo);
 - iii) l'individuazione della soglia di rischio accettabile e *gap analysis*: solo se il livello di rischio verificato è considerato superiore a quello accettabile, sarà necessario intervenire attraverso operazioni di *risk reduction/risk mitigation*;
- b) in seguito alla fase preliminare, l'elaborazione del Modello, sempre seguendo le Linee Guida Confindustria e perseguendo:

- i) l'integrazione tra Modello e altri sistemi aziendali di gestione e controllo, in quanto questi, ove già presenti, non sostituiscono mai il Modello;
- ii) l'individuazione delle Attività Sensibili nel cui ambito possono essere effettivamente commessi dei Reati;
- iii) l'integrazione dei controlli, mediante la verifica che le componenti siano tra loro coordinate e interdipendenti e che il Modello nel suo complesso sia a sua volta integrato nel piano organizzativo della Società al fine di garantire un assetto unitario;
- iv) la tracciabilità di ogni processo, per la quale ogni azione sia riscontrabile e verificabile;
- v) la segmentazione dei processi, in modo tale che nessuno di questi venga gestito da un unico individuo al fine di incrementare il livello di controlli.

2.3. Le caratteristiche del Modello.

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

L'efficacia.

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

La specificità.

La specificità di un modello organizzativo è uno degli elementi che ne connota l'efficacia. È necessaria una specificità connessa alle aree a rischio, così come richiamata dall'articolo 6, comma 2, lettera a) del Decreto, che impone un censimento delle attività nel cui ambito possono essere commessi i Reati.

È altrettanto necessaria una specificità dei processi di formazione delle decisioni dell'Ente e dei processi di attuazione nei settori "*sensibili*", così come previsto dall'articolo 6, comma 2, lettera b) del Decreto.

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

Il modello, ancora, deve tener conto delle caratteristiche proprie, delle dimensioni dell'Ente e del tipo di attività svolte, nonché della storia dell'Ente medesimo.

L'attualità.

Riguardo a tale aspetto, un modello è idoneo a ridurre i rischi da reato in quanto sia costantemente adattato ai caratteri della struttura e dell'attività d'impresa.

2.4. Funzione e scopo del Modello.

Digital Solutions è consapevole del valore che può derivare da un sistema di controllo interno idoneo a prevenire la commissione dei Reati da parte dei propri Dipendenti, Organi Sociali, Consulenti, *Partner* e Fornitori.

Inoltre, la Società è consapevole altresì che l'adozione e l'efficace attuazione del Modello migliorano il sistema di *corporate governance* in quanto limitano il rischio di commissione dei Reati e consentono di beneficiare dell'esimente prevista dal Decreto.

Pertanto, scopo del presente Modello è la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo finalizzato alla riduzione del rischio di commissione dei Reati mediante l'individuazione delle Aree a Rischio, delle Attività Sensibili e dei principi di comportamento che devono essere rispettati dai Destinatari del Modello. A tal fine, viene di seguito individuata e descritta la costante attività dell'Organismo di Vigilanza finalizzata a garantire il rispetto del sistema organizzativo adottato e la vigilanza sull'operato dei suoi Destinatari, anche attraverso il ricorso a idonei strumenti sanzionatori, sia disciplinari che contrattuali.

I principi contenuti nel presente Modello sono volti, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata da Digital Solutions perché contraria alle norme di deontologia cui essa s'ispira e ai suoi interessi, anche quando apparentemente la Società potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a Digital Solutions di reagire tempestivamente nel prevenire od impedire la commissione del Reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare nei Dipendenti, negli Organi Sociali, nei Consulenti, nei *Partner*, nei Fornitori e in tutti coloro che operano nell'ambito delle Attività Sensibili la consapevolezza di poter determinare – in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure aziendali (oltre che alla legge) – illeciti passibili di conseguenze penalmente rilevanti non solo per sé stessi, ma anche per la Società.

A tal riguardo, le procedure aziendali già adottate e quelle di futura emanazione, così come i principi procedurali indicati nel presente Modello, si caratterizzano per:

- a) separazione all'interno di ciascun processo tra il soggetto che lo inizia e/o lo esegue ed il soggetto che lo controlla;
- b) tracciabilità di ciascun passaggio rilevante del processo sia cartaceo che elettronico;
- c) adeguato livello di formalizzazione.

2.5. Identificazione delle Aree a Rischio e delle Attività Sensibili: attività preliminare.

Per l'identificazione delle Aree a Rischio e delle Attività Sensibili si è proceduto:

- i) all'esame preliminare della documentazione aziendale, tra cui a titolo esemplificativo: organigramma societario, statuto sociale, verbali del Consiglio di Amministrazione (in particolare relativi al conferimento di deleghe e procure), contratti, procedure aziendali su tematiche sensibili in relazione ai reati previsti dal Decreto.

- ii) all'interviste ai soggetti chiave della struttura aziendale, mirate all'individuazione delle Aree a Rischio e all'approfondimento delle Attività Sensibili e del controllo sulle stesse.

2.6. As is e gap analysis.

Sulla base dell'analisi sopra descritta, la Società ha individuato – insieme ai propri Consulenti – le proprie Attività Sensibili relativamente alla situazione aziendale esistente (*as-is analysis*), nonché le azioni di miglioramento (*gap analysis*) da attuare nell'ambito delle stesse sia a livello di procedure interne che di requisiti organizzativi al fine di pervenire alla definizione del Modello.

2.7. **Predisposizione del Modello.**

Il presente Modello è così composto:

- i) una “**Parte Generale**”, contenente l'insieme delle regole e dei principi generali dettati dal Modello;
- ii) una “**Parte Speciale**”, composta da n. 11 “*Parti Speciali*”, ciascuna relativa alle diverse categorie di Reato applicabili alla Società in relazione all'attività dalla stessa svolta, ossia:
 - 1) “**Parte Speciale A**”, denominata “*Reati commessi nei rapporti con la Pubblica Amministrazione ai sensi degli articoli 24 e 25 del Decreto Legislativo 231/2001*”;
 - 2) “**Parte Speciale B**”, denominata “*Reati societari ai sensi dell'articolo 25-ter del Decreto Legislativo 231/2001*”;
 - 3) “**Parte Speciale C**”, denominata “*Reati di corruzione tra privati e di istigazione alla corruzione tra privati ai sensi dell'articolo 25-ter, comma 1, lettera s-bis) del Decreto Legislativo 231/2001*”;
 - 4) “**Parte Speciale D**”, denominata “*Delitti informatici, trattamento illecito di dati e Reati in materia di violazione del diritto d'autore ai sensi degli articoli 24-bis e 25-novies del Decreto Legislativo 231/2001*”;
 - 5) “**Parte Speciale E**”, denominata “*Delitti di criminalità organizzata, Delitti con finalità di terrorismo o di eversione dell'ordine democratico e Reati transnazionali ai sensi degli articoli 24-ter e 25-quater del Decreto Legislativo 231/2001 e 10 della legge 16 marzo 2006, n. 146*”;
 - 6) “**Parte Speciale F**”, denominata “*Delitti di omicidio colposo e lesioni personali colpose gravi e gravissime commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro e Delitto di impiego di cittadini di Stati terzi il cui soggiorno è irregolare ai sensi degli articoli 25-septies e 25-duodecies del Decreto Legislativo 231/2001*”;
 - 7) “**Parte Speciale G**”, denominata “*Delitti contro la personalità individuale ai sensi dell'articolo 25-quinquies del Decreto Legislativo 231/2001*”;
 - 8) “**Parte Speciale H**”: denominata “*Reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita nonché auto-riciclaggio e Delitti in materia*”;

di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori ai sensi degli articoli 25-octies e 25-octies.1 del Decreto Legislativo 231/2001”;

- 9) **“Parte Speciale I”**: denominata *“Reati Tributari ai sensi dell’articolo 25-quinquiesdecies del Decreto Legislativo 231/2001”;*
- 10) **“Parte Speciale J**, denominata *“Reati di falsità in monete in carte di pubblico credito, in valori di bollo ed in strumenti o segni di riconoscimento e Delitti contro l’industria e il commercio ai sensi degli articoli 25-bis e 25-bis.1 del Decreto Legislativo 231/2001”;*
- 11) **“Parte Speciale K”**, denominata *“Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria ai sensi dell’articolo 25-decies del Decreto Legislativo 231/2001”.*

2.7.1. Principi generali cui si ispira il Modello.

Nella predisposizione del Modello si è tenuto conto delle procedure e dei sistemi di controllo esistenti in azienda (rilevati in fase di *“as-is analysis”*), ove considerati idonei a valere anche come misure di prevenzione dei Reati e strumenti di controllo sulle Attività Sensibili. Detto Modello si pone, pertanto, quale ulteriore componente del sistema di controllo interno adottato dalla Società.

