

**MODELLO DI ORGANIZZAZIONE E
GESTIONE ex D.Lgs. 231/2001
-
LEPIDA SCPA**



INDICE

Revisioni	8
Definizioni e Glossario	10
PARTE GENERALE	13
1. Introduzione	14
1.1 Premessa	14
1.2 Le motivazioni di Lepida per l'adozione del Modello di organizzazione e gestione	15
1.3 Interazione del MOG con altri strumenti di Prevenzione	16
1.3.1 Prevenzione della corruzione	16
1.3.1.1 Tutela del segnalante illeciti (cd. whistleblower)	16
1.3.2 Sistemi di Gestione	18
1.4 Obiettivo del documento	19
1.5 Campo d'applicazione	20
1.6 Allegati al documento	20
2. Il Decreto	21
2.1 Descrizione generale	21
2.2 Reati presupposto	21
2.2.1 Ipotesi di concorso colposo o di cooperazione colposa nel reato presupposto	31
2.3 Soggetti attivi	31
2.4 Interesse o vantaggio per l'Ente	32
2.5 Condizioni di esenzione	32
2.6 Sanzioni	33
3. Quadro normativo di riferimento di Lepida	34
4. Modello di Organizzazione e di Gestione	36
4.1 Caratteristiche del Modello	36
4.2 Procedimento di adozione e modifica del Modello organizzativo	37
4.3 L'elaborazione del Modello	37
4.3.1 Principi generali	37
4.4 Metodo di analisi dei rischi adottato e attività svolte	40
4.4.1 Identificazione delle macroaree di attività a rischio reato	44
4.4.2 Calcolo del peso del reato	44
4.4.2.1 Le sanzioni interdittive	44
4.4.2.2 Le sanzioni pecuniarie	45
4.4.3 L'indice di gravità del reato	45
4.4.4 Indice di correlazione del reato	46
4.4.5 Calcolo del rischio potenziale (o assoluto)	47
4.4.6 Calcolo del peso dei controlli	47
4.4.7 La valutazione del rischio residuo	48
4.5 L'analisi dei rischi	49
4.5.1 Identificazione dei reati esclusi ex ante	51



4.5.2	Identificazione delle Macroattività a rischio	57
4.5.3	Identificazione delle Macroattività particolarmente sensibili	58
4.5.4	Fattispecie di reato a maggior rischio potenziale	58
4.5.5	Parte Speciale	59
5.	Il Sistema dei controlli	59
5.1	Componenti del sistema dei controlli	59
6.	Sistema sanzionatorio	60
6.1	Criteri di applicazione delle sanzioni	61
6.2	Sanzioni per violazioni commesse da dipendenti	61
6.3	Sanzioni per violazioni commesse da Dirigenti, membri del CdA o del Collegio Sindacale	63
6.4	Sanzioni per violazioni commesse da soggetti terzi	64
6.5	Sanzioni connesse all'istituto del Whistleblowing	64
7.	L'Organismo di Vigilanza	66
7.1	Requisiti dell'Organismo Di Vigilanza	66
7.1.1	Indipendenza e autonomia	66
7.1.2	Professionalità	66
7.1.3	Autonomia nei poteri di iniziativa e controllo	66
7.1.4	Continuità di azione	66
7.1.5	Acquisizione delle informazioni	67
7.1.6	Riporto agli Organi sociali	67
7.1.7	Qualificazione e ruolo dell'OdV ai fini della normativa sul trattamento dei dati personali	67
7.2	Nomina dei membri dell'Organismo di Vigilanza	67
7.3	Rinuncia, revoca e sanzioni	68
7.4	Modalità di funzionamento dell'Organismo di Vigilanza	70
7.5	Funzioni, attività e poteri dell'Organismo di Vigilanza	70
7.6	Obblighi di informazione verso l'Organismo di Vigilanza	73
7.7	Tipologie di informazioni e segnalazioni verso l'Organismo di Vigilanza	74
7.8	Raccolta e conservazione delle informazioni	75
8.	Comunicazione e diffusione	76
8.1	Diffusione verso l'interno	76
8.1.1	Comunicazione e formazione in generale	76
8.1.2	Comunicazione e formazione	77
8.2	Diffusione verso l'esterno	77
	PARTE SPECIALE	78
	Introduzione	79
	0. Fattispecie escluse o abrogate	79
	0.1 Principi generali di comportamento	79
	0.2 Principi generali di controllo	80
	1. Reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	82
1.1	Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo	



predisposti a livello societario centrale (FASE 1)	82
1.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	82
1.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	83
1.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	84
1.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	86
1.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	86
1.2.2 Controlli societari periferici (FASE 2 - punto 2)	87
1.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	89
2. Reati informatici e illecito trattamento dei dati personali (art. 24-bis del Decreto)	89
2.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	89
2.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	89
2.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	90
2.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	91
2.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	92
2.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	92
2.2.2 Controlli societari periferici (FASE 2 - punto 2)	92
2.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	96
3. Delitti di criminalità organizzata (art. 24-ter del Decreto)	97
3.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	97
3.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	97
3.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	97
3.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	98
3.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	99
3.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	99
3.2.2 Controlli societari periferici (FASE 2 - punto 2)	99
3.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	99
4. Reati societari di cui agli artt. 2621 e ss. (art. 25-ter del Decreto)	100
4.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	100
4.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	100
4.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	101
4.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione	



dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	101
4.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	102
4.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	102
4.2.2 Controlli societari periferici (FASE 2 - punto 2)	102
4.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	103
5. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del Decreto)	104
5.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	104
5.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	104
5.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	104
5.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	105
5.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	106
5.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	106
5.2.2 Controlli societari periferici (FASE 2 - punto 2)	106
5.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	108
6. Reati relativi al riciclaggio di denaro e all'autoriciclaggio (art. 25-octies del Decreto)	109
6.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	109
6.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	109
6.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	109
6.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	110
6.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	110
6.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	110
6.2.2 Controlli societari periferici (FASE 2 - punto 2)	111
6.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	111
7. Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1 del Decreto)	111
7.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	111
7.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	111
7.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	112
7.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	112
7.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	113
7.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	113



7.2.2 Controlli societari periferici (FASE 2 - punto 2)	113
7.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	115
8. Reati in materia di violazione del diritto d'autore (art. 25-novies del Decreto)	115
8.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	116
8.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	116
8.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	116
8.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	117
8.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	117
8.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	117
8.2.2 Controlli societari periferici (FASE 2 - punto 2)	118
8.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	118
9. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies del Decreto)	119
9.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	119
9.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	119
9.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	119
9.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	120
9.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	120
9.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	121
9.2.2 Controlli societari periferici (FASE 2 - punto 2)	121
9.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	121
10. Reati in materia ambientale (art. 25-undecies del Decreto)	121
10.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	122
10.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	122
10.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	123
10.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	124
10.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	124
10.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	125
10.2.2 Controlli societari periferici (FASE 2 - punto 2)	125
10.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	125



