FONDAMENTA S.P.A.

REVISIONE 2023

MODELLO ORGANIZZATIVO E DI GESTIONE

PARTE I

SOMMARIO

INTRODUZIONE

L'IMPEGNO DI CONFORMITÀ (COMPLIANCE COMMITMENT)

I principi di trasparenza e legalità sono, oggi, tra i pilastri portanti della gestione di qualsiasi organizzazione. Gli ordinamenti giuridici, gli stakeholders, richiedono agli attori della "società civile" di rispettare tali principi e di essere in grado di provarli. In talune particolari situazioni, ritenute dai legislatori particolarmente rilevanti per la coscienza comune, tale principio di responsabilizzazione si traduce addirittura nell'inversione dell'onere della prova a carico dell'attore. Queste istanze richiedono che la gestione delle organizzazioni sia improntata ad un approccio al rischio considerato sotto il profilo dell'impatto non solo all'interno dell'organizzazione, ma anche rispetto a tutti coloro i quali interagiscono, direttamente o indirettamente con l'organizzazione (dipendenti, clienti, fornitori, soci, ecc…) e gli interessi pubblici. Lo standard internazionale ISO 31022:2020 definisce il "rischio legale" come l'effetto dell'incertezza sugli obiettivi dell'organizzazione in materia legale, regolamentare, contrattuale. Questo Modello di Organizzazione e Gestione, altresì più brevemente definito "Modello", raccoglie e testimonia le informazioni, le analisi, le valutazioni, le soluzioni e le scelte che la società Fondamenta S.p.A. ha adottato per rispettare i requisiti di conformità dalla stessa individuati quale "Impegno di conformità" e precisamente, quelli relativi:

- al D.Lgs. 231/2001 e successive modifiche ed integrazioni sino ad oggi;

- al Reg. UE 679/2016 (GDPR) e la disciplina nazionale e comunitaria ad esso collegata come successivamente integrati e modificati sino ad oggi.

IL D.LGS. 231/2001

Il D.Lgs. 231/2001 è stato emanato per effetto della delega al Governo prevista dalla L. 29/9/2000 n. 300 di recepimento, tra gli altri, della Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, fatta a Bruxelles il 26/5/1997 e della Convenzione OCSE

sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali fatta a Parigi il 17/12/1997.

Tale norma ha innovato il principio secondo cui le persone giuridiche non potevano delinquere e, conseguentemente, non potevano essere punite.

I fatti dimostravano che un sistema concernente la criminalità delle imprese, basato e limitato esclusivamente attorno alle persone fisiche, comportava una perdita di garanzia.

La mancata espressa previsione di una forma di responsabilità della persona giuridica, per effetto di comportamenti illeciti commessi dalle persone fisiche, in linea o comunque dipendenti dalla politica aziendale, infatti, determinava, di fatto, l'insensibilità delle persone giuridiche ai deterrenti contenuti nelle norme penali.

Dal 2001 il D.Lgs. 231/2001 si è comportato come un "contenitore" ove sono stati collocati, nel tempo, reati socialmente rilevanti, così accanto agli originari reati in danno alle Pubbliche Amministrazioni (malversazione, indebita percezione, truffa, concussione, corruzione), si sono aggiunti i reati di falso nummario, i reati societari, i reati con finalità di terrorismo od eversione dell'ordine democratico …

La responsabilità dell'Ente nasce da difetti di organizzazione, tanto che si semplifica definendo la responsabilità dell'Ente come l'effetto della deficienza organizzativa.

L'art. 5 della norma definisce l'ambito di responsabilità dell'Ente:

"*1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:*

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; (Soggetti Apicali)

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (Sottoposti).

2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi."

Il successivo articolo 6 precisa:

"*1. Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a)* (Soggetti Apicali), *l'ente non risponde se prova che:*

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di

organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)."

Riguardo, poi, i soggetti sottoposti il successivo articolo 7 stabilisce:

"1. Nel caso previsto dall'articolo 5, comma 1, lettera b) (Sottoposti), *l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.*

2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.".

L'ente, dunque, per non assumere la responsabilità prevista dalla norma, deve dotarsi di un sistema organizzativo che sia in grado di prevenire e ridurre al minimo la possibilità che siano commessi i reati previsti dalla norma da soggetti Apicali o da sottoposti.

IL REGOLAMENTO EUROPEO 679/2016

Il Regolamento Europeo 679/2016, di seguito altresì definito GDPR, disciplina la protezione dei dati personali integrando ed assorbendo le norme nazionali.

L'art. 5 del GDPR elenca i principi che devono essere rispettati nel trattamento dei dati personali ed al paragrafo 2 precisa che spetta al titolare del trattamento rispettarli ed essere in grado di comprovarlo («responsabilizzazione»).

Il successivo art. 24 del GDPR è ancora più esplicito stabilendo testualmente:

"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

Il Documento di Conformità è la sezione di questo Modello che persegue lo scopo di

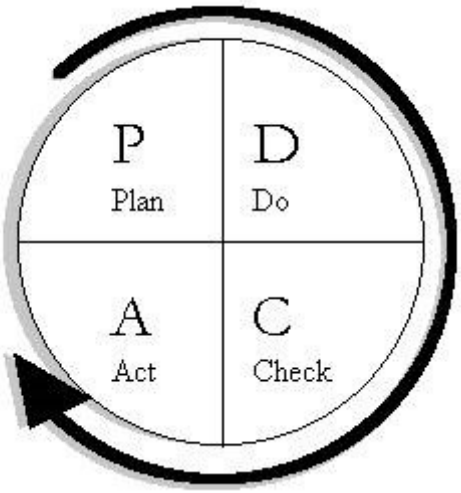
fornire la base documentale per progettare, definire, impostare e condurre un sistema di gestione conforme dei trattamenti di dati personali svolti dalla società Fondamenta S.p.A. sia nella sua veste di Titolare del trattamento, che quale Responsabile del trattamento.

IL PROCESSO DI GESTIONE DELLA CONFORMITÀ - PGC

Col termine "PGC" si intende il complesso di attività, conoscenze e risorse che sono organizzate tra loro in modo da soddisfare al meglio l'impegno di conformità assunto dall'Ente.

Si tratta di un processo ciclico che deve essere avviato dall'organo dirigente (Art.6 comma1 lett.a) D.Lgs. 231/2001 – Art.24 GDPR) e, quindi, mantenuto aggiornato ed efficacemente attuato anche attraverso la vigilanza ed impulso di funzioni di vigilanza quali l'Organismo di Vigilanza – OdV – (Art.6 comma 1 lett.b) D.Lgs.231/2001) ed il Privacy Manager.