In particolare, quali specifici strumenti diretti a programmare la formazione e l’attuazione delle decisioni della Società anche in relazione ai Reati da prevenire, Digital Solutions ha individuato i seguenti presidi:

- (i) il Codice Etico adottato dalla Società;
- (ii) la struttura gerarchico-funzionale e organizzativa della Società;
- (iii) la formazione del personale;
- (iv) il sistema sanzionatorio di cui al CCNL;
- (v) il sistema procedurale;
- (vi) il sistema di controllo;
- (vii) il sistema di gestione.

Le regole, procedure e principi di cui agli strumenti sopra elencati non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

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

- a) le Linee Guida Confindustria, i Principi e la *best practice* italiana esistente in materia, in base alle quali è stata predisposta la mappatura delle Attività Sensibili;
- b) i requisiti indicati dal Decreto ed in particolare:

- i) l'attribuzione ad un Organismo di Vigilanza del compito di attuare in modo efficace e corretto il Modello, anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del Decreto;
 - ii) la messa a disposizione dell'OdV di risorse adeguate ai compiti affidatigli e ai risultati attesi e ragionevolmente ottenibili;
 - iii) l'attività da parte dell'OdV di verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*);
 - iv) la sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- c) i principi generali di un adeguato sistema di controllo interno ed in particolare:
- i) la verificabilità e la tracciabilità di ogni operazione rilevante ai fini del Decreto;
 - ii) il rispetto del principio della separazione delle funzioni;
 - iii) la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
 - iv) la comunicazione all'Organismo di Vigilanza delle informazioni rilevanti;
- d) il sistema dei controlli interni che monitora le aree in cui vi è un'alta probabilità di commissione dei Reati ed un alto valore delle operazioni poste in essere nell'ambito delle Attività Sensibili.

2.7.2. La procedura di adozione, modifica ed integrazione del Modello.

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, la Società, in un'ottica di ricerca dell'eccellenza anche in materia di *corporate governance*, ritiene che la stessa costituisca un valido strumento di sensibilizzazione nei confronti di tutti coloro i quali operano in nome e/o per conto di Digital Solutions, affinché pongano in essere, nell'espletamento delle rispettive attività, comportamenti corretti e atti a prevenire il rischio di commissione dei Reati.

Per tale motivo Digital Solutions ha ritenuto opportuno procedere alla predisposizione del presente Modello, la cui adozione è stata sottoposta al Consiglio di Amministrazione.

Essendo il Modello un atto di emanazione dell'organo dirigente (in conformità alle prescrizioni dell'articolo 6, comma 1, lettera a) del Decreto) le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione.

2.8. Destinatari del Modello.

Le regole contenute nel presente Modello si rivolgono:

- a) alle persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;
- b) alle persone che esercitano, anche di fatto, la gestione ed il controllo della Società stessa;

- c) a tutti i Dipendenti della Società sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra;
- d) ai Consulenti, *Partner*, Fornitori, procuratori e, in genere, ai terzi che operano in nome o per conto o comunque nell'interesse della Società.

Il Modello e i contenuti dello stesso sono comunicati ai Destinatari con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato al successivo capitolo 5 della presente Parte Generale. Pertanto, i Destinatari del Modello sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Società.

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

Sotto tale profilo, infatti:

- i) il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte della Società, allo scopo di esprimere dei principi di “*deontologia aziendale*” che il Digital Solutions riconosce come propri e sui quali richiama l'osservanza da parte di tutti i suoi Destinatari;
- ii) il Modello risponde, invece, a specifiche prescrizioni contenute nel Decreto, finalizzate a prevenire la commissione di particolari tipologie di Reati (per fatti che, commessi apparentemente a vantaggio dell'azienda, possono comportare una responsabilità amministrativa in base alle disposizioni del Decreto).

CAPITOLO 3.

Il Gruppo, la Società ed architettura del sistema normativo interno.

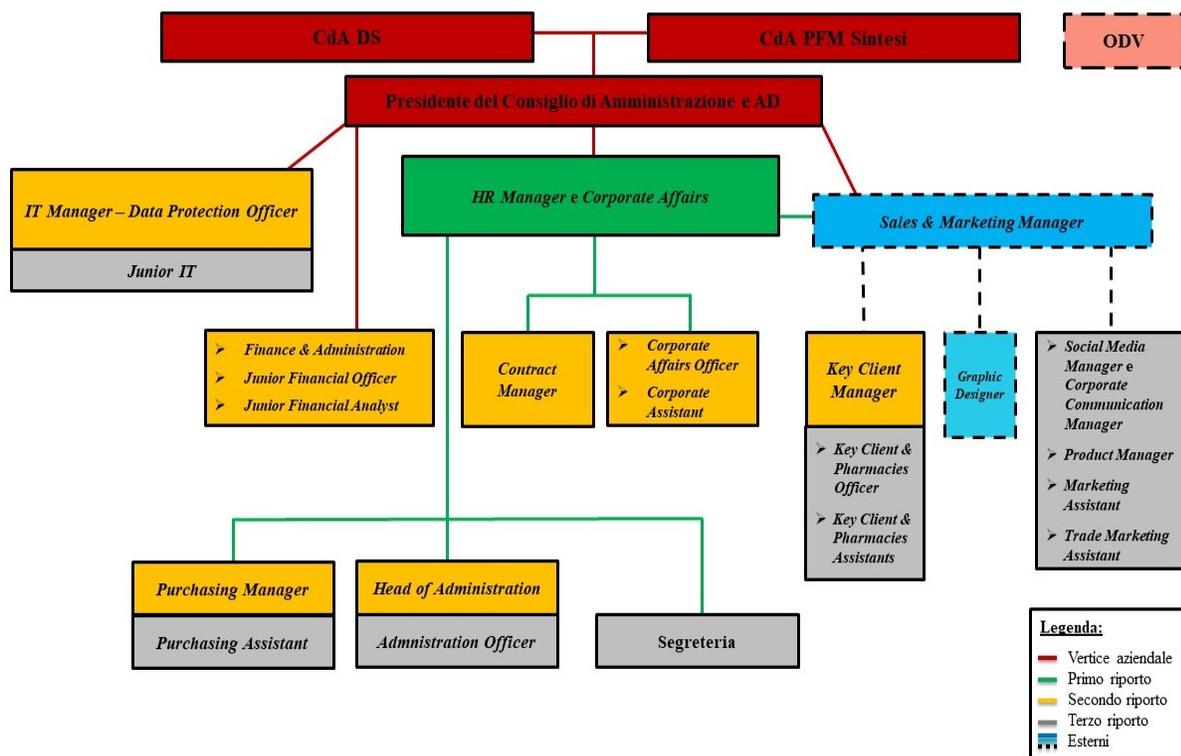
3.1. Il Gruppo PFM.

Il Gruppo PFM ha come *core business* l’offerta ai propri clienti – principalmente aziende del settore farmaceutico – di servizi di consulenza e assistenza di alto livello, anche nell’ambito delle tecnologie *web e digital media*. Il Gruppo PFM ha inoltre diversificato la propria attività, entrando nel capitale sociale di numerose società in diversi settori (quali: consulenza, medicale, *media, marketing*, pubbliche relazioni, energia e *smart city*).

La Capogruppo, in virtù della propria posizione e al fine di favorire una maggiore efficienza e attenzione alle aree di innovazione, *business, marketing* e specializzazione dei processi di ciascuna società del Gruppo PFM, conferisce diversi risorse e servizi ad alcune controllate per il perseguimento di dati obiettivi. Tale coordinamento consente di razionalizzare l’operato del Gruppo PFM.

Anche la Capogruppo ha adottato un proprio modello di organizzazione, gestione e controllo ai sensi del Decreto e un proprio codice etico. Ai consigli di amministrazione delle società del Gruppo 231, riportano i responsabili delle seguenti aree: (i) risorse umane e *corporate*, (ii) *IT e Data Protection Officer*; (iii) Finanziario; (iv) Vendite; (v) Acquisti; (vi) Amministrazione.

L’efficientamento dell’attività operativa del Gruppo 231 è stato perseguito attraverso il seguente organigramma:



3.2. La Società.

Digital Solutions è una società a responsabilità limitata che svolge prevalentemente l'attività di *marketing* e *web-marketing*, *e-mail marketing*, ivi compresa l'editoria medica e le pubblicazioni tecnico-scientifiche con qualsiasi supporto tecnico divulgativo funzionali alle esigenze del settore medico di riferimento, con una particolare *focus* sull'innovazione attraverso l'utilizzo di tecnologie informatiche rivolte alla promozione della cura della salute e della sicurezza delle persone.

L'attività di *business* si concretizza nello sviluppo di progetti di comunicazione e promozione *tailor made* per clienti appartenenti al settore dell'industria farmaceutica.

Digital Solutions, oltre all'attività di agenzia di comunicazione digitale, è specializzata nella gestione degli spazi pubblicitari in farmacia, *leader* nel settore, con una presenza predominante sul territorio italiano sin dal 2009. La Società ha, inoltre, sviluppato una rete di rapporti contrattuali con circa 12.000 farmacie, che gestisce a livello nazionale, grazie alla quale è in grado di cogliere nuove necessità e opportunità del settore farmaceutico per offrire soluzioni specifiche e all'avanguardia.