11. Reati tributari (art. 25-quinquiesdecies del Decreto)	126
11.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	126
11.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	126
11.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	126
11.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	127
11.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	128
11.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	128
11.2.2 Controlli societari periferici (FASE 2 - punto 2)	128
11.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	131
12. Reati contro il patrimonio culturale (artt. 25-septies decies e 25-duodevicies del Decreto)	131
12.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)	131
12.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)	131
12.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)	132
12.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)	132
12.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)	133
12.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)	133
12.2.2 Controlli societari periferici (FASE 2 - punto 2)	133
12.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)	134
13. Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater del Decreto)	134
14. Appendice	136
La gestione delle procedure finanziate con fondi PNRR	136



Revisioni

Storico delle revisioni del documento			
N°	Data	Descrizione	Rev. Approvata
01	02/12/2013	Revisione Modello a seguito dell'introduzione di nuovi reati nel perimetro del D.Lgs. 231/2001, del recepimento della Legge 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", del trasferimento di ulteriori funzioni a Lepida SpA e revisione dell'assetto organizzativo.	27 dicembre 2013
02	26/09/2016	Revisione Modello a seguito dell'introduzione di nuovi reati nel perimetro del D.Lgs. 231/2001.	14 ottobre 2016
03	24/01/2018	Revisione Modello a seguito della variazione dell'organigramma aziendale e dell'istituzione della Divisione Integrazioni Digitali e introduzione dei nuovi reati presupposto.	24 gennaio 2018
04	04/09/2018	Revisione Modello relativamente Parte speciale L - REATI AMBIENTALI.	4 settembre 2018
05	28/08/2019	Revisione Modello a seguito della fusione per incorporazione di CUP 2000 ScpA e contestuale trasformazione societaria da SpA a ScpA, con conseguente variazione dell'organigramma aziendale, nonché delle modifiche apportate al D.Lgs. 231/2001 (Legge 9 gennaio 2019, n. 3 e Legge 3 maggio 2019, n. 39).	10 settembre 2019
06	16/11/2020	Aggiornamento del Modello a seguito di: - (1) aggiornamento dell'Organigramma societario a partire dal 01.01.2021; - (2) modifiche normative di cui al D.L. 105/2019, dell'introduzione, ad opera del D.L. 124/2019, dell'art. 25-quinquiesdecies (Reati tributari) e dell'ulteriore modifica di tale ultima previsione ad opera del D.L. 75/2020; - (3) adeguamento ai rischi riconducibili al diffondersi della pandemia Covid-19 dovuta al virus SARS-CoV-2.	19 novembre 2020
07	22/11/2021	Aggiornamento del Modello a seguito di: - (1) in data 14.09.2021, istituzione, all'interno della Divisione Datacenter&Cloud, della nuova Area 27 - <i>Supporto IT ai Soci</i> ; - (2) nuove procedure aziendali adottate dalla Divisione Amministrativa, con particolare riferimento all'Area 71 Amministrazione&Controllo di Gestione;	23 novembre 2021



		<ul style="list-style-type: none"> - (3) l'aggiornamento al 21 giugno 2021 delle Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001; - (4) la Delibera ANAC 9 giugno 2021, n. 469, avente ad oggetto "Linee Guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del D.Lgs. 165/2001 (c.d. whistleblowing)". 	
08	16/11/2022	<p>Aggiornamento del Modello a seguito di:</p> <ul style="list-style-type: none"> - (1) modifiche normative di cui al D.Lgs. 184/2021, che ha disposto l'introduzione dell'art. 25-octies.1; - (2) modifiche normative di cui al D.Lgs. 195/2021 relativamente all'ampliamento dell'ambito di applicazione dei reati presupposto di cui all'art. 25-octies; - (3) modifiche normative di cui alla L. n. 22/2022, che ha disposto l'introduzione degli artt. 25-septies decies e 25-duodevicies; - (4) aggiornamento della Procedura e adozione del Regolamento in materia di segnalazione di illeciti o irregolarità. Disciplina della tutela del dipendente che segnala illeciti (cd. <i>whistleblowing</i>). 	18 novembre 2022
09	13/11/2023	<p>Aggiornamento del Modello a seguito di:</p> <ul style="list-style-type: none"> - (1) modifiche normative di cui al D.Lgs. 24/2023 che ha raccolto in un testo normativo unico tutta la normativa preesistente in materia di whistleblowing, abrogando, al contempo, i commi 2-ter e 2-quater di cui all'art. 6 del D.Lgs. 231/2001 e modificando il testo del comma 2-bis di cui al medesimo articolo; - (2) conseguente aggiornamento della Procedura e del Regolamento in materia di segnalazione di illeciti o irregolarità. Disciplina della tutela del dipendente che segnala illeciti (cd. <i>whistleblowing</i>); - (3) ottenimento, da parte di Lepida S.cp.A., della Certificazione ISO 37001 - Certificazione del Sistema di Gestione per la Prevenzione della Corruzione; - (4) modifiche normative di cui al D.Lgs. 19/2023, che ha disposto l'introduzione, all'art. 25-ter, comma 1, del D.Lgs. 231/2001, della lett. s-ter), di un nuovo reato presupposto (delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare); - (5) modifiche normative di cui al D.L. 105/2023 convertito con L. 137/2023, che ha disposto 	15 novembre 2023



		<p>l'introduzione, all'art. 24 del D.Lgs. 231/2001, di due nuovi reati presupposto (turbata libertà degli incanti e turbata libertà del procedimento di scelta del contraente ex artt. 353 e 353 bis c.p.) e all'art. 25.octies.1 del D.Lgs. 231/2001, di un nuovo reato presupposto (trasferimento fraudolento di valori art.512 bis c.p.);</p> <ul style="list-style-type: none"> - (6) variazione dell'organigramma aziendale di Lepida; - (7) analisi impatto della gestione delle procedure finanziate PNRR. 	
10	15/11/2024	<p>Aggiornamento del Modello a seguito di:</p> <ul style="list-style-type: none"> - modifiche normative di cui alla L. 90 / 2024 che ha disposto l'introduzione, all'art. 24 bis, comma 1 bis, di un nuovo reato presupposto (estorsione informatica ex art. 629, comma 3, c.p.) e ha abrogato l'art. 615 quinquies c.p. introducendo, all'interno del comma 2 dell'art. 24 bis D.lgs 231 / 2001 il riferimento al reato di cui all'art. 635 quater 1 c.p. (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico); - modifiche normative di cui al D.L. 4 luglio 2024, n. 92, convertito dalla L. 8 agosto 2024, n. 112 che ha disposto l'introduzione, all'art. 25, comma 1, del nuovo reato presupposto di cui all'art. 314 bis c.p. (Indebita destinazione di denaro o cose mobili) ed eliminato il riferimento al reato di abuso d'ufficio, abrogato dalla L. 9 agosto 2024, n. 114, art. 1, comma 1, lettera b). - modifiche normative di cui al D.lgs. 141/2024, che ha disposto l'introduzione, all'art. 25-sex-decies, dei reati previsti dalle disposizioni complementari al codice doganale dell'Unione e dal testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi e relative sanzioni penali e amministrative di cui al d.lgs. 504/1995. 	20 novembre 2024