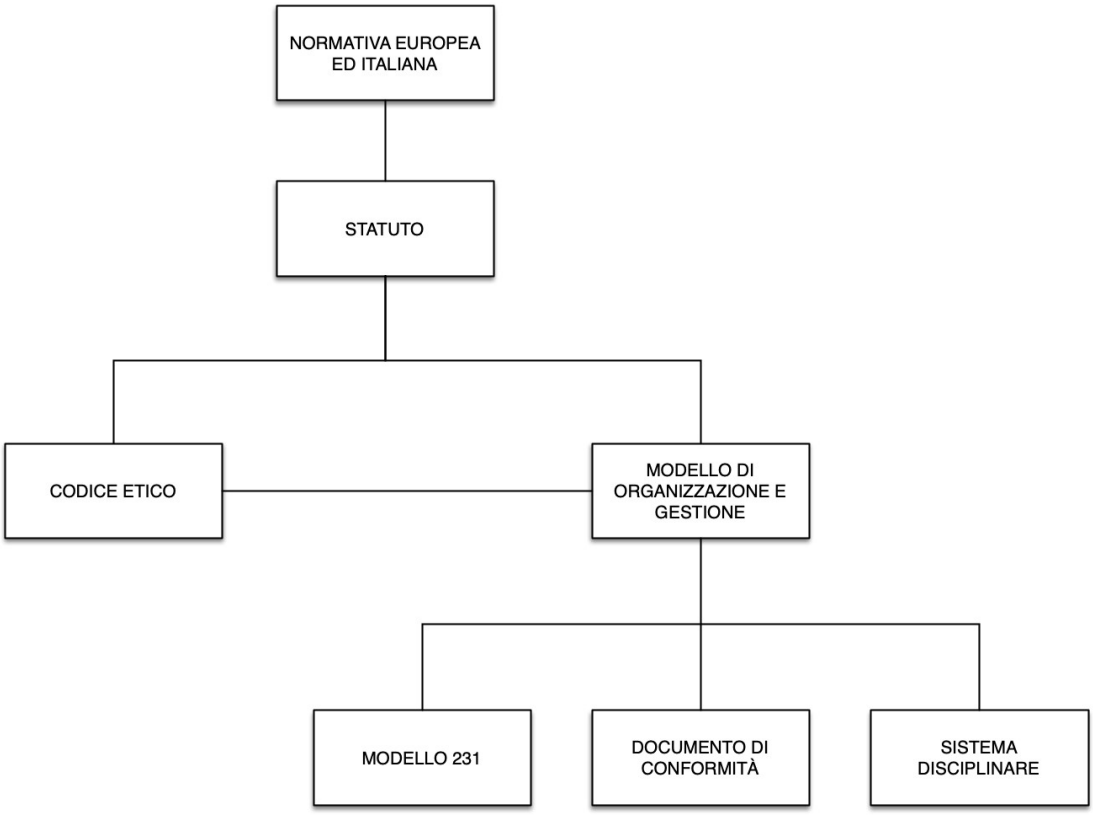
Il funzionamento del processo può ben essere descritto attraverso il noto ciclo di Deming (che, peraltro, è alla base degli standard di risk management)



IL MODELLO DI ORGANIZZAZIONE E GESTIONE - MOG

Lo schema che segue illustra sinteticamente la gerarchia delle fonti cui si ispira il Modello ed il sistema documentale adottato dall'ente.

SCHEMA GERARCHIA DELLE FONTI



Il documento che segue è il Modello di Organizzazione e Gestione predisposto ed approvato dalla società dalla società Fondamenta S.p.A. per rispettare l'impegno di conformità assunto rispetto al D.Lgs. 231/2001 ed alla vigente disciplina in materia di

protezione dei dati personali – GDPR.

Esso si compone delle parti che seguono:

I) la **prima parte** contiene le enunciazioni di carattere generale e di contenuto programmatico. Essa si divide in due sezioni:
   a. la prima sezione è intitolata "Dichiarazioni" in essa sono contenute le informazioni che descrivono l'ambiente in cui è stato sviluppato il Modello;
   b. la seconda sezione si intitola "Principi" e contiene i principi generali che guidano l'organizzazione dell'Ente coerentemente a quanto stabilito nel Codice Etico, e nel rispetto dell'ordinamento giuridico italiano.

II) La **seconda parte** contiene la parte di analisi e si divide in due sezioni:
   a. la prima sezione è intitolata "Ricognizione", essa contiene i dati, forniti dall'Ente che formano lo "Scenario dei Rischi" sul quale sono svolte l'analisi dei rischi.
   b. La seconda sezione è intitolata "Analisi", essa contiene la parte di analisi dei rischi relativa all'Impegno di Conformità adottato dalla Società. Al momento essa è divisa nei seguenti Titoli:
      i. Titolo 1; contiene i principi generali che regolano l'analisi dei rischi.
      ii. Titolo 2; contiene la parte di analisi dei rischi inerente al D.Lgs. 231/2001 arricchendo lo scenario della prima sezione con le particolari informazioni necessarie alla specifica analisi. In questa sezione è contenuto l'elenco dei rischi e le tabelle di collocazione e valutazione.
      iii. Titolo 3; contiene la parte di analisi dei rischi inerente alla conformità al vigente normativa in materia di Protezione dei Dati Personali arricchendo lo scenario della prima sezione con le particolari informazioni necessarie alla specifica analisi. In questa

sezione è contenuto l'elenco dei rischi e le tabelle di collocazione e valutazione.

III) La **terza parte**, contiene gli allegati, ovvero la documentazione rilevante in materia di supporto ad una corretta organizzazione dell'ente e si divide in sette sezioni:

a. Codice Etico, contiene i principi etici che guidano in ogni attività l'ente.
b. Processo di conformità, contiene i principi e le regole per la gestione e mantenimento del sistema di conformità.
c. Codici di comportamento, contiene i codici che, declinando il Codice Etico, fissano le regole per i comportamenti corretti da tenere in situazioni potenzialmente critiche.
d. Documenti di attuazione 231, contiene le procedure e la documentazione a livello di gestione ed operativo, rilevanti per la corretta ed efficace attuazione del Modello di Organizzazione e Gestione rispetto ai rischi connessi ai reati contemplati dal D.Lgs 231/2001.
e. Procedure di attuazione Privacy, contiene le procedure e la documentazione a livello di gestione ed operativo, rilevanti per la corretta ed efficace attuazione del Modello di Organizzazione e Gestione rispetto ai rischi della protezione dei dati personali.
f. Sistema di vigilanza, contiene le disposizioni che regolano le funzioni di vigilanza.
g. Sistema disciplinare, contiene le disposizioni rilevanti a tutela del rispetto del Modello di Organizzazione e Gestione.

IV) La **quarta parte**, infine, è destinata a contenere gli aggiornamenti che cambiamenti rilevanti esterni (p.es. novità legislative) od interni (p.es. riorganizzazioni) richiederanno di apportare al Modello perché esso sia coerente e soddisfi i requisiti di idoneità.

Le parti sono tra loro inscindibili e, unitariamente, costituiscono il Modello Organizzativo e di Gestione.

DEFINIZIONI

Qui sono contenute, in ordine alfabetico, le definizioni dei termini più significativi utilizzati nel presente documento.

AUTENTICITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere riconducibili a chi le produce o le approva.