Tra i prodotti strategici della Società giova evidenziare, al solo fine esemplificativo, un sistema di telepresenza che segna un passo in avanti nel settore dell'*advertisement* permettendo alle aziende di fornire un supporto immediato ai propri clienti e di promuovere il proprio *brand* e prodotti in modo innovativo.

Il sistema unisce la semplicità di una videochiamata, la mobilità di un dispositivo controllato da remoto e le funzionalità di un *i-Pad*; l'assistente digitale controllabile a distanza che guarda, ascolta, si muove e parla, interagisce con gli utenti come se si fosse presenti di persona.

Tra i prodotti commercializzati dall'azienda è di rilievo anche il servizio telefonico multilingua per ricevere supporto immediato nella gestione del cliente a livello internazionale. Il servizio H24 per 7 giorni permette di superare le barriere linguistiche tramite una semplice chiamata ad un interprete madrelingua per traduzioni immediate.

Una *app* dedicata permette di trovare una farmacia del *network*, o fornire tutti i numeri di emergenza, o rendere disponibile un dizionario dei farmaci e principi attivi nelle lingue più parlate al mondo.

Da ultimo, la Società ha assunto la qualifica di società *benefit* e in tal senso intende perseguire una o più finalità di beneficio comune e operare in modo responsabile, sostenibile e trasparente nei confronti di persone, comunità, territori e ambiente, beni e attività culturali e sociali, enti e associazioni ed altri portatori di interesse. Tali obiettivi verranno concretamente realizzati mediante, a titolo esemplificativo, (i) la promozione e realizzazione di progetti sociali e ambientali basati sul coinvolgimento e il dialogo collaborativo con gli investitori e la trasparenza nella *governance*; (ii) l'organizzazione di *workshop*, corsi di formazione e campagne di comunicazione per i dipendenti volti a diffondere la cultura della sostenibilità promuovendo, a tale scopo, modalità di lavoro in linea con la tutela dell'ambiente che valorizzino, tra gli altri, lo *smart working* e altre forme flessibili di gestione delle attività lavorative, l'eliminazione degli sprechi, la riduzione dei consumi di carta e, più in generale, l'utilizzo di risorse ecosostenibili; (iii) la promozione di modalità di lavoro che favoriscano la creazione di un ambiente di lavoro positivo nel rispetto, tra gli altri, della parità di genere e finalizzato alla valorizzazione, alla crescita e al benessere delle persone per svilupparne competenze e potenziale, rispettando, altresì, tempi e bisogni individuali.

La Società opera in Italia con base operativa in Milano e, inoltre, è certificata ISO/IEC 27001:2023 (“*Tecnologia delle informazioni – Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni – Requisiti*”) e ISO/IEC 9001:2015 (“*Sistemi di Gestione per la Qualità – IEC*”).

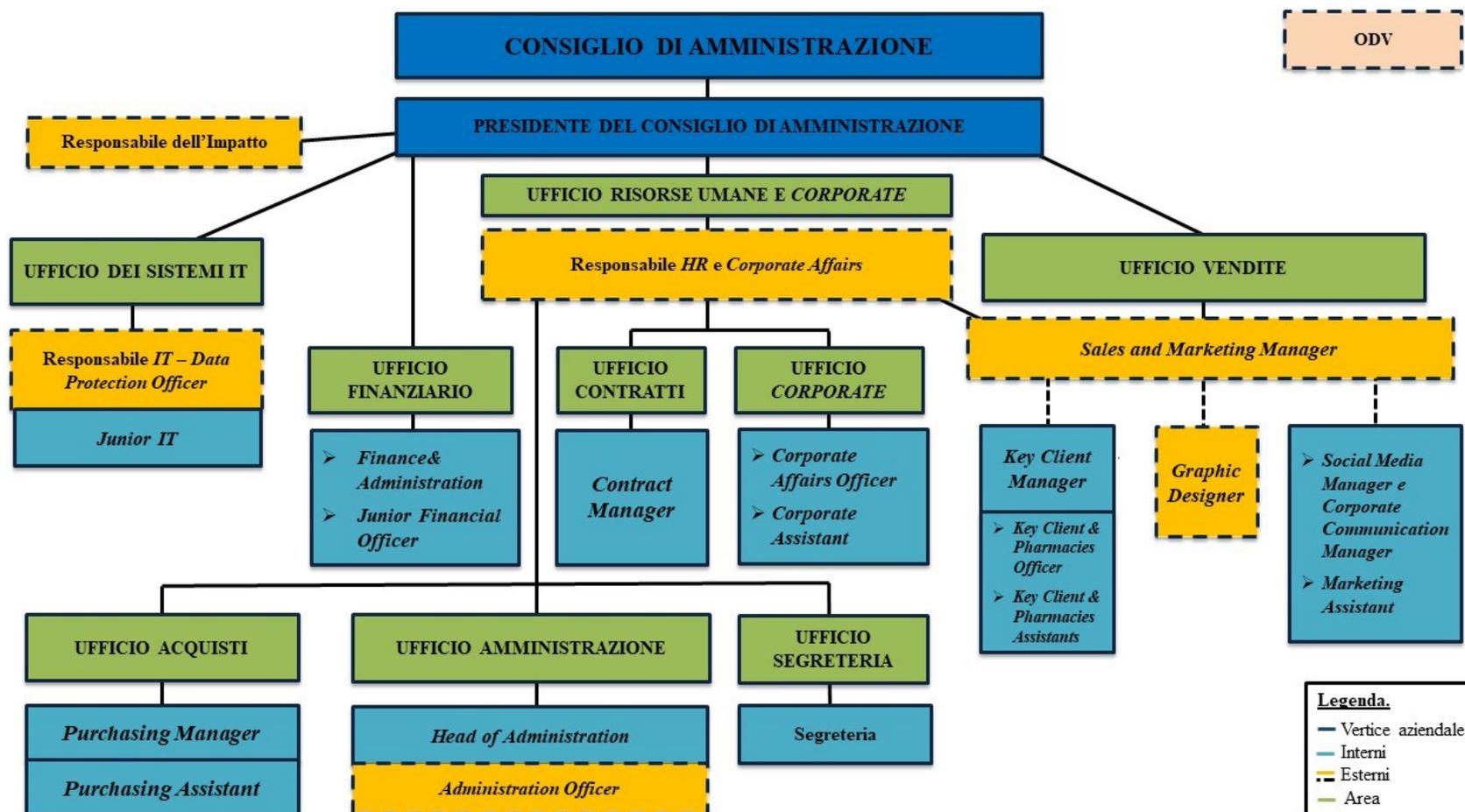
3.3. La Corporate Governance di Digital Solutions.

Digital Solutions è caratterizzata da una struttura organizzativa funzionale, ove le diverse unità funzionali della Società sono: (i) gestite da un responsabile, il quale a sua volta riporta direttamente al Consiglio di Amministrazione; (ii) suddivise in vari dipartimenti. La Società, inoltre, in virtù dell’assunzione della qualifica di società *benefit*, ha nominato un Responsabile dell’Impatto.

La Società è amministrata da un Consiglio di Amministrazione, nel cui ambito il Presidente è dotato dei poteri di ordinaria e straordinaria amministrazione, ed è dotata di una società di revisione esterna.

Al Consiglio di Amministrazione riportano i responsabili dei seguenti settori: (i) risorse umane e corporate; (ii) sistemi IT; (iii) vendite; (iv) finanziario; (v) contratti; (vi) acquisti e (vii) amministrazione.

Tale schema organizzativo è qui di seguito rappresentato³⁴:



Le regole di *governance* della Società sono definite nello statuto sociale della stessa e nel sistema di deleghe e procure adottato dalla Società. Si precisa che nel successivo paragrafo 3.4 vengono dettagliatamente previste le regole generali del sistema di deleghe e procure.

³⁴ I riquadri tratteggiati ed evidenziati in giallo indicano le risorse esterne di cui la Società si avvale.

3.4. Regole generali.

3.4.1. Il sistema in linea generale.

Tutte le Attività Sensibili indicate nelle Aree a Rischio devono essere svolte in conformità alle leggi vigenti, al Codice Etico, ai valori e ai principi comportamentali generali e specifici della Società e alle regole contenute nel presente Modello.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di: (i) formalizzazione e chiarezza, (ii) comunicazione e separazione dei ruoli, in particolare per quanto attiene all'attribuzione di responsabilità e di rappresentanza, (iii) formazione e (iv) definizione delle linee gerarchiche e delle attività operative.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, eccetera) improntati a principi generali di:

- i) conoscibilità all'interno della Società;
- ii) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;
- iii) chiara descrizione dei flussi informativi all'interno della Società.

Le procedure interne devono essere caratterizzate dai seguenti elementi:

- a) massima separatezza possibile, compatibilmente con le risorse disponibili, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;
- b) traccia scritta di ciascun passaggio rilevante del processo;
- c) adeguato livello di formalizzazione;
- d) sistemi premianti dei soggetti dotati di poteri di spesa o facoltà decisionali a rilevanza esterna, quando esistenti, basati su *target* di *performance* sostanzialmente raggiungibili.