Definizioni e Glossario

Termini	Definizioni
Decreto	Decreto Legislativo n. 231 dell'8 Giugno 2001 e successive modificazioni e integrazioni.
Società/Lepida	Lepida ScpA (di seguito Lepida).
Destinatari	Soggetti, sia dipendenti che terzi rispetto alla Società, ai quali sono indirizzati i principi etici, le istruzioni operative e il Modello Organizzativo nel suo insieme, ciascuno secondo i livelli di responsabilità a loro attribuiti.
Modello Organizzativo	Indica il modello di organizzazione, gestione e controllo idoneo a prevenire i reati predisposto dalla Società ai sensi del D.Lgs. 231/2001.
Enterprise Model	Documento contenente il modello e la descrizione dei processi aziendali di Lepida.
Attività sensibile	Operazione (o serie di operazioni) svolta ordinariamente dal personale nell'ambito delle proprie mansioni e che, per sua caratteristica, richiede l'applicazione di specifici controlli volti a limitare l'esposizione al rischio di commissione dei reati previsti dal Decreto.
Codice Etico e di Comportamento	Documento allegato al Modello Organizzativo che indica i principi e i valori - finalizzati ad evitare comportamenti che possono integrare le fattispecie di reato previste dal Decreto e, più in generale, a favorire comportamenti virtuosi in ambito aziendale - che la Società e i suoi dipendenti si impegnano a rispettare e promuovere.
Linee guida di Confindustria	Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del Decreto, approvate il 7 marzo 2002 (aggiornate a giugno 2021).
Mappatura dei rischi	Documentazione predisposta per: <ul style="list-style-type: none"> • analizzare le attività "sensibili" della Società con riferimento ai rischi di commissione dei reati di cui al Decreto; • sintetizzare i protocolli posti in essere per contrastare i rischi di reato; • rinviare, dove applicabile, alla documentazione più estesa dei controlli e delle procedure disponibili nel sistema aziendale; • indicare analiticamente i livelli di responsabilità per la corretta applicazione delle regole aziendali.
Repository dei rischi	Documento in formato excel contenente l'elenco dei comportamenti/attività a rischio rilevati in corrispondenza dei processi aziendali di Lepida, attraverso l'attività di analisi dei rischi.
OdV	Organismo di Vigilanza: organismo, nominato dalla Società, dotato di autonomi poteri di iniziativa e di controllo di cui all'art. 6 del Decreto.
PNA	Piano Nazionale Anticorruzione di cui all'art. 1, co. 2-bis, L. 6 novembre 2012 n. 190 "Disposizioni per la prevenzione e la repressione della



	<p><i>corruzione e dell'illegalità nella pubblica amministrazione". La funzione principale del P.N.A. è quella di assicurare l'attuazione coordinata delle strategie di prevenzione della corruzione nella pubblica amministrazione, elaborate a livello nazionale e internazionale.</i></p>
<p>PTPCT</p>	<p>Le società in controllo pubblico di cui al D.Lgs. 175/2016, ai sensi degli artt. 1, co. 2-bis, L. 190/2012 e 2-bis, co 2, D Lgs. 14 marzo 2013, n. 33, adottano misure di prevenzione della corruzione <i>integrative</i> di quelle adottate ai sensi del decreto legislativo 8 giugno 2001, n. 231. Il PTPCT- Misure integrative al MOG costituisce pertanto parte integrante del presente Modello.</p>
<p>Sistema disciplinare</p>	<p>Si intende il sistema disciplinare previsto dal Decreto per il mancato rispetto delle misure indicate nel Modello Organizzativo.</p>
<p>Soggetti apicali</p>	<p>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 (art. 5, comma 1, lett. a) del Decreto).</p>
<p>Soggetti subordinati</p>	<p>Persone sottoposte alla direzione o alla vigilanza di uno dei Soggetti Apicali (art. 5, comma 1, lett. b) del Decreto).</p>



PARTE GENERALE



1. Introduzione

1.1 Premessa

Il decreto legislativo 8 giugno 2001 n. 231 (nel seguito "Decreto") ha introdotto per la prima volta nel nostro ordinamento una forma di responsabilità, amministrativa e pur sempre ricollegata alla commissione di un reato, per gli enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica.

La responsabilità si configura in caso di commissione **a vantaggio o nell'interesse dell'Ente** di uno dei **reati presupposto** specificamente individuati dal Decreto, purché gli stessi siano stati **commessi da**:

- **persone che rivestono funzioni amministrative di amministrazione o di direzione dell'ente**, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
- **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera precedente.**

Salvo che costoro non abbiano agito nell'interesse esclusivo proprio o di terzi, la Società sarà ritenuta direttamente e autonomamente responsabile, perfino laddove il reato sia estinto o l'autore del reato non sia mai stato identificato o sia non imputabile.

L'Ente non risponderà qualora dimostri di aver adottato un modello di organizzazione, gestione e controllo (nel seguito anche "MOG"), attuato anche per il tramite di uno specifico Organismo di Vigilanza, che il reo, proprio al fine di commettere il reato, abbia dovuto eludere fraudolentemente.

Il quadro normativo è stato profondamente modificato dal decreto legislativo 25 maggio 2016, n. 97, recante *"Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"*, insieme al decreto legislativo 19 agosto 2016, n. 175, *"Testo unico in materia di società a partecipazione pubblica"* (Tusp), come modificato dal decreto legislativo 16 giugno 2017, n. 100. Tale decreto ha apportato numerose novità con riferimento all'applicazione delle misure di trasparenza e di prevenzione della corruzione nelle società a controllo pubblico, negli enti di diritto privato controllati, nelle società partecipate e negli altri enti di diritto privato considerati dal legislatore all'art. 2 bis, co. 3, del D.Lgs. 33/2013, tra cui figurano gli obblighi di pubblicazione e l'accesso generalizzato nel nuovo D.Lgs. 33/2013 e il nuovo ambito soggettivo definito dal nuovo art. 2-bis, riferito tanto agli obblighi di pubblicazione quanto all'accesso generalizzato.

Con riferimento alle misure di prevenzione della corruzione diverse dalla trasparenza, l'art. 41 del d. Lgs. 97/2016, aggiungendo il co. 2-bis all'art. 1 della l. 190/2012, prevede che tanto le pubbliche amministrazioni quanto gli *"altri soggetti di cui all'articolo 2-bis, comma 2, del d. Lgs. n. 33 del 2013"* siano destinatari delle indicazioni contenute nel PNA (del quale è la legge stessa a definire la natura di atto di indirizzo), ma secondo un regime differenziato: mentre le prime sono tenute ad adottare un vero e proprio PTPCT, i secondi devono adottare *"misure integrative di quelle adottate ai sensi del decreto legislativo 8 giugno 2001, n. 231"*.

Lepida, quale ente di diritto privato in controllo pubblico, è tenuta ad introdurre e ad implementare le misure organizzative e gestionali previste dalla Legge 190/2012 "Disposizioni



per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione". La legge è entrata in vigore il 28 novembre 2012.

Con tale provvedimento normativo è stato introdotto anche nel nostro ordinamento un sistema organico di prevenzione della corruzione, il cui aspetto caratterizzante consiste nell'articolazione del processo di formulazione e attuazione delle strategie di prevenzione della corruzione su due livelli.