AUTORIZZATI, si intendono tutti coloro i quali prestando la propria opera a favore dell'ente, sono stati autorizzati al trattamento di dati personali (essi corrispondono alla categoria degli "incaricati del trattamento" nella previgente disciplina).

CIS, si intende il Center for Internet Security.

CODICE, si intende il D.Lgs. 196/2003 come riformato dal D.Lgs. 101/2018.

DANNO, si intende l'impatto prodotto dall'avveramento di un rischio sull'ente ed i suoi stakeholders.

DATI, si intende ogni informazione nella sua accezione più ampia, indipendentemente dal formato o dal supporto su cui essa è contenuta, sia in forma sciolta che aggregata.

DESIGNATI, si intendono coloro che, persone fisiche, a norma dell'art. 2-quaterdecies del Codice, sotto la responsabilità ed autorità del titolare, società Fondamenta S.p.A. e, nell'ambito del suo assetto organizzativo, svolgono specifici compiti e funzioni connessi al trattamento di dati personali in virtù di espressa designazione (essi corrispondono alla categoria dei "responsabili interni del trattamento" nella previgente disciplina.

DISPONIBILITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni, quando occorrono, devono essere a disposizione di chi ne ha diritto.

DPO, si intende il Data Protection Officer, è l'acronimo inglese del Responsabile della Protezione dei Dati ovvero della figura prevista dall'art. 37 del Regolamento Europeo 679/2016.

EDPB, si intende lo European Data Protection Board, ovvero il Comitato Europeo per la Protezione dei Dati.

ENISA, si intende la European Union Agency for Network and Information Security.

GARANTE, si intende il Garante per la Protezione dei Dati Personali, ovvero l'Autorità di Controllo italiana.

GDPR, si intende il General Data protection Regulation, è l'acronimo inglese del Regolamento Europeo 679/2016.

GDPD, si intende il Garante per la Protezione dei Dati Personali, è l'acronimo italiano che individua l'Autorità di Controllo nazionale.

INTEGRITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere integre, esatte ed aggiornate.

MINACCIA, si intendono quegli eventi che, associati a debolezze (vulnerabilità) dell'ente, permettono l'avverarsi di un rischio; la minaccia si esprime in probabilità di accadimento.

MODELLO DI ORGANIZZAZIONE E GESTIONE (MOG), si intende il

documento che definisce e formalizza gli obiettivi, i principi, i presupposti e le attività organizzative che l'ente, in conformità all'art.6 del D.Lgs. 231/2001 adotta ed attua al fine di ridurre al minimo il rischio che soggetti da esso dipendenti (sia Apicali che Sottoposti) possano commettere reati delle specie previste dal D.Lgs. 231/2001 nell'interesse od a vantaggio dell'ente medesimo.

ORGANISMO DI VIGILANZA (OdV), si intende l'organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo, cui l'organo dirigente ha affidato il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento in conformità a quanto previsto dall'art.6 comma 1 lett.b) del D.Lgs. 231/2001.

PRIVACY MANAGER, si intende la persona cui è affidata la responsabilità di condurre e mantenere il processo di conformità dei trattamenti dei dati personali.

PROCESSO, si intende il complesso di attività e risorse tra loro organizzate al fine di produrre un determinato output partendo da un determinato input.

QUOTE, si tratta del sistema sanzionato rio previsto dall'art. 10 del D.Lgs. 231/2001.

REGOLAMENTO, si intende il Regolamento Europeo 679/2016.

RESPONSABILE DEL TRATTAMENTO, si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi dell'art. 28 del regolamento.

RGPD, si intende il Regolamento Generale della Protezione dei Dati, è l'acronimo italiano del Regolamento Europeo 679/2016.

RISCHIO, si intende la possibilità che un evento non desiderato si attui arrecando un danno all'ente.

RISERVATEZZA, si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere conosciute solo da coloro che ne hanno diritto.

RPD, si intende il Responsabile della Protezione dei Dati, è l'acronimo italiano della figura prevista dall'art. 37 del Regolamento Europeo 679/2016.

SISTEMA INFORMATIVO (SI), il complesso delle risorse (risorse umane, tecnologia, applicazioni, infrastrutture, dati) organizzate dall' azienda per il trattamento delle informazioni in genere e dei dati personali in modo specifico.

SISTEMA INFORMATIVO DI VIGILANZA (SIV), il documento che definisce il contenuto delle informazioni che obbligatoriamente devono essere trasmesse all'organismo di vigilanza, individuando compiti e responsabilità.

SOGGETTI APICALI, si intendono le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché le persone che esercitano, anche di fatto, la gestione ed il controllo dell'ente medesimo, secondo quanto previsto dall'art. 5 comma 1 lett. a) del D.Lgs. 231/2001.

SOGGETTI SOTTOPOSTI, si intendono le persone sottoposte alla direzione o alla vigilanza di un soggetto apicale, così come definito dall'art.5 comma 1 lett. b) del D.Lgs. 231/2001.

VULNERABILITA', si intende la debolezza dell'ente rispetto specifiche ipotesi di rischio; attraverso tali debolezze le minacce determinano l'avverarsi dei rischi.

WP29, si intende il Working Party article 29, ora EDPB.

PARTE I

SEZIONE I - DICHIARAZIONI

I dati che seguono sono stati ricavati dalle interviste con gli organi ed il personale dell'ente nonché da documenti forniti dagli stessi interessati.

I.1. ENTE

L'Ente che adotta e si impegna ad efficacemente attuare il presente Modello di Organizzazione è la società Fondamenta S.p.A., Titolare del trattamento dei dati personali, con sede legale in via Turati, 26, Milano; cap. 20121; P. IVA: 01543610180; tel. 02 29001647; fax. 02 29012417; email info@fondamentaspa.it; pec fondamentaspa@postacertificata.com.

I.2. RAPPRESENTANZA LEGALE

La rappresentanza dell'Ente di fronte ai terzi ed in giudizio spetta al Presidente del Consiglio di Amministrazione Ing. Giulio Borelli.

I.3. NATURA E DESCRIZIONE

Fondamenta S.p.A. nasce nel 1993 come evoluzione della Sogefon S.p.A., società specializzata sino dal 1963 nelle opere in sottosuolo, e incorpora la Penati e la Titania, importanti e storiche società del settore.
Sin dalla nascita Fondamenta opera nel campo delle fondazioni in tutti i settori delle costruzioni.

Nel 2006 Fondamenta incorpora per fusione la Sogefon S.p.A. in quanto l'attività delle due società è diventata sempre più complementare e simile ed un'unica società è in grado di dare alle imprese un servizio più completo come varietà di lavori ed elasticità nella loro esecuzione.

L'azienda, che fino ad oggi ha completato oltre 1000 commesse, ha lavorato nelle più importanti infrastrutture italiane (strade, autostrade, ferrovie, aeroporti, metropolitane etc) e nelle più importanti opere civili e di edilizia sia pubblica che privata (centri commerciali, ospedali, edilizia residenziale etc).