3.4.2. Il sistema di deleghe e procure.

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di “sicurezza” ai fini della prevenzione dei Reati (tracciabilità delle Attività Sensibili svolte all'interno delle Aree a Rischio) e, al contempo, consentire la gestione efficiente della struttura operativa.

Si intende per “*delega*” l'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per “*procura*” il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi.

Ai titolari di una funzione, che necessitano per lo svolgimento dei loro incarichi di poteri di rappresentanza, viene conferita una “*procura generale funzionale*” di estensione adeguata e coerente con le funzioni e i poteri di gestione attribuiti al titolare attraverso la “*delega*”.

I requisiti essenziali del sistema di deleghe, ai fini di un'efficace prevenzione dei Reati sono i seguenti:

- i) tutti coloro che intrattengono per conto della Società rapporti con la Pubblica Amministrazione o con soggetti terzi devono essere dotati di delega formale in tal senso, limitata alla reale attività svolta;
- ii) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità attribuita alla specifica funzione aziendale, nonché alla posizione ricoperta nell'organigramma ed essere aggiornate in conseguenza ad eventuali mutamenti organizzativi;
- iii) ciascuna delega deve definire in modo specifico ed inequivoco:
 - a) i poteri del delegato;
 - b) il soggetto (organo o individuo) cui il delegato riporta gerarchicamente;
 - c) i poteri gestionali assegnati che dovranno essere coerenti con gli obiettivi imprenditoriali della Società;
- iv) il delegato, ove pertinente, deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei Reati, sono i seguenti:

- i) le procure generali funzionali sono conferite esclusivamente a soggetti dotati di delega interna;
- ii) le procure generali devono descrivere i poteri di gestione conferiti e, ove necessario, sono accompagnate da apposita comunicazione organizzativa che fissi: l'estensione di poteri di rappresentanza ed i limiti di spesa numerici; ovvero i limiti assuntivi per categorie di rischio, richiamando comunque il rispetto dei vincoli posti dai processi di approvazione del *budget* e degli eventuali *extra budget*, dai processi di determinazione dei poteri assuntivi, dai processi di monitoraggio delle Aree a Rischio da parte di funzioni diverse;
- iii) la procura deve essere conferita 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;
- iv) le procure speciali devono dettagliatamente stabilire l'ambito di operatività e i poteri del procuratore;
- v) devono essere individuate le modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le procure devono essere attribuite, modificate e revocate (assunzione o estensione di nuove responsabilità e poteri, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, revoca, eccetera).

L'OdV verifica periodicamente, eventualmente con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni

organizzative (tali sono quei documenti interni alla Società con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

3.5. Il sistema di controlli interni e gestione dei rischi.

Il sistema di controllo adottato dalla Società si caratterizza per la presenza di una serie di regole, di procedure e di strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

La responsabilità del sistema di controllo interno compete al Consiglio di Amministrazione e all'OdV, che provvede a fissarne le linee di indirizzo e a verificarne periodicamente l'adeguatezza e l'effettivo funzionamento, assicurandosi che i principali rischi aziendali vengano identificati e gestiti in modo corretto.

3.6. Descrizione delle Attività Sensibili e piano dei controlli.

Dall'analisi dei rischi condotta ai fini dell'adozione del Modello e dal suo aggiornamento alla luce dell'introduzione di ulteriori Reati, è emerso che le principali Aree a Rischio e le Attività Sensibili individuate all'interno della Società al momento riguardano i seguenti Reati:

- 1) reati commessi nei rapporti con la P.A.;
- 2) reati societari;
- 3) reati di corruzione tra privati e di istigazione alla corruzione tra privati;
- 4) delitti informatici e trattamento illecito di dati;
- 5) reati in materia di violazione del diritto d'autore;
- 6) reati di criminalità organizzata;
- 7) delitti con finalità di terrorismo o di eversione all'ordine democratico;
- 8) reati transnazionali;
- 9) reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- 10) reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare;
- 11) delitti contro la personalità individuale;
- 12) reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita, nonché auto-riciclaggio;

- 13) delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori;
- 14) reati tributari;
- 15) reati di falsità di monete in carte di pubblico credito, in valori di bollo ed in strumenti di riconoscimento;
- 16) reati contro l'industria e il commercio;
- 17) delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

Si rinvia alla Parte Speciale del Modello per la descrizione analitica delle Aree a Rischio e delle singole Attività Sensibili relative a ciascuna categoria di Reato sopra elencate e dei principi di comportamento generali e specifici, nonché alle relative procedure.

L'Organismo di Vigilanza ha il potere di individuare eventuali ulteriori Aree a Rischio e Attività Sensibili che – a seconda dell'evoluzione legislativa o dell'attività della Società – potranno essere comprese nel novero delle stesse.

I profili di rischio inerenti ai Reati previsti dal Decreto non ricompresi nell'elenco sopra riportato si reputano complessivamente presidiati dalle disposizioni di cui al Modello e dai principi di cui al Codice Etico ovvero non applicabili alla Società.

CAPITOLO 4.

L'Organismo di Vigilanza.

4.1. Identificazione dell'Organismo di Vigilanza.

Ai sensi dell'articolo 6, comma 1, lettera b), del Decreto, condizione indispensabile per la concessione dell'esimente dalla responsabilità amministrativa è l'attribuzione ad un organismo della Società, dotato di autonomi poteri di iniziativa e di controllo, del compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

Sul tema, le Linee Guida Confindustria, interpretando le disposizioni del Decreto, suggeriscono l'individuazione in un organo interno alla struttura della Società, caratterizzato da *autonomia, indipendenza, continuità di azione*, nonché in possesso di *professionalità e onorabilità* adeguate al ruolo.

Volendo nello specifico analizzare i singoli requisiti che devono caratterizzare l'Organismo di Vigilanza, si precisa quanto segue.

A. Autonomia e indipendenza.

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (ad esempio, amministratore delegato, consiglio di amministrazione, amministratore unico), che sia dotato di effettivi poteri di ispezione e controllo, che abbia possibilità di accesso alle informazioni aziendali rilevanti e che sia dotato di risorse finanziarie adeguate delle quali potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (quali ad esempio: consulenze specialistiche, eventuali trasferte, eccetera).

L'indipendenza, inoltre, presuppone che l'Organismo di Vigilanza non si trovi in una posizione, neppure potenziale, di conflitto d'interessi con la Società, né sia titolare all'interno della stessa di funzioni con poteri di tipo esecutivo.

B. Onorabilità e cause di ineleggibilità.

Non possono essere eletti membri dell'Organismo di Vigilanza, e se lo sono, decadono necessariamente ed automaticamente dalla carica:

- i) coloro che si trovano nelle condizioni previste dall'articolo 2382 del codice civile, ovvero sia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi;
- ii) coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423 ("*legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità*") o della legge 31 maggio 1965, n. 575 ("*legge contro la mafia*");

- iii) coloro che siano stati condannati a seguito di sentenza ancorché non ancora definitiva, o emessa *ex* articoli 444 e seguenti del codice di procedura penale o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
 - a) per uno dei delitti previsti nel Titolo XI del Libro V del codice civile (recante le “*Disposizioni penali in materia di società e consorzi*”) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni (recante la “*Disciplina del fallimento, del concordato preventivo, dell’amministrazione controllata e della liquidazione coatta amministrativa*”);
 - b) per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l’ordine pubblico, contro l’economia pubblica ovvero per un delitto in materia tributaria;
 - c) alla reclusione per un tempo non inferiore a 2 (due) anni per un qualunque delitto non colposo;
 - d) per uno o più illeciti tra quelli tassativamente previsti dal Decreto, fatto salvo il caso di sentenze emesse *ex* articoli 444 e seguenti del codice di procedura penale comportanti l’applicazione di sole sanzioni pecuniarie di importo non superiore a Euro 1.500,00;
- iv) coloro che abbiano rivestito la qualifica di componente dell’OdV in società nei cui confronti siano state applicate le sanzioni previste dall’articolo 9 del Decreto, salvo che siano trascorsi 5 (cinque) anni dalla inflizione in via definitiva delle sanzioni e il componente non sia incorso in condanna penale ancorché non definitiva;
- v) coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall’articolo 187-*quater* del TUF.

C. Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale.

L’Organismo di Vigilanza deve possedere, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l’obiettività di giudizio; è necessario, pertanto, che all’interno dell’Organismo di Vigilanza siano presenti soggetti con professionalità adeguate in materia economica, di controllo e gestione dei rischi aziendali. L’Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica, di organizzazione aziendale, revisione, contabilità e finanza.

D. Continuità d’azione.

L’Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine in modo da garantire la dovuta continuità nell’attività di vigilanza. In particolare, l’Organismo di Vigilanza: (i) cura l’attuazione del Modello assicurandone il costante

aggiornamento; (ii) non svolge mansioni esecutive che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

In ottemperanza a quanto stabilito dal Decreto, e considerato tutto quanto sopra indicato, il Consiglio di Amministrazione della Società, con delibera del 19 dicembre 2018, ha deciso che la composizione dell'Organismo di Vigilanza fosse monocratica, con nomina di consulente esterno alla Società dotato di particolare e consolidata esperienza in materia 231.