Ad un primo livello, quello "nazionale", il Comitato interministeriale per la prevenzione e il contrasto della corruzione e dell'illegalità nella pubblica amministrazione definisce linee di indirizzo sulla cui base, ai sensi dell'art. 19, co. 15, D.L. 90/2014, l'Autorità Nazionale Anticorruzione (A.N.A.C.) redige e - acquisito il parere positivo dello stesso Comitato interministeriale e della Conferenza Unificata di cui al D.Lgs. 28 agosto 1997 n. 281, - approva il Piano Nazionale Anticorruzione (P.N.A.).

Al secondo livello, quello "decentrato", ogni amministrazione pubblica definisce un P.T.P.C.T. (Piano Triennale di Prevenzione della Corruzione e della Trasparenza), che, sulla base delle indicazioni presenti nel P.N.A., effettua l'analisi e valutazione dei rischi specifici di corruzione e conseguentemente indica gli interventi organizzativi volti a prevenirli.

1.2 Le motivazioni di Lepida per l'adozione del Modello di organizzazione e gestione

Lepida, per assicurare sempre migliori e più idonee condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, con particolare riferimento al rapporto con la Regione Emilia-Romagna e con tutti i propri Enti Soci a tutela delle loro aspettative, ha deliberato un progetto di analisi degli strumenti organizzativi, di gestione e di controllo, volto a:

- verificare la conformità delle prassi e delle dinamiche aziendali rispetto alle finalità previste dal Decreto;
- definire e adottare un modello di organizzazione, di gestione e di controllo coerente alle prescrizioni del Decreto.

Il MOG rappresenta:

- uno strumento di sensibilizzazione per tutti i soggetti che operano per conto della Società, affinché mantengano, nell'espletamento delle proprie attività, comportamenti conformi alle norme esterne e alle regole interne;
- un mezzo di prevenzione contro il rischio di commissione dei reati previsti dal Decreto.

L'adozione del presente MOG, oltre a rappresentare una precisa scelta aziendale volta a identificare i rischi potenziali derivanti dall'espletamento delle attività necessarie al raggiungimento dell'Oggetto Sociale e a definire e implementare regole, strumenti e, ove necessario, disposizioni disciplinari per arginare, trasferire e in definitiva gestire i suddetti rischi, si è resa indispensabile anche per via della connotazione pubblicitica di Lepida, dovuta alla proprietà totalmente pubblica del capitale sociale - in linea con la propria natura in house, tale da richiedere la realizzazione di un sistema idoneo a gestire i rapporti con la Regione stessa e con gli altri Enti Soci.

Ove Lepida venisse a conoscenza, nei limiti di quanto consentitole dalla natura e dalla disciplina di ciascun rapporto con i propri dipendenti e collaboratori, di comportamenti potenzialmente idonei ad integrare le fattispecie di reato elencate nel presente Modello, o



comunque volte ad agevolare la commissione dei suddetti reati, saranno adottati i provvedimenti disciplinari ritenuti più opportuni per i dipendenti o si potrà far ricorso ad apposite clausole risolutive espresse del rapporto di collaborazione, ex art. 1456 c.c., negli altri casi.

1.3 Interazione del MOG con altri strumenti di Prevenzione

1.3.1 Prevenzione della corruzione

Lepida ha predisposto, e aggiornato anche per l'anno 2024, un proprio Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.- Misure integrative al MOG - parte integrante del presente Modello di Organizzazione e gestione (Allegato 2) - quale documento fondamentale per la definizione della strategia di prevenzione della corruzione all'interno della propria organizzazione. Nella stesura dell'aggiornamento per il triennio 2024-2026 Lepida ha tenuto in considerazione le indicazioni del PNA 2022-2024 approvato da ANAC con delibera n. 7 del 17 gennaio 2023 e dell'aggiornamento 2023 del PNA 2022, approvato con delibera n. 605 del 19 dicembre 2023. Anche alla luce delle *"Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e dagli enti pubblici economici"*, approvate da ANAC con Delibera 8 novembre 2017 n. 1134, esso costituisce parte integrante del presente Modello di Organizzazione e Gestione. Il MOG e il P.T.P.C.T. di Lepida assicurano espressamente la *"Tutela del dipendente che effettua segnalazioni di illecito (cd. whistleblower)"*, aggiornata da ultimo nel 2023 per effetto del mutato quadro normativo di riferimento, come di seguito rappresentato.

1.3.1.1 Tutela del segnalante illeciti (cd. whistleblower)

La tutela del dipendente che segnala condotte illecite all'interno dell'ambiente di lavoro è stata introdotta nell'ordinamento nazionale con la Legge n. 190/2012, che ha modificato l'art. 54-bis del D.Lgs. 165/2001. Quanto al settore privato, la Legge 30 novembre 2017, n. 179 (*"Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"*) è intervenuta inserendo i commi 2-bis, ter e quater nell'art. 6 del Decreto. Da ultimo, in data 30 marzo 2023 è entrato in vigore il D.Lgs. 24/2023, che ha raccolto in un testo normativo unico *tutta la normativa preesistente in materia di canali di segnalazione e di tutela del segnalante, sia nel settore pubblico che privato ed ha, al contempo, da un lato abrogato il citato articolo 54-bis D.Lgs. 165/2001, i commi 2-ter e 2-quater, di cui all'art. 6 D.Lgs. 231/2001, nonché, l'articolo 3 della L. 179/2017, dall'altro modificato anche il testo del comma 2-bis di cui all'art. 6 del D.Lgs. 231/2001.*

Conseguentemente, il modello organizzativo di Lepida, conformemente a quanto disposto dal citato comma 2-bis, prevede i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare.

Nella consapevolezza del generale divieto di ritorsione posto dall'art. 17, comma 11, del D.Lgs. 24/2023 e delle previsioni di cui al citato comma 2-bis, D.Lgs. 231/2001, Lepida ha conseguentemente:



- integrato il proprio [PTPCT](#) con specifiche indicazioni circa Comunicazioni e Segnalazioni ad opera di dipendenti e soggetti esterni;
- approvato un [Regolamento](#) e una [Procedura](#) di segnalazione di illeciti o di irregolarità. Disciplina della tutela del dipendente che segnala illeciti (cd. whistleblowing)", entrambi aggiornati al D.Lgs. 24/2023, cui è allegato un modulo per la segnalazione di illeciti, laddove si prevede che le segnalazioni possono essere presentate secondo una delle seguenti modalità:
 - tramite invio all'indirizzo di posta elettronica segnalazioneilleciti@lepida.it, appositamente dedicato alla ricezione delle segnalazioni; l'indirizzo di posta elettronica è pubblicato sul sito istituzionale e nella intranet di Lepida e la posta inviata a tale indirizzo verrà visionata e trattata solo dal Responsabile della Prevenzione della Corruzione e della Trasparenza;
 - tramite servizio postale; in tal caso, per avere le garanzie di tutela di riservatezza, occorre che la segnalazione sia inserita in una busta chiusa che all'esterno rechi il seguente indirizzo "Al Responsabile della Prevenzione della Corruzione e della Trasparenza di Lepida, Via della Liberazione, n. 15, 40128 Bologna" e a lato la dicitura "RISERVATA";
 - tramite apposito [Form di segnalazione illeciti](#)" presente su sito web istituzionale (raggiungibile anche mediante browser anonimizzante tipo Tor Browser), che permette di inviare la segnalazione all'indirizzo di posta elettronica segnalazioneilleciti@lepida.it in modalità cifrata, allo scopo di tutelare in maniera più sicura l'identità del segnalante;
 - tramite colloquio orale con il Responsabile della Prevenzione della Corruzione e della Trasparenza, secondo le modalità indicate nei sopra citati Regolamento e Procedura.
- predisposto una specifica pagina denominata ["Prevenzione della corruzione"](#) all'interno della sezione Società Trasparente del sito istituzionale;
- predisposto una specifica pagina denominata ["Trasparenza e Anticorruzione"](#) all'interno della Intranet aziendale;
- attribuito evidenza specifica al whistleblowing e al form di segnalazione nel proprio sito istituzionale, in ogni pagina, subito al di sopra del footer.