I.4. LA MISSIONE

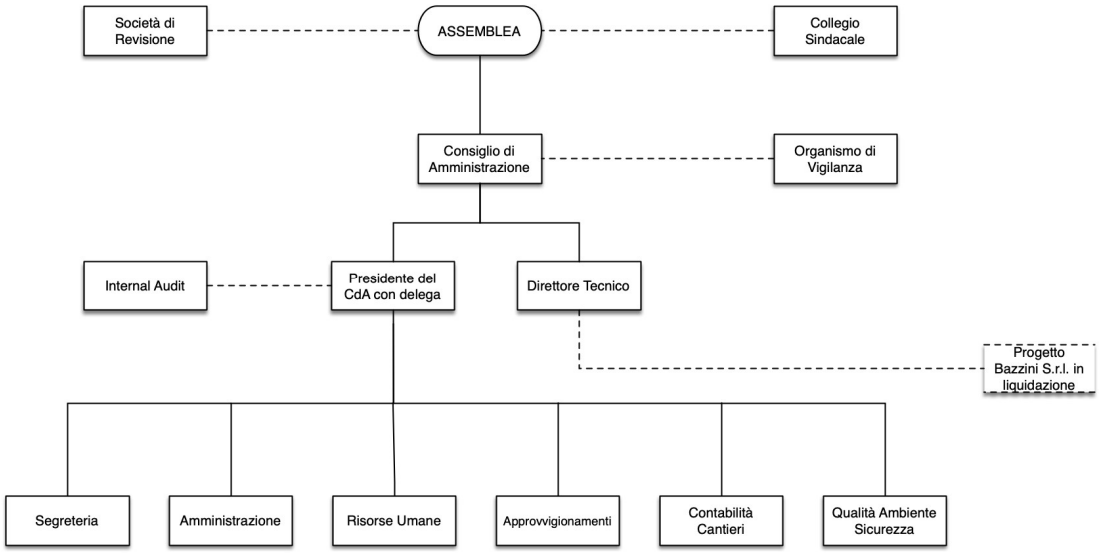
Da sempre Fondamenta opera esclusivamente con proprie maestranze ed attrezzature coprendo l'intera gamma delle opere specialistiche del sottosuolo, l'intera gestione degli scavi e delle impermeabilizzazioni, le opere di fondazione in calcestruzzo e, grazie alla cinquantennale esperienza e la costante formazione del personale e il continuo adeguamento del macchinario all'evolversi tecnologico del settore, può intervenire sempre con grande efficienza e con la garanzia di un ottimo risultato.

I.5. AMMINISTRAZIONE

La Società è amministrata da un Consiglio di Amministrazione come previsto dallo Statuto. Il Consiglio di Amministrazione è investito dei più ampi poteri per l'amministrazione ordinaria e straordinaria della società. Esso ha facoltà di compiere tutti gli atti anche di disposizione che ritiene opportuni per il conseguimento dell'oggetto sociale, esclusi soltanto quelli che la legge espressamente riserva all'assemblea dei soci. La rappresentanza della società difronte ai terzi ed in giudizio spetta al presidente del Consiglio di Amministrazione.

I.6. MAPPA ORGANIZZATIVA

Si precisa che la mappa che segue ha funzione meramente schematica ed è esclusivamente finalizzata alla analisi che è alla base di questo Modello, per alcuna ragione può essere considerata "organigramma" o "funzionigramma" od espressione delle prerogative organizzative proprie del vertice amministrativo.



I.7. CONDIZIONI

L'Ente è vincolato all'osservanza, oltre che della vigente normativa italiana, dello statuto, del codice etico e dei regolamenti interni.

I.8. NORMATIVA

Sono disposizioni mandatorie come risultanti alla data del 31 dicembre 2022:

- il D.Lgs. 231/2001 e successive modificazioni ed integrazioni.
- Il Regolamento Europeo 679/2016.
- Il D.Lgs. 196/2003 Codice della privacy e s.m.i..
- Il Provvedimento del GPDP - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008.
- Il Provvedimento del GDPD - Linee guida del Garante per posta elettronica e internet del 10 marzo 2007.
- Il Provvedimento del GDPD - Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati - 23 novembre 2006.

- Il D.Lgs. 33/2013 in materia di trasparenza.
- Lo EDPB "Guidelines 3/2019 on processing of personal data through video devices" del 29/1/2020.
- Lo EDPB WP243-1 "Guidelines on Data Protection Officers ('DPOs')".
- Lo EDPB WP248-1 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679".
- Lo EDPB WP250 "Guidelines on Personal data breach notification under Regulation 2016/679".
-Lo ENISA "Recommendations for a methodology of the assessment of severity of personal data breaches".
- Lo EDPB WP259-1 "Guidelines on consent under Regulation 2016/679".
- Lo EDPB "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default".

I.9. STANDARDS DI RIFERIMENTO

Al fine di attribuire al Modello la massima obiettività e condivisibilità possibile, sfruttando lo stato dell'arte, esso è ispirato ai seguenti standard, good practice, linee guida:

- ISO 31022:2020 Risk management — Guidelines for the management of legal risk.
- ISO 31000:2018 Risk management – Guidelines.
- ISO 31010:2019 Risk management – Risk assessment techniques.
- ISO/IEC 27001:2013 (Information Security Management Systems) per quanto riguarda gli aspetti di sicurezza del Sistema Informativo.
- ISO 19600:2014 (Compliance Management System) per quanto riguarda i principi di rispetto e conformità cui l'ente è soggetto.
- UNI/PdR 43:2018 Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Gestione e monitoraggio dei dati personali in ambito ICT.
- ISO/IEC 29100:2011 - Privacy Framework.
- ISO/IEC 29134:2017 - Guidelines for privacy impact assessment.

- ISO/IEC 29151:2017 - Code of practice for personally identifiable information protection.
- Linee guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) – UNI-INAIL 2001.
- Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001 – Confindustria 2021.
- Codice di comportamento delle imprese di costruzione – ANCE 2022.

I.10. OBIETTIVI DEL MODELLO

L'Ente si propone quindi di ridurre al minimo i rischi di mancato rispetto di obblighi derivanti da leggi, regolamenti, convenzioni, prassi cui esso è soggetto, con particolare riferimento:

per quanto riguarda i requisiti derivanti dal D.Lgs. 231/2001, che i soggetti da esso dipendenti (sia Apicali che Sottoposti) possano commettere reati delle specie previste dal D.Lgs. 231/2001, nell'interesse od a vantaggio dell'ente medesimo; ciò al fine di rispettare i principi etici che lo ispirano e lo guidano ed al fine di essere sollevato dalla responsabilità prevista dal citato D.Lgs. 231/2001.

Per quanto riguarda i requisiti derivanti dal Regolamento Europeo 679/2016 e la corrispondente normativa nazionale, che siano messe in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento e che dette misure siano riesaminate e aggiornate qualora necessario.

I.11. SCOPO DEL DOCUMENTO

Questo documento ha lo scopo di definire e formalizzare i principi, i presupposti, le attività ed i progetti organizzativi, che l'Ente intende adottare ed attuare al fine di raggiungere l'obiettivo sopra enunciato.