Difatti, le decisioni relative all'individuazione e alla nomina dei componenti sono demandate al Consiglio di Amministrazione tra le figure che saranno riconosciute come le più adeguate ad assumere il ruolo dell'OdV, in quanto in possesso dei requisiti di autonomia, indipendenza, professionalità, onorabilità e continuità d'azione che si richiedono per tale funzione e delle capacità specifiche in tema di attività ispettive e di consulenza, nonché in possesso di quei requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito affidato, quali onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli Organi Sociali.

4.2. Durata in carica.

L'Organismo di Vigilanza è nominato dall'organo amministrativo della Società per un periodo di 3 (tre) anni, mediante apposita delibera: a tal riguardo, al momento della nomina devono essere forniti, nel corso della riunione consiliare, adeguati chiarimenti in merito alla professionalità dei suoi componenti, il cui *curriculum vitae* deve essere allegato al relativo verbale.

Alla scadenza dell'incarico, l'OdV potrà continuare a svolgere le proprie funzioni e ad esercitare i poteri di propria competenza, come in seguito meglio specificati, sino alla nomina dei nuovi componenti da parte del Consiglio di Amministrazione.

Al fine di garantire i requisiti di indipendenza e di autonomia, dal momento della nomina e per tutta la durata della carica, i componenti (ovvero in caso di unico membro, il componente) dell'Organismo di Vigilanza:

- a) non devono rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione della Società;
- b) non devono svolgere funzioni con poteri di tipo esecutivo;
- c) non devono intrattenere significativi rapporti d'affari con la Società, con società da essa controllate o ad essa collegate, salvo il rapporto di lavoro subordinato, né intrattenere significativi rapporti d'affari con gli eventuali amministratori muniti di deleghe (amministratori esecutivi);
- d) non devono avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai parenti ed affini entro il quarto grado;
- e) non devono risultare titolari, direttamente o indirettamente, di partecipazioni nel capitale della Società;

- f) devono avere e mantenere i requisiti di onorabilità indicati nella lettera B del paragrafo 4.1 che precede.

I componenti dell'Organismo di Vigilanza sono tenuti a sottoscrivere, all'atto della nomina, una dichiarazione attestante l'esistenza dei requisiti di indipendenza di cui sopra e, comunque, a comunicare immediatamente al Consiglio di Amministrazione, nonché agli altri componenti dell'Organismo di Vigilanza nel caso di organismo collegiale, l'insorgere di eventuali condizioni ostative e/o la perdita delle condizioni di cui sopra.

Rappresentano ipotesi di decadenza automatica le incompatibilità di cui alle precedenti lettere da a) ad e) del presente paragrafo, le circostanze di cui alla lettera f), la sopravvenuta incapacità e la morte. Fatte salve le ipotesi di decadenza automatica, il/i membro/i dell'Organismo di Vigilanza non può/possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

A tal proposito, rappresentano ipotesi di giusta causa di revoca, a titolo meramente esemplificativo:

- (i) l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'articolo 6, comma 1, lettera d) del Decreto, risultante una sentenza di condanna, passata in giudicato, emessa nei confronti della Società ai sensi del Decreto ovvero da una sentenza di patteggiamento;
- (ii) la violazione degli obblighi di riservatezza di cui al successivo paragrafo 4.9;
- (iii) la mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo;
- (iv) grave negligenza nell'adempimento dei propri compiti;
- (v) in caso di soggetti interni alla struttura aziendale, le eventuali dimissioni o licenziamento.

In casi di particolare gravità, l'organo amministrativo potrà comunque disporre la sospensione dei poteri dell'Organismo di Vigilanza e procedere alla nomina di un organismo *ad interim*.

In caso di dimissioni o di decadenza automatica di un membro effettivo dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o altre cause, la maggioranza dei componenti. In tal caso, il Consiglio di Amministrazione provvede a nominare nuovi componenti.

4.3. Funzione e poteri dell'Organismo di Vigilanza.

All'OdV è affidato il compito di vigilare:

- a) sull'osservanza del Modello da parte dei Dipendenti, degli Organi Sociali, dei Consulenti, dei *Partner* e dei Fornitori;
- b) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;

- c) sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

Su di un piano più operativo, all'OdV sono affidati i compiti di seguito riportati.

A. Aggiornamenti, potestà normativa, segnalazioni.

- (i) Sugerire e promuovere l'emanazione di disposizioni procedurali attuative dei principi e delle regole contenute nel Modello;
- (ii) interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando al Presidente le possibili aree di intervento;
- (iii) valutare le esigenze di aggiornamento del Modello, segnalando al Presidente le possibili aree di intervento;
- (iv) indicare nella relazione annuale al Consiglio di Amministrazione di cui al paragrafo 4.6 le opportune integrazioni, ad esempio, ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita) per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto;
- (v) indicare nella relazione annuale al Consiglio di Amministrazione di cui al paragrafo 4.6 l'opportunità di emanare particolari disposizioni procedurali attuative dei principi contenuti nel Modello, che potrebbero non essere coerenti con quelle in vigore attualmente nella Società, curando altresì il coordinamento delle stesse con quanto esistente.

B. Verifiche e controlli.

- (i) Condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Aree a Rischio e delle Attività Sensibili;
- (ii) in ottemperanza a quanto previsto nel calendario annuale delle attività dell'Organismo di Vigilanza, effettuare periodiche verifiche mirate su determinate operazioni o specifici atti posti in essere da Digital Solutions, soprattutto nell'ambito delle Aree a Rischio e delle Attività Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di *reporting* agli Organi Sociali deputati;
- (iii) raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere ad esso trasmesse o tenute a propria disposizione (vedi in dettaglio il successivo paragrafo 4.6);
- (iv) coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale (sia cartacea sia informatica) che ritiene rilevante e deve essere costantemente informato dal *management*: (i) sugli aspetti dell'attività aziendale che possono esporre Digital

Solutions al rischio di commissione di uno dei Reati; (ii) sui rapporti con i Consulenti, *Partner* e Fornitori che operano per conto della Società nell'ambito di Attività Sensibili;

- (v) attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine;
- (vi) sollecitare l'attuazione delle procedure di controllo previste dal Modello, anche tramite l'emanazione o proposizione di disposizioni (normative e/o informative) interne.

C. **Formazione.**

- (i) Definire i programmi di formazione per il personale e il contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Sociali, finalizzate a fornire ai medesimi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al Decreto;
- (ii) monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;
- (iii) far predisporre ed aggiornare con continuità lo spazio nell'*intranet* della Società contenente tutte le informazioni relative al Decreto, al Codice Etico e al Modello.

D. **Sanzioni.**

- (i) Coordinarsi con il *management* aziendale per valutare o proporre l'adozione di eventuali sanzioni o provvedimenti, fermo restando la competenza di quest'ultimo - e in particolare degli incaricati della gestione delle risorse umane - in merito alla decisione e all'irrogazione dei medesimi (si rinvia in merito a tale punto al successivo capitolo 6 della presente Parte Generale).

4.4. **Poteri dell'Organismo di Vigilanza.**

L'OdV ha, *ex lege*, autonomi poteri di iniziativa e controllo ai fini di vigilare sul funzionamento e sull'osservanza del Modello, ma non ha poteri coercitivi o di intervento sulla struttura aziendale ovvero poteri sanzionatori, poteri questi che sono demandati ai competenti Organi Sociali o alle funzioni aziendali competenti.

Tenuto conto delle peculiarità delle attribuzioni e degli specifici contenuti professionali richiesti, nello svolgimento dei compiti di vigilanza e controllo l'OdV sarà costantemente supportato anche da tutti i dirigenti e dal *management* della Società. In capo a questi ultimi, nell'ambito delle rispettive funzioni e nei limiti delle deleghe assegnate, ricade una responsabilità primaria per quanto concerne: (i) il controllo delle attività e delle aree di competenza; (ii) l'osservanza del Modello da parte dei Dipendenti sottoposti alla loro direzione; (iii) la tempestiva e puntuale informazione verso l'OdV su eventuali anomalie, problematiche riscontrate e/o criticità rilevate.

L'OdV potrà richiedere ai dirigenti, o qualora tale funzione non fosse prevista dall'organigramma ai quadri, specifiche attività di controllo sul corretto e preciso funzionamento del Modello.

Tutti i soggetti coinvolti all'interno della struttura aziendale sono tenuti a vigilare ed informare l'OdV sulla corretta applicazione del presente Modello, ciascuno nell'ambito delle proprie competenze operative.

L'OdV può avvalersi, ogni qualvolta lo ritenga necessario, nell'espletamento della propria attività di vigilanza e di tutto quanto previsto nel presente Modello, della collaborazione di ulteriori risorse, prescelte nell'ambito delle varie funzioni aziendali, senza limitazioni di tempo e di numero.