Le segnalazioni ricevute vengono protocollate e custodite con modalità tecniche tali da garantire la massima sicurezza, anche con riguardo all'identità del segnalante.

Si dà atto che alla data dell'attuale aggiornamento del Modello di Lepida non si sono registrate segnalazioni, né tramite i tradizionali canali di comunicazione, né tramite l'apposito sistema informativo - form, disponibile sul sito istituzionale della Società.

In relazione alla disciplina del cd. Whistleblower sono altresì previste [specifiche sanzioni](#) riconnesse alla violazione delle misure di tutela del segnalante, da un lato, e all'effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.

La natura giuridica di Lepida quale società a partecipazione pubblica - che la rende anche destinataria della normativa dell'anticorruzione - e, dunque, la coesistenza del sistema di



segnalazione relativo tanto alla commissione dei reati presupposto di cui al d. Lgs. 231/2001, quanto alle irregolarità di natura pubblicistica, fanno sì che in coerenza con le prescrizioni di ANAC e di quanto disposto, da ultimo, anche dall'art. 4, comma 5, D.Lgs. 24/2023, solo il RPCT sia l'unico soggetto destinatario delle segnalazioni riconducibili all'istituto del c.d. whistleblowing¹ e l'unico soggetto affidatario della gestione del canale di segnalazione interna.

1.3.2 Sistemi di Gestione

Lepida implementa diversi Sistemi di Gestione certificati secondo le relative norme ISO.

In particolare:

- Sistema di Gestione per la Qualità (SGQ): certificato dal 2012 secondo la norma ISO 9001;
- Sistema di Gestione per la Sicurezza delle Informazioni (SGSI): certificato dal 2009 secondo la norma ISO/IEC 27001; e dal 2019 secondo le norme ISO/IEC 27017 (sicurezza nel cloud) e ISO/IEC 27018 (privacy nel cloud);
- Sistema di Gestione per la Salute e Sicurezza sul Lavoro (SGSSL): certificato dal 2020 secondo la norma ISO 45001;
- Sistema di Gestione per la Prevenzione della Corruzione (SGPC): certificato dal 2022 secondo la norma ISO 37001;
- Sistema di Gestione Ambientale (SGA): certificato dal 2023 secondo la norma ISO 14001.

Le politiche dei Sistemi di Gestione costituiscono uno strumento per il raggiungimento degli obiettivi strategici della Società e, al contempo, impegnano la stessa a soddisfare i requisiti applicabili e a migliorare in modo continuativo la propria azione. Esse sono definite dall'alta direzione, comunicate all'interno dell'organizzazione e rese disponibili alle parti interessate attraverso pubblicazione sul sito Internet aziendale.

L'approccio impiegato per raggiungere gli obiettivi si basa sui seguenti principi:

- approccio per processi: permette di pianificare i processi dell'organizzazione e le loro interazioni;
- ciclo Plan-Do-Check-Act: permette di assicurare che i processi e i sistemi di gestione siano adeguatamente dotati di risorse e gestiti e migliorati con continuità;
- risk-based thinking: permette di determinare i fattori che potrebbero fare deviare i processi e i sistemi di gestione aziendali dai risultati pianificati e di mettere in atto controlli preventivi per minimizzare gli effetti negativi e massimizzare le opportunità quando si presentano.

L'impianto dei processi definito per i sistemi di gestione, così come i risultati delle attività di valutazione e trattamento dei rischi effettuate all'interno di essi, vengono utilizzati come supporto per identificare le attività e le unità organizzative in corrispondenza delle quali potrebbero verificarsi illeciti rilevanti ai fini del D.Lgs. 231/2001, nonché per individuare controlli adeguati a contrastarli.

¹ Si veda in tal senso anche AUTORITÀ NAZIONALE ANTICORRUZIONE, *Whistleblowing Guida per la ricezione e la gestione delle segnalazioni Guida sintetica sul whistleblowing*; documento redatto nell'ambito del progetto SRSS / S2019 / 046 - 19IT22 Reinforcing the Institutional Corruption Prevention Community in Italy, finanziato dalla Commissione europea, 31 gennaio 2022, p.11



Nell'ambito del Sistema di Gestione per la Prevenzione della Corruzione, il Direttore Generale di Lepida, già R.P.C.T., è stato nominato Responsabile per la funzione di conformità per la prevenzione della corruzione, giusta Delibera del CdA n. D0522_25 e successivo provvedimento di nomina prot. 225393/out/GEN del 2022-05-25.

1.4 Obiettivo del documento

Il presente documento costituisce e descrive il Modello Organizzativo per la prevenzione dei reati previsti nel Decreto. Il Modello Organizzativo ha l'obiettivo di dare attuazione alle prescrizioni del Decreto mediante integrazione delle norme di condotta, dei principi, delle policies e delle procedure di Lepida, anche attraverso adeguati strumenti organizzativi e controlli preventivi.

Il ricorso all'integrazione delle differenti modalità di prevenzione e controllo esplicitate nel documento permette:

- il mantenimento del Sistema di governance già in essere, agendo sui processi che, direttamente o indirettamente, possono influenzare il sistema di gestione aziendale di Lepida e il Modello Organizzativo;
- di adottare, successivamente, anche altri Sistemi di governance (normativi, cogenti o volontari) sempre in modo integrato.

Il presente documento è soggetto a revisione periodica ad opera del Consiglio di Amministrazione come specificato al par. 4.2 *Adozione e modifiche del Modello Organizzativo*, in funzione del principio di miglioramento continuo posto alla base del sistema di governo dei processi aziendali.

Il Modello predisposto da Lepida si fonda su un sistema strutturato e organico di procedure nonché di attività di controllo che nella sostanza:

- individuano le aree o i processi di possibile rischio nell'attività aziendale, vale a dire quelle attività nel cui ambito si ritiene esista la possibilità che siano commessi i reati;
- definiscono un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi/reati da prevenire tramite:
 - un Codice Etico, che fissa le linee di orientamento generali, e procedure formalizzate, tese a disciplinare in dettaglio le modalità operative nei settori "sensibili";
 - l'individuazione di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni.
- delineano un sistema organizzativo con declaratorie chiare e coerenti, volte ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara e organica attribuzione dei compiti, applicando una giusta collocazione delle funzioni, assicurando che gli assetti voluti della struttura organizzativa siano realmente attuati;
- individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporre l'aggiornamento.