I.13. DATE E TERMINI

Questo Modello Organizzativo e di Gestione è stato revisionato sulla base delle informazioni alla data del 30 aprile 2023.

Esso è approvato dal Consiglio di Amministrazione che ne dispone l'immediata adozione.

Tutti coloro i quali, a qualsiasi titolo ed a qualsiasi livello prestano la propria opera per la società sono tenuti allo scrupoloso rispetto di quanto di seguito stabilito e ciascuno, nei limiti delle proprie competenze e funzioni, è obbligato a darne immediata attuazione.

SEZIONE II – PRINCIPI

Questa sezione contiene i principi, che guidano ed ispirano il presente Modello di organizzazione e gestione e l'agire di tutti coloro i quali operano per la società Fondamenta S.p.A..

II.1. - ETICITA'

L'adozione di principi etici deve essere considerata rilevante sia ai fini della prevenzione dei reati previsti dal D.Lgs. 231/2001, costituendone elemento essenziale del sotto-processo "231", sia ai fini della effettiva ed efficace tutela dei dati personali, come richiesto dal Reg. EU 679/2016 .

La società Fondamenta S.p.A. riconosce l'importanza della responsabilità etico-sociale nella conduzione degli affari e delle attività aziendali impegnandosi al rispetto dei legittimi interessi dei propri stakeholder e della collettività in cui opera.

Non sono etici, e favoriscono l'assunzione di atteggiamenti ostili nei confronti dell'ente, i comportamenti di chiunque, singolo o organizzazione, cerchi di appropriarsi dei benefici della collaborazione altrui, sfruttando posizioni di forza.

In ogni caso il perseguimento dell'interesse dell'ente non può mai giustificare una condotta contraria ai principi di correttezza ed onestà.

II.2. - LEGALITA'

II.2.1. RISPETTO DELLE LEGGI

È condizione imprescindibile di ogni attività dell'ente il rispetto della normativa vigente ed applicabile all'ente. Per normativa si intendono la Costituzione e le Leggi italiane, le disposizioni di pari rango dell'Unione Europea, le Leggi nazionali dei Paesi in cui l'Ente opera.

II.2.2. RISPETTO DEGLI OBBLIGHI DI NATURA NEGOZIALE

La Fondamenta S.p.A. si obbliga altresì a rispettare scrupolosamente tutti gli obblighi derivati da contratti od altri strumenti negoziali di cui è parte. Come pure a rispettare gli altri obblighi legati dal contesto sociale in cui essa opera.

II.2.3. RISPETTO DEL D.Lgs. 231/2001

La Fondamenta S.p.A.si impegna a ridurre i rischi di commissione dei reati previsti dal D.Lgs. 231/2001. La riduzione dei rischi deve essere più bassa possibile ritenendo il rispetto della legge obiettivo prioritario. La revisione ed aggiornamento periodici hanno il fine di restringere il livello di rischio accettabile al più basso possibile e conferire la massima efficacia al Modello di organizzazione e gestione.
Il processo "231" è dettagliatamente descritto nella sezione b) della III Parte di questo documento.

II.2.4. RISPETTO DEL Reg.EU 679/2016

La Fondamenta S.p.A.si impegna a rispettare la disciplina applicabile in materia di protezione dei dati personali come attualmente definita dal Regolamento Europeo 679/2016 e dalla normativa nazionale ad esso collegata mettendo in atto e mantenendo adeguate misure tecniche ed organizzative. La riduzione dei rischi di mancato rispetto, con particolare riferimento ai rischi per i diritti e le libertà delle persone fisiche che

possono derivare dal trattamento dei loro dati personali, deve essere la più bassa possibile ritenendo il rispetto della legge obiettivo prioritario. La revisione ed aggiornamento periodici hanno il fine di restringere il livello di rischio accettabile al più basso possibile e conferire la massima efficacia al Modello di organizzazione e gestione.
Il processo di gestione della conformità (PGC) è dettagliatamente descritto nella sezione b) della III Parte di questo documento.

II.3. - RIGORE

Le disposizioni del presente documento, come pure le disposizioni di legge o di altra natura che sono vincolanti per l'ente devono essere interpretate in maniera rigorosa avendo come guida i fini primari del presente documento che sono il rispetto dei principi etici e delle leggi.
Eventuali deroghe devono essere eccezionali, giustificate da ragioni obiettivi, urgenti, necessarie, ineludibili e deve esserne data comunicazione alle funzioni di vigilanza.
In ogni caso non sono ammesse deroghe che violino norme cogenti.

II.4. - GESTIONE DEI RISCHI

Le attività dell'ente e le scelte conseguenti devono essere condotte con consapevolezza secondo le migliori prassi quali ad esempio lo standard ISO 31000:2018.
Nel gestire i rischi deve essere garantito il rispetto oltre che delle leggi degli interessi degli stakeholders[1], in ogni caso i rischi devono essere gestiti assegnando chiari e specifici poteri e responsabilità.

II.4.1. ANALISI DEI RISCHI

Ogni attività rilevante dell'Ente deve essere preceduta da analisi dei rischi. L'analisi dei rischi deve individuare e descrivere gli scenari di rischio in relazione ai requisiti come sopra definiti nell'Impegno di Conformità. I ruoli, poteri e responsabilità per le analisi dei rischi

[1] Col termine stakeholder si individuano i soggetti sostenitori nei confronti di una iniziativa economica.

devono essere chiaramente e specificamente allocate.

II.4.2. VALUTAZIONE DEI RISCHI

Nella valutazione dei rischi deve essere seguito il massimo rigore, ovvero in caso di indecisione deve essere scelta la soluzione di maggior garanzia tenuto conto dei principi etici e della legge. Il danno deve essere considerato sempre massimo indipendentemente dai criteri di valutazione qualitativi o quantitativi, poiché la commissione di un reato, seppure lieve, non può essere tollerata. La scelta delle contromisure deve essere effettuata in coerenza preferendo tra le misure quelle che offrono le maggiori protezioni e non secondo criteri di mera economicità.

Il "Rischio accettabile" deve essere valutato conformemente ai superiori principi considerando che il sistema di prevenzione deve essere tale da non poter essere aggirato se non fraudolentemente.

II.5. – CORRETTEZZA E TRASPARENZA

Le informazioni che vengono diffuse dall'ente sono complete, trasparenti, comprensibili ed accurate, in considerazione di coloro che sono i destinatari, in modo che questi ultimi possano assumere decisioni consapevoli.

Le informazioni, in considerazione della propria natura, devono soddisfare adeguati livelli di integrità e di disponibilità; alle informazioni destinate a diffusione o che possono avere impatti rilevanti sull'ente, sulle risorse umane, sugli stakeholder deve essere garantito un idoneo livello di autenticità.

Tutte le azioni e le operazioni compiute ed i comportamenti tenuti coloro che operano per l'ente, nello svolgimento del proprio incarico o funzione, devono pertanto essere ispirate a trasparenza, correttezza e reciproco rispetto, nonché alla legittimità sotto l'aspetto sia formale che sostanziale, secondo le norme vigenti e le procedure e regolamenti interni e di gruppo.