L'autonomia e l'indipendenza che necessariamente devono connotare le attività dell'OdV hanno reso necessario introdurre alcune forme di tutela in suo favore, al fine di garantire l'efficacia del Modello e di evitare che la sua attività di controllo possa ingenerare forme di ritorsione a suo danno. Pertanto, le decisioni in merito a trasferimento o sanzioni relative all'OdV e ai suoi membri, allorquando essi siano Dipendenti della Società, sono attribuite alla competenza esclusiva del Consiglio di Amministrazione, sentito, laddove necessario, il responsabile delle risorse umane.

Il Consiglio di Amministrazione conferisce all'OdV i seguenti poteri:

- a) potere di accedere a tutti i documenti e a tutte le informazioni relative alla Società;
- b) potere di avvalersi di tutte le strutture della Società, che sono obbligate a collaborare, dei revisori e di Consulenti esterni;
- c) potere di raccogliere informazioni presso tutti i Destinatari del presente Modello, incluso il revisore, in relazione a tutte le attività della Società;
- d) potere di richiedere, attraverso i canali e le persone appropriate, la riunione con il Presidente per affrontare questioni urgenti;
- e) potere di richiedere ai titolari delle funzioni aziendali di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza;
- f) potere di avvalersi di Consulenti esterni ai quali delegare circoscritti ambiti di indagine o attività. A tale proposito, il Consiglio di Amministrazione dovrà approvare ogni anno un budget di spesa per l'OdV, il quale ne potrà disporre liberamente in relazione alle proprie attività attraverso le strutture aziendali preposte, salvo richieste integrazioni per eventuali necessità sopravvenute;
- g) potere di proporre, sulla base delle verifiche di cui sopra, l'aggiornamento del Modello medesimo laddove si riscontrino esigenze di adeguamento dello stesso.

4.5. Regole di convocazione e di funzionamento.

L'Organismo di Vigilanza può disciplinare con specifico regolamento le modalità del proprio funzionamento, sulla base delle specifiche di seguito riportate:

- a) l'Organismo di Vigilanza si riunisce (ovvero in caso di organismo monocratico si reca presso la Società) con cadenza trimestrale e la relativa documentazione deve essere distribuita almeno 3 (tre) giorni prima della seduta;

- b) le sedute potranno tenersi di persona, ovvero per video o teleconferenza (o in combinazione);
- c) l'organo amministrativo della Società ha la facoltà che, in caso di comprovate esigenze, l'Organismo di Vigilanza si riunisca in qualsiasi momento;
- d) in caso di organismo collegiale, per la validità delle sedute è richiesto l'intervento della maggioranza dei membri in carica;
- e) possono essere effettuate sedute *ad hoc* e tutte le decisioni prese durante queste sedute devono essere riportate nella successiva seduta trimestrale;
- f) la decisione viene assunta sulla base dell'unanimità; in mancanza, prevale la decisione maggioritaria e ciò viene riportato immediatamente al Consiglio di Amministrazione;
- g) i verbali delle sedute riportano tutte le decisioni prese e riflettono le principali considerazioni effettuate per raggiungere la decisione; tali verbali vengono conservati dall'OdV nel proprio archivio.

4.6. Flussi informativi dell'OdV verso gli Organi Sociali.

L'OdV riferisce agli Organi Sociali in merito all'attuazione del Modello e all'emersione di eventuali criticità.

In particolare, l'OdV:

- a) con cadenza semestrale, informa l'organo amministrativo della Società in merito all'attività svolta;
- b) con cadenza annuale, informa l'organo amministrativo della Società in merito all'attività svolta nell'anno in corso, nonché in relazione ad eventuali criticità (e spunti per il miglioramento), sia con riferimento a comportamenti o eventi interni a Digital Solutions, sia in termini di efficacia del Modello;
- c) immediatamente, informa l'organo amministrativo della Società, al verificarsi di situazioni straordinarie e/o in caso di segnalazioni ricevute che rivestano il carattere dell'urgenza.

Inoltre, l'OdV predispose annualmente una relazione scritta per il Consiglio di Amministrazione ove sia contenuta:

- i) un'analisi sintetica di tutta l'attività svolta nel corso dell'anno (indicando in particolare i controlli effettuati e l'esito degli stessi, le verifiche specifiche di cui al successivo capitolo 7 e l'esito delle stesse, l'eventuale aggiornamento della mappatura delle Attività Sensibili, eccetera);
- ii) il piano di attività previsto per l'anno successivo.

L'organo amministrativo della Società ha la facoltà di convocare in qualsiasi momento l'OdV che, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione di tale organo per motivi urgenti.

L'OdV deve, inoltre, coordinarsi con le funzioni competenti presenti in Società per i diversi profili specifici, come ad esempio:

- (i) con la funzione legale (ove presente), amministrativa e la funzione responsabile della segreteria societaria per gli adempimenti sociali che possono avere rilevanza ai fini della commissione dei reati societari;
- (ii) con il responsabile della gestione del personale in ordine alla formazione e ai provvedimenti disciplinari;
- (iii) con i responsabili della funzione amministrativa in ordine alla gestione dei flussi finanziari;
- (iv) con il datore di lavoro e/o il soggetto delegato, l'RLS o l'RSPP o Medico Competente per le tematiche relative alla salute e sicurezza sul lavoro;
- (v) con il responsabile dell'*information technology* per le tematiche legate alla gestione degli strumenti e dei sistemi IT.

Qualora i Dipendenti dovessero richiedere informazioni e chiarimenti o domande relative a tematiche collegate al rispetto delle leggi sia nazionali che europee, del Modello e/o del Codice Etico adottati dalla Società, l'OdV è tenuto a fornire quanto richiesto entro un termine congruo, così come previsto nell'apposita procedura adottata al fine di meglio precisare e disciplinare i flussi di informazione, comunicazione e segnalazione da e verso l'OdV.

4.7. Flussi informativi nei confronti dell'Organismo di Vigilanza.

L'OdV deve essere informato, mediante apposite segnalazioni³⁵ da parte, tra l'altro, dei Dipendenti, degli Organi Sociali e dei suoi componenti, dei Consulenti, dei *Partner*, dei Fornitori in merito ad eventi che potrebbero essere delle violazioni ai sensi del Decreto e ai sensi del Modello così come previsto nell'apposita procedura adottata dalla Società.

Valgono al riguardo le seguenti prescrizioni di carattere generale:

- a) i Dipendenti e gli Organi Sociali devono segnalare all'OdV le notizie relative alla commissione, o alla ragionevole convinzione di commissione dei Reati;
- b) i Dipendenti con la qualifica di dirigente hanno l'obbligo di segnalare all'OdV anche le violazioni delle regole di comportamento o procedurali contenute nel presente Modello di cui vengano a conoscenza;
- c) i Consulenti, i *Partner* e i Fornitori, sono tenuti ad effettuare le segnalazioni con le modalità e nei limiti previsti contrattualmente ovvero con le modalità previsti nell'apposita procedura.

³⁵ Il decreto legislativo 10 marzo 2023, n. 24, definisce la segnalazione come la comunicazione, scritta od orale, tramite canali interni ed esterni, di informazioni sulle violazioni poste in essere ed apprese durante l'attività lavorativa.

In ogni caso, Digital Solutions garantisce alle persone segnalanti una tutela adeguata e delle misure di protezione da qualsiasi forma di ritorsione, discriminazione o penalizzazione ed assicura la massima riservatezza circa la loro identità, così come meglio specificato nel paragrafo 4.9, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni sopra descritte, gli Organi Sociali, i Dipendenti, i Consulenti, i *Partner* e i Fornitori devono obbligatoriamente ed immediatamente trasmettere all'OdV le informazioni concernenti:

- a) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati, qualora tali indagini coinvolgano Digital Solutions o i suoi Dipendenti, Organi Sociali, Consulenti, *Partner*, Fornitori;
- b) le notizie relative ai procedimenti sanzionatori svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.

In ogni caso devono essere trasmesse all'Organismo di Vigilanza, da parte delle funzioni aziendali che operano nell'ambito delle Aree a Rischio e delle Attività Sensibili, le informazioni relative:

- i) alle risultanze periodiche dell'attività di controllo dalle stesse poste in essere per dare concreta attuazione al Modello (attività di monitoraggio, *report* riepilogativi dell'attività svolta, eccetera);
- ii) le eventuali anomalie riscontrate nello svolgimento delle proprie attività.

L'OdV, inoltre, ha il diritto di richiedere informazioni in merito al sistema di deleghe adottato da Digital Solutions, secondo modalità dallo stesso stabilite.

Qualora uno dei soggetti sopra indicati non adempia agli obblighi informativi di cui al presente paragrafo 4.7, allo stesso sarà irrogata una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza agli obblighi sopra menzionati e che sarà comminata secondo le regole indicate nel capitolo 6 del presente Modello.

In aggiunta ai principi generali stabiliti nella presente Parte Generale, la Società ha adottato apposite procedure al fine di meglio precisare e disciplinare i flussi di informazione, comunicazione e segnalazione da e verso l'OdV, a cui si rinvia.