Pertanto il Modello si propone come finalità quelle di:

- migliorare il sistema di gestione della Società;



- predisporre un sistema strutturato e organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale con particolare riguardo alla riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome e per conto di Lepida nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti dell'Azienda;
- informare tutti coloro che operano, a qualsiasi titolo in nome, per conto o comunque nell'interesse di Lepida che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale;
- ribadire che Lepida non tollera comportamenti illeciti, di qualsiasi tipo e indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui la Società intende attenersi.

1.5 Campo d'applicazione

Il presente Modello Organizzativo è applicabile a tutti i soggetti a qualsiasi titolo coinvolti nei processi e attività aziendali a rischio di Lepida e nei confronti di tutti i Destinatari.

In particolare, l'osservanza del presente Modello si impone, dunque:

- a tutti coloro che, seppure incardinati presso Lepida, operino per conto o nell'interesse dei Soci;
- a tutti coloro i quali, pur non facendo parte dell'Azienda, operino per il conseguimento degli scopi e degli obiettivi di Lepida (collaboratori esterni, clienti/fornitori, Partner, etc).

Il Modello Organizzativo è soggetto a modifiche a seguito di cambiamenti derivanti dall'osservanza delle norme giuridiche in materia e loro integrazioni e variazioni; i principi e le metodologie del presente Modello Organizzativo trovano applicazione anche in riferimento a eventuali ulteriori ipotesi di reato successivamente integrate nel Decreto.

1.6 Allegati al documento

Oltre alla Parte generale e alla Parte speciale, costituiscono parte integrante del presente documento i seguenti allegati:

- **Allegato 1:** Codice Etico e di Comportamento di Lepida;
- **Allegato 2:** Piano triennale di prevenzione della corruzione e della Trasparenza - Misure integrative al MOG di Lepida (P.T.P.C.T.).



2. Il Decreto

2.1 Descrizione generale

Il Decreto Legislativo 8 giugno 2001 n. 231, avente ad oggetto la *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”*, sancisce la responsabilità amministrativa dell’ente per reati posti in essere da amministratori, dirigenti e/o dipendenti nell’interesse o a vantaggio dell’Ente stesso. Si tratta di un regime di responsabilità amministrativa (connessa sostanzialmente ad una responsabilità di natura penale) a carico degli Enti derivante dalla commissione di specifiche fattispecie di reato accertata dal giudice penale. Tale responsabilità si aggiunge a quella (*stricto sensu* penale) della persona fisica che ha realizzato materialmente il reato. Essa coinvolge il patrimonio dell’ente e, indirettamente, gli interessi economici dei soci.

Prima dell’entrata in vigore del Decreto, il principio di personalità della responsabilità penale posto dall’art. 27 Cost. precludeva la possibilità di condannare in sede penale gli Enti per reati commessi nel loro interesse, potendo invece sussistere soltanto una responsabilità solidale in sede civile per il danno eventualmente cagionato dal proprio dipendente, ovvero per l’obbligazione civile derivante dalla condanna al pagamento della multa o dell’ammenda del dipendente in caso di sua insolvenza.

La responsabilità è ora attribuibile all’Ente qualora i reati indicati dal Decreto siano stati commessi da soggetti legati a vario titolo all’Ente stesso e qualora il reato venga compiuto nell’interesse dell’Ente o a vantaggio (anche di natura “indiretta”) dello stesso.

Le disposizioni contenute nel Decreto si applicano a Enti dotati di personalità giuridica, società e associazioni anche prive di personalità giuridica. Restano invece esclusi lo Stato, gli Enti pubblici territoriali, gli altri Enti pubblici non economici, gli Enti che svolgono funzioni di rilievo costituzionale. Lepida rientra quindi tra i soggetti sottoponibili al regime della responsabilità amministrativa di cui al Decreto.

2.2 Reati presupposto

Si riportano in seguito le diverse classi di reato e le relative fattispecie previste dal Decreto:

Reati presupposto di cui al D.Lgs. 8 giugno 2001, n. 231			
Classe di reato	Articolo	Comma	Fattispecie
A) Indebita percezione di erogazioni, truffa in danno dello Stato, di un Ente pubblico o dell’Unione	24	1	Malversazione a danno dello Stato (316-bis c.p.)
			Indebita percezione di erogazioni a danno dello Stato (316-ter c.p.)
			Truffa aggravata in danno dello Stato o di altro Ente pubblico (art. 640, co. 2, n. 1 c.p.)



<p>Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture</p>			Truffa aggravata per il conseguimento di erogazioni pubbliche (640-bis c.p.)
			Frode informatica (640-ter c.p.) se commesso in danno dello Stato, di altro Ente pubblico o dell'Unione Europea
			Frode nelle pubbliche forniture (356 c.p.)
			Turbata libertà degli incanti (353 c.p.)
			Turbata libertà del procedimento di scelta del contraente (353 bis c.p.)
		2-bis	Delitti di cui all'art. 2 della Legge 23 dicembre 1986, n. 898
<p>B) Delitti informatici e trattamento illecito di dati</p>	24 bis	1	Accesso abusivo ad un sistema informatico o telematico (615-ter c.p.)
			Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater c.p.)
			Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 quinquies c.p.)
			Danneggiamento di informazioni, dati e programmi informatici (635 bis c.p.)
			Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (635 ter c.p.)
			Danneggiamento di sistemi informatici o telematici (635 quater c.p.)
Danneggiamento di sistemi informatici o telematici di pubblica utilità (635 quinquies c.p.)			



		1 bis	Estorsione informatica (art. 629, comma 3, c.p.)
		2	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 quater c.p.)
			Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (635 quater 1 c.p.)
		3	Falsità in documenti informatici (491 bis c.p.)
			Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.)
			Delitti di cui all'art. 1, co. 11, D.L. 21 settembre 2019, n. 105
C) Delitti di criminalità organizzata	24 ter	1	Associazione per delinquere (art. 416, co. 6, c.p.)
			Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.)
			Scambio elettorale politico-mafioso (art. 416 ter c.p.)
			Sequestro di persona a scopo di estorsione (art. 630 c.p.)
			Delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo
			Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DpR 309/1990)
		2	Associazione per delinquere (art. 416, c.p., eccetto comma 6)
			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 terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), n. 5) c.p.p.)
D) Peculato, indebita destinazione di denaro o cose mobili, concussione,	25	1	Corruzione per l'esercizio delle funzione (art. 318 c.p.)
			Pene per il corruttore (321 c.p.)
			Istigazione alla corruzione (322, co. 1 e 3, c.p.)
			Traffico di influenze illecite (346 bis c.p.)
			Peculato (314, co. 1, c.p.), quando sono offesi