II.6. – RISERVATEZZA

L'ente, in conformità alle disposizioni di legge, pur nel rispetto dei principi di trasparenza, garantisce la generale riservatezza delle informazioni in proprio possesso, secondo il principio del "need to know".

A coloro che operano per conto dell'ente è fatto espresso divieto di utilizzare informazioni riservate per scopi non connessi all'esercizio della propria attività professionale anche successivamente alla cessazione del rapporto che li lega all'ente.

II.7. – PREVENZIONE RICICLAGGIO

Qualsiasi attività, direttamente o indirettamente, finalizzata a nascondere la provenienza di denaro o altre risorse economiche della Società o di terzi, ovvero le persone beneficiarie di tali beni, non è consentita né tollerata dalla società Fondamenta S.p.A. perché viola il principio di trasparenza e può essere strumentale alla commissione di reati quali, ad esempio, il riciclaggio, l'autoriciclaggio, il supporto al terrorismo.

II.7. - PROTEZIONE DEI DATI PERSONALI

La società Fondamenta S.p.A. con specifico riferimento alla protezione dei dati personali, nel rigoroso rispetto del Regolamento Europeo 679/2016 nel trattare i dati personali individua ed adotta come propri i seguenti principi.

II.7.1. LICEITÀ

Fondamenta S.p.A. svolge i soli trattamenti di dati personali che si fondano su una delle basi giuridiche di cui all'art. 6 GDPR (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Fondamenta S.p.A. tratta categorie particolari di dati personali, (ovvero dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in

modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), solo se sussiste uno dei casi previsti dall'art. 9.2 GDPR.

Fondamenta S.p.A. tratta i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, solo su una delle basi giuridiche di cui all'articolo 10 GDPR e soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

II.7.2. CORRETTEZZA DEL TRATTAMENTO

Fondamenta S.p.A. tratta i dati personali esclusivamente per scopi determinati, espliciti e legittimi, senza scorrettezze o raggiri nei confronti degli interessati attenendosi rigidamente nei limiti delle basi giuridiche che ne legittimano il trattamento.

II.7.3. TRASPARENZA NEL TRATTAMENTO

Fondamenta S.p.A. adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. In particolare, Fondamenta S.p.A., per ogni trattamento che svolge, rende noto all'interessato le modalità con cui i dati personali sono raccolti, utilizzati, consultati o altrimenti trattati nonché la misura in cui i dati personali sono o saranno trattati. Le informazioni e le comunicazioni relative al trattamento di tali dati personali devono essere facilmente accessibili e comprensibili

II.7.4. LIMITAZIONE DELLA FINALITÀ

Fondamenta S.p.A. tratta i dati personali per finalità determinate, esplicite e legittime, ed assicurandosi che i trattamenti non siano incompatibili con tali finalità.

II.7.5. MINIMIZZAZIONE DEI DATI

Fondamenta S.p.A. tratta dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

II.7.6. ESATTEZZA

Fondamenta S.p.A. tratta dati personali esatti e, se necessario, aggiornati; adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

II.7.7. LIMITAZIONE DELLA CONSERVAZIONE

Fondamenta S.p.A. conserva i dati personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

II.7.8. INTEGRITÀ E RISERVATEZZA

Fondamenta S.p.A. tratta i dati personali in maniera da garantirne un'adeguata sicurezza, proteggendoli, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti o dalla loro perdita, distruzione o da danni accidentali.

II.7. 9. RESPONSABILIZZAZIONE

Fondamenta S.p.A. mette in atto misure adeguate ed efficaci adottando modalità che possano consentire la tracciabilità delle decisioni e delle attività svolte fornendo evidenza, con livelli adeguati rispetto eventuali giudizi, della conformità delle attività di trattamento con il Regolamento, compresa l'efficacia delle misure.

II.7.10. DATA PROTECTION BY DESIGN E BY DEFAULT

Fondamenta S.p.A. adotta l'approccio metodologico a qualsiasi progetto, in base al quale deve essere valutata la protezione dei dati personali sin dalla progettazione. Per qualunque attività di trattamento, quindi, sia strutturale sia ancora concettuale, si deve considerare la protezione dei dati personali dal momento della sua progettazione e si devono prevedere soluzioni per la protezione dei dati personali.

Fondamenta S.p.A. mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento; in particolare le misure tecniche e organizzative messe in atto hanno lo scopo di garantire che – per impostazione predefinita – i dati personali vengano trattati solo per le specifiche finalità del trattamento e solo da un numero di

persone fisiche limitato al perseguimento di dette finalità.

II.8. – RISORSE UMANE

Il fattore umano costituisce allo stesso tempo la risorsa chiave dell'ente ed è la fonte da cui possono essere commessi i reati da prevenire. Ne consegue che l'ente pone la massima attenzione nella gestione delle risorse umane selezionando e mantenendo personale particolarmente qualificato. Particolare attenzione è prestata agli aspetti motivazionali ed alle specifiche esigenze formative, tenendo conto delle potenzialità degli individui e favorendo le condizioni per un ambiente di lavoro propositivo, collaborativo, gratificante e non conflittuale. Ciò nella convinzione che un sano ambiente di lavoro irrobustisce l'ente riguardo le minacce di commissione di reato.

Coloro che operano in nome e/o per conto dell'ente devono svolgere la propria attività lavorativa ed il proprio incarico con impegno professionale, diligenza, efficienza e correttezza, utilizzando al meglio gli strumenti ed il tempo a loro disposizione ed assumendo le responsabilità connesse agli impegni assunti.

L'ente garantisce un adeguato grado di professionalità nell'esecuzione dei compiti assegnati ai propri collaboratori, impegnandosi a valorizzare le competenze delle proprie risorse, mettendo a disposizione delle medesime idonei strumenti di formazione, di aggiornamento professionale e di sviluppo.

Tutto il personale è assunto con regolare contratto di lavoro, non essendo tollerata alcuna forma di lavoro irregolare e di sfruttamento.

Qualsiasi azione che possa configurare abuso d'autorità e, più in generale, che violi la dignità e l'integrità psico-fisica della persona non è tollerata dall'ente.

II.9. -DIVIETO DI DISCRIMINAZIONE

Per discriminazione si intende l'atto di fare una distinzione tra esseri umani o gruppi sociali, sia per azione o omissione con un senso sprezzante, esclusivo o negativo e che porta alla disuguaglianza di opportunità; si tratta di un atto di abuso e ingiustizia che viola il diritto all'uguaglianza. La discriminazione si verifica allorquando un individuo venga svantaggiato in quale modo, sulla base di una caratteristica protetta. Fondamenta S.p.A.

vieta qualsiasi forma di discriminazione quale, a titolo esemplificativo e non esaustivo, quella fondata: sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale."

Il trattamento sfavorevole assume rilievo ai fini della discriminazione qualora sia tale rispetto al trattamento riservato a un'altra persona che si trovi in situazione analoga.