4.8. Modalità delle segnalazioni.

I Dipendenti, i Consulenti, i *Partner*, i Fornitori e gli Organi Sociali potranno effettuare le segnalazioni, tra quelle sopra indicate, direttamente all'OdV mediante i canali a tal fine predisposti.

Tutte le informazioni sui canali, sulla procedura e sui presupposti per effettuare le segnalazioni all'OdV sono esposte e rese facilmente visibili a tutti i Destinatari, tra l'altro, nel sito *internet* di proprietà della Società.

Le segnalazioni potranno essere effettuate secondo una delle seguenti modalità:

- (i) **in forma orale**, attraverso il sistema di messagistica vocale registrata integrato sulla piattaforma *web* raggiungibile al seguente *link*: <https://dsit.whistlelink.com/>; ovvero mediante linea telefonica, ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

In proposito, inoltre, si precisa che:

- (a) se per la segnalazione si utilizza una linea telefonica non registrata, la segnalazione potrà documentata per iscritto mediante resoconto dettagliato della conversazione a cura dell'OdV;
- (b) se per la segnalazione si utilizza un sistema di messagistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata mediante registrazione sulla predetta piattaforma;
- (c) quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con l'OdV, essa, previo consenso del segnalante, è documentata a cura dell'OdV mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale.

In tutti i casi di cui alle lettere che precedono, il segnalante può verificare, rettificare o confermare il contenuto della trascrizione, mediante la propria sottoscrizione.

- (ii) **in forma scritta**, attraverso la piattaforma *web* raggiungibile al seguente indirizzo *link*: <https://dsit.whistlelink.com/>.

Qualora uno dei Dipendenti lo desideri, potrà riferire la segnalazione al suo diretto superiore (o al suo riporto), o a uno dei componenti degli Organi Sociali, il quale dovrà trasmettere la suddetta segnalazione all'Organismo di Vigilanza entro 7 (sette) giorni dal suo ricevimento, dando contestuale notizia di trasmissione al segnalante. In caso di mancata canalizzazione verso l'OdV da parte del superiore gerarchico o del componente dell'Organo Sociale, il Dipendente dovrà provvedere ad effettuare la segnalazione direttamente all'OdV.

In aggiunta ai principi generali stabiliti nella presente Parte Generale, la Società ha adottato apposite procedure al fine di meglio precisare e disciplinare i flussi di informazione, comunicazione e segnalazione da e verso l'OdV, oltre che un'apposita procedura in merito alle segnalazioni a cui si rinvia.

4.9. **Obblighi di riservatezza.**

L'Organismo di Vigilanza assicura la riservatezza delle informazioni e delle segnalazioni di cui venga in possesso. Più in particolare, l'OdV garantisce la riservatezza dell'identità del segnalante, del soggetto coinvolto e/o del soggetto menzionato nella segnalazione, di qualsiasi altro soggetto che potrà direttamente o indirettamente essere identificato dalle segnalazioni e/o informazioni, del contenuto della segnalazione e della relativa documentazione³⁶.

³⁶ Così come previsto dal decreto legislativo del 10 marzo 2023, n. 24.

In tal senso, l'identità del segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità non possono dall'OdV essere rivelate, senza il consenso espresso del segnalante stesso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi della Normativa Privacy.

Inoltre, si precisa che l'identità del segnalante, nell'ambito del procedimento disciplinare, 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 sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del segnalante alla rivelazione della propria identità. In tal caso, è dato avviso al segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, nonché nelle procedure di segnalazione interna ed esterna quando la rivelazione dell'identità del segnalante e delle informazioni è indispensabile anche ai fini della difesa della persona coinvolta.

L'OdV si astiene, altresì, dall'utilizzare informazioni riservate per fini diversi da quelli di cui al precedente paragrafo e comunque per scopi non conformi alle funzioni proprie di un Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione. Le segnalazioni, pertanto, non verranno utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

L'inosservanza degli obblighi previsti dal presente Modello da parte dell'OdV costituisce giusta causa di revoca della carica.

4.10. Gestione delle segnalazioni da parte dell'Organismo di Vigilanza.

L'OdV, in caso di ricezione di una segnalazione ai sensi del paragrafo 4.8 che precede, provvede a rilasciare al segnalante entro 7 (sette) giorni dalla data di ricezione un avviso di ricevimento e, senza indugio e con la dovuta diligenza, verifica la fondatezza della segnalazione, mantenendo le interlocuzioni con il segnalante, al quale potrà richiedere se necessario delle integrazioni.

Inoltre, l'OdV potrà porre in essere tutte le attività che ritenga opportune, ivi compreso l'avvalersi della collaborazione delle competenti strutture aziendali e l'audizione del responsabile della presunta violazione e/o di eventuali altri soggetti che possano riferire sui fatti segnalati, nel rispetto in ogni caso delle garanzie di riservatezza.

A seguito della verifica, qualsiasi sia l'esito della stessa, l'OdV fornisce riscontro al segnalante. Tale riscontro deve comunque in ogni caso essergli fornito entro 3 (tre) mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro 3 (tre) mesi dalla scadenza del suddetto termine di 7 (sette) giorni dalla presentazione della segnalazione.

Nel caso in cui, all'esito dell'attività di verifica, la segnalazione risulti fondata, l'Organismo di Vigilanza provvederà, tenuto conto della natura della segnalazione, a:

- i) comunicare l'esito dell'accertamento al soggetto responsabile della struttura aziendale a cui appartiene l'autore della violazione accertata, per i provvedimenti di competenza, ivi compresi i provvedimenti disciplinari ove ne sussistano i relativi presupposti;

- ii) comunicare l'esito dell'accertamento al vertice societario per consentire ogni ulteriore azione che si rendesse necessaria al fine di tutelare gli interessi della Società;
- iii) suggerire, ove pertinente, alla Società la presentazione di denunce alle autorità competenti.

Per informazioni e regole più dettagliate si rinvia alle apposite procedure aziendali adottate dalla Società, ove sono indicate anche le modalità di raccolta e conservazione della documentazione e delle segnalazioni da parte dell'OdV.

4.11. Whistleblowing: la tutela del dipendente e/o del collaboratore che segnala illeciti.

Le segnalazioni relative a condotte illecite rilevanti ai sensi del Decreto e/o a violazioni del Modello, nei termini dettagliati nell'apposita procedura aziendale adottata dalla Società in tema di sistema interno di segnalazione delle violazioni, rientrano nell'alveo delle disposizioni normative previste in materia di *whistleblowing*³⁷ di cui al decreto legislativo 10 marzo 2023, n. 24, precisandosi inoltre che l'OdV è stato nominato quale gestore dei canali di segnalazione interna *ex* articolo 4 dello predetto decreto.

La procedura aziendale adottata in tema di sistema interno di segnalazione di violazioni, che costituisce parte integrante del Modello, è conforme al suddetto decreto in materia di c.d. *whistleblowing*, e ad essa si rinvia per maggiori dettagli ed informazioni in proposito. Tale procedura è esposta e resa facilmente visibile a tutti i Destinatari, tra l'altro, nel sito *internet* di proprietà della Società.

Qui si precisa, in linea generale, che è vietato porre in essere atti di ritorsione o discriminazione, diretti o indiretti, nei confronti del segnalante (o *whistleblower*) per motivi collegati direttamente o indirettamente alla segnalazione, in ossequio alle disposizioni normative di cui agli articoli 16 e seguenti del decreto legislativo 10 marzo 2023, n. 24.

L'adozione di misure ritorsive e discriminatorie nei confronti dei soggetti che abbiano effettuato delle segnalazioni può essere denunciata all'Ispettorato Nazionale del Lavoro, per i provvedimenti di relativa competenza, oltre che dal segnalante, anche dall'organizzazione sindacale.

A tal riguardo, si precisa che, in conformità alle disposizioni vigenti, il licenziamento ritorsivo o discriminatorio del soggetto segnalante è da ritenersi nullo, come allo stesso modo sono nulli il mutamento di mansioni, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante medesimo.

L'onere della prova grava sul datore di lavoro, il quale dovrà dimostrare che, in caso di controversie legate all'irrogazione di sanzioni disciplinari o a demansionamenti, licenziamenti, trasferimenti ovvero sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi (diretti o indiretti) sulle condizioni di lavoro, successivi alla presentazione della segnalazione, tali misure siano fondate su ragioni estranee alla segnalazione stessa.

Eventuali violazioni delle misure a tutela del *whistleblower* o segnalazioni infondate effettuate con dolo o colpa grave saranno sanzionate in conformità alle disposizioni di cui al successivo capitolo 6 "*Sistema Sanzionatorio*".

³⁷ Così come modificata dal decreto legislativo 10 marzo 2023, n. 24.

CAPITOLO 5.

La formazione delle risorse e la diffusione del Modello.

5.1. Formazione ed informazione dei Dipendenti.

Ai fini dell'efficacia del presente Modello, è preciso obiettivo di Digital Solutions quello di garantire una corretta conoscenza delle regole di condotta ivi contenute, sia alle risorse già presenti in Società sia a quelle future.