La disparità di trattamento non costituisce discriminazione ed è consentita quando vi è una finalità legittima e i mezzi impiegati per il suo conseguimento sono obiettivi, appropriati e necessari, quali, ad esempio, finalità organizzative o la necessità di ricoprire specifici ruoli. Questo principio, ove possibile ed appropriato, si applica anche nei confronti dei clienti e dei fornitori.

II.10.- SEGNALAZIONI – WHISTLEBLOWING

Tutti coloro i quali prestano la propria opera a qualsiasi titolo e/o livello per la società Fondamenta S.p.A. e gli stakeholder in genere hanno il diritto/dovere di fare segnalazioni all'Organismo di Vigilanza ove avessero ragione di credere che qualcosa di pericoloso, illegale o non etico stia accadendo sul lavoro o che stia condizionando (o minacciando di condizionare) loro o altri colleghi. A titolo esemplificativo, ma non esaustivo il whistleblowing può includere:

- qualsiasi attività che si sospetta sia di natura criminale;
- qualsiasi attività che si sospetta possa comportare un rischio per la salute e la sicurezza;
- qualsiasi attività che si sospetta possa danneggiare l'ambiente;
- qualsiasi attività che si sospetta possa coinvolgere tangenti e corruzione;
- qualsiasi inadempienza degli obblighi legali o regolamentari;
- qualsiasi mancanza di requisiti professionali;
- qualsiasi tentativo di nascondere una o più di tali attività.

Fondamenta S.p.A. protegge adeguatamente i contenuti delle segnalazioni come pure il segnalante. Le modalità di segnalazione e di gestione della segnalazione sono disciplinate specificamente.
Questo principio, ove possibile ed appropriato, si applica anche nei confronti dei clienti e dei fornitori.

II.9. - DOCUMENTAZIONE

Ogni operazione, transazione, azione, rilevanti ai fini dell'Impegno di Conformità (quali ad esempio la documentazione contabile e di sicurezza) deve essere verificabile, documentata, coerente e congrua rispettando i principi di sicurezza del Sistema informativo di seguito meglio specificati.
Il sistema di controllo e vigilanza deve documentare l'effettuazione dei controlli, anche di supervisione; il sotto-processo "documentazione di vigilanza" è parte del processo "PGC" contenuto nella sezione b) della III Parte di questo documento.
La documentazione deve essere prodotta e mantenuta secondo idonei livelli di efficacia probatoria tenuto conto della vigente normativa.

II.10. SICUREZZA

II.10.1. SUL LAVORO

Fondamenta S.p.A. promuove e diffonde la cultura della sicurezza, sviluppando la consapevolezza dei rischi, promuovendo comportamenti responsabili da parte di tutti i dipendenti e collaboratori, al fine di preservarne la salute e la sicurezza.
Fondamenta S.p.A. garantisce un ambiente lavorativo conforme alle vigenti norme in materia di sicurezza e salute mediante il monitoraggio, la gestione e la prevenzione dei rischi connessi allo svolgimento delle attività professionali.
La gestione della salute e della sicurezza sul lavoro costituisce parte integrante della gestione generale dell'Ente.
Fondamenta S.p.A. adotta un sistema di gestione della salute e della sicurezza sul lavoro

(SGSL).

Il SGSL integra obiettivi e politiche per la salute e la sicurezza nella progettazione e gestione di sistemi di lavoro e di produzione di beni e servizi, definendo le modalità per individuare, all'interno dell'ente, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme di salute e sicurezza vigenti (D.Lgs. 81/2008).

Adeguate risorse sono specificamente allocate per la realizzazione dei principi sopra espressi.

II.10.2. DEL SISTEMA INFORMATIVO

Le informazioni e gli strumenti con cui sono trattate (elettronici e non, inclusi i programmi software) sono una risorsa chiave dell'Ente e, allo stesso tempo, sono, da un lato uno dei principali strumenti per la commissione di alcuni dei reati contemplati dal D.Lgs. 231/2001 (p.es. Reati ai danni delle P.A. Gr. 1 – Reati societari Gr. 3 – Delitti contro la personalità individuale Gr. 6 — Delitti informatici Gr. 10). Dall'altro lato, con specifico riferimento ai dati personali, le informazioni e gli strumenti di trattamento sono oggetto dell'obbligo di protezione da parte del Titolare che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Per Sistema informativo si intende il complesso delle risorse organizzate ed utilizzate dall'ente per il trattamento delle informazioni, ne consegue che l'ente ritiene prioritaria la protezione del Sistema informativo.

II.10.3. DELLE RISORSE FINANZIARIE

Le risorse finanziarie sono strategiche per l'ente ed allo stesso tempo sono uno degli strumenti maggiormente interessati dalla commissione di alcuni dei reati previsti dal D.Lgs. 231/2001.

L'art. 6 co. 2 lett. c) del D.Lgs. 231/2001 prescrive l'obbligo di individuare modalità di

gestione delle risorse finanziarie idonee ad impedire la commissione dei reati, a tal fine l'Ente si attiene scrupolosamente al rispetto della vigente normativa di settore sottoponendo le suddette attività al controllo del collegio sindacale.

II.11 - AMBIENTE

Fondamenta S.p.A. contribuisce attivamente nelle sedi appropriate alla promozione dello sviluppo scientifico e tecnologico volto alla salvaguardia delle risorse e dell'ambiente. La gestione operativa deve fare riferimento a criteri avanzati di salvaguardia ambientale e di efficienza energetica perseguendo il miglioramento continuo delle condizioni di salute e di sicurezza sul lavoro e di protezione ambientale.

Le Persone dell'ente, nell'ambito delle proprie mansioni, partecipano attivamente al processo di prevenzione dei rischi, di salvaguardia dell'ambiente e dell'incolumità pubblica e di tutela della salute e della sicurezza nei confronti di se stessi, dei colleghi e dei terzi.

II.12.- PATRIMONIO CULTURALE

La tutela e la valorizzazione del patrimonio culturale, come definito dal D.Lgs. 42/2004 e s.m.i., concorrono a preservare la memoria della comunità nazionale e del suo territorio e a promuovere lo sviluppo della cultura. La società Fondamenta S.p.A., nei limiti statutari ed operativi suoi propri, osserva gli adempimenti di legge e garantisce la conservazione richiedendo il rispetto delle disposizioni di tutela a tutti coloro i quali prestano la propria opera a qualsiasi titolo e livello, ai propri partner ed ai propri fornitori.

II.12 - VIGILANZA ED AGGIORNAMENTO

L'art. 6 co.1 lett. b) D.Lgs. 231/2001 prevede l'obbligo di affidare ad un organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento. La vigilanza è altresì requisito di adeguatezza delle misure tecniche ed organizzative a rispetto della normativa in materia di protezione dei dati personali.

All'Odv come sopra nominato spetta il compito di controllare il funzionamento e

l'osservanza del MOG e di curarne l'aggiornamento.
Il processo "Vigilanza" è meglio definito nella III Parte di questo documento "Sistema di vigilanza" nel rispetto dei principi contenuti nella policy dell'Organismo di vigilanza.
Per quanto riguarda la vigilanza del rispetto del GDPR, al momento l'Ente non rientra tra i soggetti obbligati alla designazione di un Responsabile della Protezione dei Dati Personali (DPO), pertanto, tale compito è stato affidato al Privacy Manager che riferisce direttamente all'Amministratrice Delegata.
Il Privacy Manager e l'Organismo di Vigilanza coordinano tra loro le attività di controllo.
Al fine di garantire l'efficacia ed efficienza del MOG, periodicamente, almeno una volta l'anno, ed anche prima qualora intervengano rilevanti mutamenti organizzativi dell'Ente o legislativi, ad iniziativa di chi è incaricato della vigilanza è promossa la revisione ed aggiornamento del MOG medesimo.
Il processo di attività è dinamico e ricalca il modello del ciclo di miglioramento continuo (ad es. il ciclo di Deming); il Modello, per poter essere efficace ed efficiente deve essere coerente con l'ente e con l'ambiente entro cui esso opera, ne consegue che in occasione di rilevanti cambiamenti interni e/o esterni il Modello deve essere aggiornato e periodicamente revisionato.
Il sotto-processo "Revisione" è parte del processo "231" descritto nella sezione b) della III Parte di questo documento.

II.13 - COMUNICAZIONI

L'art. 6 co. 2 lett. d) del D.Lgs. 231/2001 prevede l'obbligo di organizzare un sistema di informazioni nei confronti di chi è tenuto alla vigilanza.
Peraltro, corrette, puntuali ed esatte informazioni sono alla base di ogni processo decisionale e di controllo dell'Ente. I compiti relativi alle comunicazioni interne ed esterne dell'Ente devono essere definiti ed assegnati al fine di assicurare il rispetto degli obblighi di trasparenza, l'autenticità ed integrità delle comunicazioni dell'Ente, l'adeguatezza, tempestività ed accuratezza delle informazioni in genere, la diffusione delle informazioni nell'ente secondo le necessità.

Le informazioni trasmesse a chi effettua la vigilanza devono soddisfare alti livelli di integrità, disponibilità, riservatezza ed autenticità.

Devono essere individuati e stabiliti idonei canali di comunicazione verso chi effettua la vigilanza, attraverso i quali tutti coloro che operano per l'ente possano segnalare fatti rilevanti ai fini del D.Lgs. 231/2001 (quali ad esempio incidenti di sicurezza, violazioni o sospetto di violazioni delle norme previste dal MOG), ai fini della protezione dei dati personali, ai fini degli obblighi di whistleblowing in genere.

A coloro che svolgono attività di vigilanza, oltre al rispetto dei requisiti eventualmente previsti da norme, deve essere assicurata autonomia e indipendenza per garantire l'obiettività del controllo, nonché le risorse ed i poteri necessari e la disposizione di canali di comunicazione diretti con i vertici. Le persone che svolgono attività di vigilanza devono essere scelte tra coloro che offrono adeguate garanzie di buona reputazione, di capacità, conoscenza, professionalità ed esperienza in relazione all'oggetto della vigilanza.

II.14 - FORMAZIONE

L'efficacia e l'efficienza del processo di rispetto dell'Impegno di Conformità assunto dalla società, unitamente al rispetto dei principi di correttezza e trasparenza e della normativa giuslavoristica richiede che coloro che prestano la propria opera, a qualsiasi titolo e livello per la società Fondamenta S.p.A. siano regolarmente ed adeguatamente formati. L'art. 6 co. 2 lett. b) prevede l'obbligo di definire specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire, allo stesso modo il GDPR considera la formazione come una imprescindibile attività che assicura il rispetto dei principi di correttezza e trasparenza e costituisce una delle condizioni della efficace attuazione delle misure tecniche ed organizzative di conformità.

Tutti coloro che operano per conto dell'ente devono essere informati e ricevere formazione sugli aspetti rilevanti della norma, le regole decise dall'ente in materia, le responsabilità e le conseguenze per la mancata osservanza delle regole.

La formazione è elemento primario del sistema di sicurezza e prevenzione dei rischi assunti nell'Impegno di Conformità.

Le attività di formazione devono essere programmate e diversificate tenendo conto delle necessità specifiche dei destinatari.
L'attività di formazione deve essere misurata al fine di verificarne l'efficacia.
Le responsabilità per la formazione devono essere chiaramente attribuite.
La formazione deve essere aggiornata quando intervengono modifiche rilevanti del MOG ovvero quando da controlli sull'efficacia o sui livelli di consapevolezza dei destinatari ne emerga la necessità.
Il sotto-processo "formazione" è parte del processo "PGC" contenuto nella III Parte di questo documento.

II.15 - SISTEMA DISCIPLINARE

L'art. 6 co.2 lett. e) prevede espressamente l'obbligo di conformare il sistema disciplinare in modo da renderlo idoneo a sanzionare il mancato rispetto delle misure indicate nel modello. Questo principio è peraltro condizione di efficacia per qualsiasi direttiva, regola, indicazione collegata all'Impegno di Conformità.
Il Sistema Disciplinare affianca ed integra il Codice Disciplinare prevedendo le azioni da assumere in caso di comportamenti scorretti rilevanti ai fini dei requisiti identificati nell'Impegno di Conformità tenuti non soltanto dai prestatori d'opera, ma anche dai collaboratori, amministratori e chiunque altro opera in nome o per conto dell'Ente.
In particolare, per quanto riguarda i dipendenti, coerentemente a quanto previsto dall'art. 7 della L. 300/1970 (Statuto dei lavoratori), le conseguenze disciplinari per il mancato rispetto delle decisioni adottate dall'Ente riguardo alla conformità devono essere chiaramente e specificamente formalizzate nel Sistema Disciplinare. Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro di riferimento. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua

difesa.

Le responsabilità per i controlli e per le contestazioni disciplinari devono essere chiaramente e specificamente definite e portate a conoscenza con idonei mezzi a tutti gli interessati.

Il Sistema Disciplinare connesso a questo Modello è riportato nella III Parte di questo documento.

APPROVAZIONE

Questa parte I del Modello di Organizzazione e Gestione della società Fondamenta S.p.A.

è approvata

con delibera del **18 settembre 2023** dal Consiglio di Amministrazione.

Tutti i documenti in essa contenuti si intendono approvati e diventano vincolanti per tutti coloro che ricadono nell'ambito di applicazione a far data da oggi.

Ogni documento precedente si intende da oggi abrogato e sostituito.

Si dà mandato a ciascun responsabile di Punto Organizzativo e Referente Aziendale:

- di dare comunicazione ai propri interessati delle regole approvate, in sintonia al piano di comunicazione;
- di vigilare il rispetto del Modello e della documentazione sussidiaria;
- di ricevere e riferire eventuali feedback e/o segnalazioni che dovessero pervenire.

Milano il **18 settembre 2023**

FONDAMENTA S.p.A.
Via Turati 26
20121 MILANO
Partita I.V.A. 01543610180

Giulio Borelli

Presidente del C.d.A.