Il livello di conoscenza è realizzato con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

5.1.1. La comunicazione iniziale.

L'adozione del presente Modello è comunicata a tutti i Dipendenti presenti in azienda al momento della sua adozione. Ai nuovi assunti, invece, viene consegnato un *set* informativo (ad esempio CCNL, Modello, Decreto, Codice Etico, eccetera), con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

5.1.2. La formazione.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al Decreto è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i Destinatari funzioni di rappresentanza della Società.

In particolare, Digital Solutions cura l'adozione e l'attuazione di un adeguato livello di formazione mediante idonei strumenti di diffusione e, in particolare attraverso:

- a) *meeting* aziendali;
- b) corsi istituzionali (in aula ovvero *web-based*) aventi ad oggetto specifiche Attività Sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'OdV avvalendosi della collaborazione degli incaricati della gestione delle risorse umane o di Consulenti esterni.

La mancata partecipazione all'attività di formazione senza giustificazione da parte dei Dipendenti costituisce una violazione dei principi contenuti nel presente Modello e, pertanto, sarà sanzionata ai sensi di quanto indicato nel capitolo 6 che segue.

5.2. Informazione dei Consulenti, Partner e Fornitori.

Relativamente ai Consulenti, ai Partner e ai Fornitori, gli stessi devono essere informati al momento della stipula del relativo contratto, anche attraverso la previsione di specifiche clausole contrattuali, che Digital Solutions ha adottato il presente Modello e il Codice Etico e quali sono i principi fondamentali a cui gli stessi si ispirano e le conseguenze in caso di loro violazione.

CAPITOLO 6.

Sistema sanzionatorio.

6.1. Funzione del sistema sanzionatorio.

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabile in caso di violazione delle regole di cui al presente Modello rende effettiva l'azione di vigilanza dell'OdV e ha lo scopo di garantirne l'efficace attuazione.

La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'articolo 6, comma 1, lettera e), del Decreto, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della Società.

L'applicazione del sistema sanzionatorio e dei relativi provvedimenti è indipendente dallo svolgimento e dall'esito del procedimento penale che l'autorità giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto.

Il presente capitolo contiene la descrizione delle misure sanzionatorie adottate dalla Società in caso di violazione del Modello da parte dei Destinatari, in coordinamento con il sistema disciplinare di cui al CCNL e di cui all'articolo 21 del decreto legislativo 10 marzo 2023, n. 24, nel rispetto delle procedure previste dall'articolo 7 dello Statuto dei Lavoratori.

6.2. Dipendenti soggetti al CCNL - Sistema sanzionatorio.

I comportamenti tenuti dai Dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari.

Con riferimento alle sanzioni irrogabili nei riguardi di detti Dipendenti, esse saranno irrogate nel rispetto delle procedure di cui all'articolo 7 dello Statuto dei Lavoratori ed eventuali normative speciali applicabili.

In relazione a quanto sopra, il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui al CCNL.

Tali categorie descrivono i comportamenti sanzionati a seconda del rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

In particolare, si prevede che:

- a) **incombe nei provvedimenti di rimprovero verbale o scritto il Dipendente e/o Lavoratore che violi le procedure interne e/o le regole previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di dare comunicazione all'OdV delle informazioni prescritte, ometta di svolgere controlli, eccetera) o adotti, nell'espletamento delle Attività Sensibili, un comportamento non conforme alle prescrizioni del Modello stesso;**

- b) **incorre nel provvedimento della multa sino a 3 (tre) ore di lavoro il Dipendente e/o Lavoratore che** violi più volte le procedure interne e/o le regole previste dal presente Modello o adottati, nell'espletamento delle Attività Sensibili, un comportamento più volte non conforme alle prescrizioni del Modello stesso, prima ancora che dette mancanze siano state singolarmente accertate e contestate;
- c) **incorre nel provvedimento della sospensione dal servizio e dalla retribuzione sino a 3 (tre) giorni il Dipendente e/o Lavoratore che,** nel violare le procedure interne e/o le regole previste dal presente Modello o adottando, nell'espletamento delle Attività Sensibili, un comportamento non conforme alle prescrizioni del Modello stesso, ovvero compiendo atti contrari all'interesse di Digital Solutions, arrechi danno alla Società o la esponga a una situazione oggettiva di pericolo per l'integrità dei beni dell'azienda;
- d) **incorre nel provvedimento del licenziamento con indennità sostitutiva del preavviso il Dipendente e/o Lavoratore che** adotti, nell'espletamento delle Attività Sensibili, un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un Reato o di un illecito, dovendosi ravvisare in tale comportamento la determinazione di un danno notevole o di una situazione di notevole pregiudizio.
- e) **incorre nel provvedimento del licenziamento senza preavviso il Dipendente e/o Lavoratore che,** nel violare le procedure interne previste dal Modello, ovvero adottando, nell'espletamento delle Attività Sensibili, un comportamento palesemente in violazione alle prescrizioni del presente Modello, determini la concreta applicazione a carico della Società delle misure previste dal Decreto, dovendosi ravvisare in tale comportamento il compimento di atti tali da far venire meno radicalmente la fiducia della Società nei suoi confronti.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, saranno applicate, ai sensi di quanto previsto dal codice disciplinare aziendale vigente in Digital Solutions, in relazione:

- i) all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- ii) al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- iii) alle mansioni;
- iv) alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- v) alle altre particolari circostanze che accompagnano la violazione disciplinare.

È fatta salva la possibilità per la Società di chiedere il risarcimento dei danni derivante dalla violazione del Modello da parte del lavoratore. Tale risarcimento, ove eventualmente richiesto, sarà commisurato:

- i) al livello di responsabilità del lavoratore autore dell'illecito;
- ii) al grado di intenzionalità del comportamento del lavoratore;
- iii) all'eventuale esistenza di precedenti disciplinari a carico dello stesso;

- iv) alla gravità degli effetti della condotta censurata, con ciò intendendosi il livello di rischio cui la Società ragionevolmente ritiene di essere stata esposta (ai sensi e per gli effetti del Decreto) a seguito della commissione della violazione.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, alla direzione aziendale e, pertanto, responsabili ultimi della concreta applicazione delle misure disciplinari sopra descritte sono i soggetti aziendali a ciò delegati, i quali commineranno le sanzioni su eventuale segnalazione dell'Organismo di Vigilanza, sentito, ove opportuno, anche il parere del superiore gerarchico dell'autore della condotta censurata.

È in ogni caso attribuito all'Organismo di Vigilanza, in collaborazione con le funzioni aziendali preposte, il compito di verificare e valutare l'idoneità del sistema disciplinare ai sensi e per gli effetti del Decreto.

6.3. Misure nei confronti dei dirigenti.

In caso di violazione, da parte di Dipendenti che ricoprono la qualifica di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso, la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dalla legge e dalla contrattazione collettiva applicabile, tra cui la risoluzione del rapporto di lavoro.

6.4. Misure nei confronti degli amministratori.

In caso di violazione del Modello da parte dell'organo amministrativo della Società o di uno dei suoi componenti, l'OdV informa l'Assemblea e l'intero Consiglio di Amministrazione, i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa.

In caso di accertata violazione da parte dell'organo amministrativo della Società o di uno dei suoi componenti, sono applicabili le seguenti misure:

- i) censura e/o richiamo formale;
- ii) revoca della carica.

La misura di cui al precedente punto ii) dovrà essere in ogni caso applicata alla stregua del combinato disposto degli articoli 2475 e 2383 del codice civile.

6.5. Misure nei confronti dei membri dell'OdV.

In caso di violazione del presente Modello da parte dell'OdV ovvero da parte di uno o più membri dell'OdV, gli altri membri dell'OdV ovvero uno tra i membri dell'organo di controllo (ove nominato) della Società o tra i membri dell'organo amministrativo, informerà immediatamente l'Assemblea e il Consiglio di Amministrazione, i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che hanno violato il Modello e la conseguente nomina di nuovi membri in sostituzione degli stessi, ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

6.6. Misure nei confronti dei Consulenti, *Partner* e Fornitori.

Ogni violazione da parte dei Consulenti, dei *Partner* e dei Fornitori delle regole di cui al presente Modello agli stessi applicabili o di commissione dei Reati è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte dell'autorità giudiziaria delle misure previste dal Decreto.

CAPITOLO 7.

Verifiche sull'adeguatezza del Modello.

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei Destinatari ed il Modello stesso), lo stesso periodicamente effettua specifiche verifiche sulla reale capacità del Modello di prevenire la commissione dei Reati.

Tale attività si concretizza, tra le altre cose, in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi o negoziati da Digital Solutions in relazione alle Attività Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.

Inoltre, con verifiche a campione, viene svolta una *review* di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV, degli eventi considerati rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa.

Per le verifiche l'OdV si avvale, di norma, anche del supporto di quelle funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Le verifiche e il loro esito sono oggetto del *report* annuale di cui al paragrafo 4.6. In particolare, in caso di esito negativo delle verifiche espletate, l'OdV esporrà, nel piano relativo all'attività per l'anno successivo, le proposte di miglioramenti da attuare.