<p>induzione indebita a dare o promettere utilità, corruzione</p>			interessi finanziari UE
			Indebita destinazione di denaro o cose mobili, quando sono offesi interessi finanziari dell' UE (art. 314 bis c.p.)
			Peculato mediante profitto dell'errore altrui (316 c.p.), quando sono offesi interessi finanziari UE
		2	Corruzione per un atto contrario ai doveri d'ufficio (319 c.p.)
			Corruzione in atti giudiziari (319 ter, co. 1 c.p.)
			Pene per il corruttore (art. 321 c.p.)
			Istigazione alla corruzione (art. 322, co. 2 e 4 c.p.)
		3	Concussione (317 c.p.)
			Corruzione per un atto contrario ai doveri d'ufficio aggravata quando dal fatto l'ente ha conseguito un profitto di rilevante entità (319 e 319 bis c.p.)
Corruzione in atti giudiziari (319 ter, co. 2, c.p.)			
Induzione indebita a dare o promettere utilità (319 quater c.p.)			
<p>E) Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento</p>	25 bis	1	Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (453 c.p.)
			Alterazione di monete (454 c.p.)
			Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (460 c.p.)
			Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (461 c.p.)
			Spendita e introduzione nello Stato, senza concerto, di monete falsificate (455 c.p.)
			Spendita di monete falsificate ricevute in buona fede (457 c.p.)
			Uso di valori di bollo contraffatti o alterati (464, co. 2, c.p.)
			Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (459 c.p.)
			Uso di valori di bollo contraffatti o alterati (464, co. 1, c.p.)
			Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e



			disegni (473 c.p.)
			Introduzione nello Stato e commercio di prodotti con segni falsi (474 c.p.)
F) Delitti contro l'industria e il commercio	25 bis.1	1	Turbata libertà dell'industria o del commercio (513 c.p.)
			Frode nell'esercizio del commercio (515 c.p.)
			Vendita di sostanze alimentari non genuine come genuine (516 c.p.)
			Vendita di prodotti industriali con segni mendaci (517 c.p.)
			Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (517 ter c.p.)
			Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (517 quater c.p.)
			Illecita concorrenza con minaccia o violenza (513 bis c.p.)
			Frodi contro le industrie nazionali (514 c.p.)
G) Reati societari	25 ter	1	False comunicazioni sociali (2621 c.c.)
			Fatti di lieve entità (2621 bis c.c.)
			False comunicazioni sociali delle società quotate (2622 c.c.)
			(2623, co. 1, c.c, abrogato dal DL 78/2009)
			(2623, co. 2, c.c, abrogato dal DL 78/2009)
			Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 1, c.c, abrogato dal D.Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D.Lgs. 39/2010)
			Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 2, c.c, abrogato dal D.Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D.Lgs. 39/2010)
			Impedito controllo (2625, co. 2, c.c.)
			Formazione fittizia del capitale (2632 c.c.)
			Indebita restituzione dei conferimenti (2626 c.c.)
			Illegale ripartizione degli utili e delle riserve (2627 c.c.)
			Illecite operazioni sulle azioni o quote sociali o della società controllante (2628 c.c.)
			Operazioni in pregiudizio dei creditori (2629 c.c.)
			Indebita ripartizione dei beni sociali da parte dei liquidatori (2633 c.c.)
Illecita influenza sull'assemblea (2636 c.c.)			
Aggiotaggio (2637 c.c.)			



			Omessa comunicazione del conflitto d'interessi (2629 bis c.c.) Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (2638, co. 1 e 2 c.c.) Corruzione tra privati (2635, co. 3 c.c.) Istigazione alla corruzione tra privati (2635 bis, co. 1 c.c.)
			False o omesse dichiarazioni per il rilascio del certificato preliminare di cui alla normativa attuativa della direttiva (UE) 2019/2121, del Parlamento europeo e del Consiglio, del 27 novembre 2019
H) Delitti con finalità di terrorismo o di eversione dell'ordine democratico	25 quater	1	Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali
I) Pratiche di mutilazione degli organi genitali femminili	25 quater.1	1	Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.)
J) Delitti contro la personalità individuale	25 quinquies	1	Riduzione o mantenimento in schiavitù o in servitù (600 c.p.) Tratta di persone (601 c.p.) Acquisto e alienazione di schiavi (602 c.p.) Intermediazione illecita e sfruttamento del lavoro (603 bis c.p.) Prostituzione minorile (600 bis, co. 1, c.p.) Pornografia minorile (600 ter, co. 1 e 2, c.p.) Prostituzione minorile (600 bis, co. 2, c.p.) Pornografia minorile (600 ter, co. 3 e 4, c.p.) Detenzione di materiale pornografico (600 quater c.p.) Adescamento di minorenni (609 undecies c.p.)
K) Abusi di mercato	25 sexies	1	Abuso di informazioni privilegiate (art. 184, D.Lgs. 58/1998) Manipolazione del mercato (art. 185, D.Lgs. 58/1998)
L) Omicidio colposo o lesioni gravi o gravissime commesse con	25 septies	1	Omicidio colposo (art. 589 c.p.) commesso con violazione dell'art. 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro



violazione delle norme sulla tutela della salute e sicurezza sul lavoro		2	Omicidio colposo (art. 589 c.p.) commesso con violazione delle norme in materia di tutela della salute e sicurezza sul lavoro
		3	Lesioni personali gravi (art. 590, co.3, c.p.) commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro
M) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	25 octies	1	Ricettazione (648 c.p.)
			Riciclaggio (648 bis c.p.)
			Impiego di denaro, beni o utilità di provenienza illecita (648 ter c.p.)
			Autoriciclaggio (648 ter.1 c.p.)
N) Delitti in materia di strumenti di pagamento diversi dai contanti	25 octies.1	1	Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (493 ter c.p.)
			Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (493 quater c.p.)
			Frode informatica, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (640ter c.p.)
		2	Ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti
		2 bis	Trasferimento fraudolento di valori (512 bis c.p.)
O) Delitti in materia di violazione del diritto d'autore	25 novies	1	Delitti in materia di violazione del diritto d'autore di cui agli artt: (171, co. 1, lett. a) bis e co. 3, L.633/1941); (171 bis L.633/1941); (171 ter L.633/1941); (171 septies L.633/1941); (171 octies L.633/1941).
P) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci	25 decies	1	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.)



mendaci all'autorità giudiziaria			
Q) ambientali	Reati 25 undecies	1	Inquinamento ambientale (452 bis c.p.)
			Disastro ambientale (452 quater c.p.)
			Delitti colposi contro l'ambiente (452 quinquies c.p.)
			Circostanze aggravanti (452 octies c.p.)
			Traffico e abbandono di materiale ad alta radioattività (452 sexies c.p.)
			Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (727 bis c.p.)
			Distruzione o deterioramento di habitat all'interno di un sito protetto (733 bis c.p.)
		2	Sanzioni penali (137, commi 3, 5, primo periodo, e 13, D.Lgs. 152/2006)
			Sanzioni penali (137, commi 2, 5, secondo periodo, e 11, D.Lgs. 152/2006)
			Attività di gestione di rifiuti non autorizzata (256, commi 1, lett. a), e 6 primo periodo, D.Lgs. 152/2006)
			Attività di gestione di rifiuti non autorizzata (256, commi 1, lett. b), 3, primo periodo, e 5 D.Lgs. 152/2006)
			Attività di gestione di rifiuti non autorizzata (256, comma 3, secondo periodo, D.Lgs. 152/2006)
			Bonifica dei siti (257, commi 1 e 2, D.Lgs. 152/2006)
			Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (258, co. 4, secondo periodo, D.Lgs. 152/2006)
			Traffico illecito di rifiuti (259, co. 1, D.Lgs. 152/2006)
			Attività organizzate per il traffico illecito di rifiuti (art. 260, co. 1 e 2 D.Lgs. 152/2006, ora 452 quaterdecies c.p.)
			Sistema informatico di controllo della tracciabilità dei rifiuti (260 bis, co. 6, 7 secondo e terzo periodo, 8 primo e secondo periodo, D.Lgs. 152/2006)
			Sanzioni (279, co. 5, D.Lgs. 152/2006)
		3	Art. 1, co. 1, L. 150/1992
			Art. 2, co. 1 e 2, L. 150/1992
			Art. 6, co. 4, L. 150/1992
			Art. 1, co. 2, L. 150/1992



			Fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996 (art. 3 bis, co. 1, L. n. 150/1992)
		4	Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3, co. 6, L. 549/1993)
		5	Inquinamento colposo (art. 9, co. 1, DLgs. 202/2007)
			Inquinamento doloso (art. 8, co. 1 e 9, co. 2, D.Lgs. 202/2007)
			Inquinamento doloso (art. 8, co. 2, D.Lgs. 202/2007)
R) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	25 duodecimes	1	Lavoro subordinato a tempo determinato e indeterminato (art. 22, co. 12 bis, D.Lgs. 286/1998)
		1 bis	Disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3-bis e 3-ter D.Lgs. 286/1998)
		1 ter	Disposizioni contro le immigrazioni clandestine (art. 12, co. 5, D.Lgs. 286/1998)
S) Razzismo e xenofobia	25 terdecimes	1	Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 3, co. 3 bis, L. 654/1975, ora 604 bis c.p.)
T) Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati	25 quaterdecimes		Frode in competizioni sportive (art. 1, L. 401/1989)
		1	Esercizio abusivo di attività di giuoco o di scommessa (art. 4 L. 401/1989)
U) Reati tributari	25 quindicimes	1	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, co. 1, D.Lgs. 74/2000)
			Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, co. 2-bis, D.Lgs. 74/2000)
			Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 74/2000)
			Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, co. 1, D.Lgs. 74/2000)



			<p>Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, co. 2-bis, D.Lgs. 74/2000)</p> <p>Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 74/2000)</p> <p>Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 74/2000)</p>
		<p>1-bis (delitti commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fini di evadere IVA per importi non inferiori a 10M €)</p>	<p>Dichiarazione infedele (art. 4, D.Lgs. 74/2000)</p>
			<p>Omessa dichiarazione (art. 5, D.Lgs. 74/2000)</p>
			<p>Indebita compensazione (art. 10-quater, D.Lgs. 74/2000)</p>
<p>v) Contrabbando</p>	<p>25 sex decies</p>	<p>1</p>	<p>Reati previsti dal testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi e relative sanzioni penali e amministrative, di cui al d.lgs. 504/1995</p>
<p>w) Delitti contro il patrimonio culturale</p>	<p>25-septies decies</p>	<p>1</p>	<p>Violazioni in materia di alienazione di beni culturali (518-novies c.p.)</p>
		<p>2</p>	<p>Appropriazione indebita di beni culturali (518-ter c.p.)</p>
			<p>Importazione illecita di beni culturali (518-decies c.p.)</p>
			<p>Uscita o esportazione illecite di beni culturali (518-undecies c.p.)</p>
		<p>3</p>	<p>Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (518-duodecies c.p.)</p>
			<p>Contraffazione di opere d'arte (518-quaterdecies c.p.)</p>
		<p>4</p>	<p>Furto di beni culturali (518-bis c.p.)</p>
<p>Ricettazione di beni culturali (518-quater c.p.)</p>			



			Falsificazione in scrittura privata relativa a beni culturali (518-octies c.p.)
X) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	25-duodevicies	1	Riciclaggio di beni culturali (518-sexies c.p.)
			Devastazione e saccheggio di beni culturali e paesaggistici (518-terdecies c.p.)

2.2.1 Ipotesi di concorso colposo o di cooperazione colposa nel reato presupposto

Come evidenziano alcuni interpreti, la responsabilità dell'Ente può realizzarsi non solo nel caso di commissione dolosa del reato presupposto, ma anche qualora il dipendente abbia concorso colposamente nel reato doloso commesso da terzi o abbia cooperato colposamente alla realizzazione dello stesso.

Rilevante, tra le altre, è la possibilità di **concorso colposo nei reati presupposto in materia di salute e sicurezza sul lavoro** (v. art. 25 septies del Decreto) **in materia di appalti**, laddove alla violazione colposa dell'obbligo della ditta appaltatrice di adottare adeguate misure preventive abbiano contribuito i criteri economici di aggiudicazione dell'appalto adottati dal committente o, ancor di più, la violazione dell'obbligo di valutare la congruità dei costi della sicurezza (art. 26, co.6 D.Lgs. 81/2008).

Considerazioni simili possono farsi per i reati presupposto in materia ambientale di cui all'art. 25 undecies del Decreto. La mancata valutazione da parte del committente circa il possesso da parte dell'appaltatore dei requisiti di legge per la gestione di rifiuti - come anche l'accettazione pedissequa di condizioni economiche di particolare vantaggio, se non addirittura fuori mercato - può ben costituire il presupposto per un **concorso colposo nel reato di gestione non autorizzata di rifiuti** di cui all'art. 256 D.Lgs. 152/2006.

Va comunque tenuto presente che, secondo l'orientamento giurisprudenziale dominante, il concorso colposo nel reato doloso è ammissibile sia nel caso di "cause colpose indipendenti" sia nel caso di "cooperazione colposa", purché (1) il reato del partecipe sia previsto anche nella forma colposa e (2) nella fattispecie siano effettivamente presenti tutti gli elementi che caratterizzano la colpa (ovvero (2a) il soggetto dev'essere titolare di una posizione di garanzia e di un obbligo di tutela o di protezione e (2b) la regola cautelare dal medesimo non osservata dev'essere diretta ad evitare il rischio dell'atto doloso del terzo). Così Cass. pen, sez. IV, sent. 34285/2011.

2.3 Soggetti attivi

In base al Decreto, uno dei presupposti indispensabili per il concretizzarsi della responsabilità dell'Ente, è che gli illeciti presupposti siano realizzati da:

- **persone che rivestono funzioni amministrative di amministrazione o di direzione dell'ente**, nonché da **persone che esercitano, anche di fatto, la gestione e il controllo**



- **dello stesso** (cd. soggetti apicali di cui all'art. 5, co. 1, lett. a);
- oppure, **persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera precedente** (cd. soggetti subordinati di cui all'art. 5, co. 1, lett. b).

Quanto alla categoria sub a), il Legislatore ha inteso fare riferimento a coloro i quali:

- siano titolari, all'interno della Società, di qualifiche formali, come quelle di rappresentante legale, amministratore, direttore generale, ad eccezione di quella di membro del collegio sindacale;
- svolgano funzioni di direzione in veste di Direttori di Dipartimento/Divisione/Progetto;
- seppure sprovvisti di una formale investitura, esercitino nei fatti attività di gestione e controllo della Società. La previsione, di portata residuale, è finalizzata a conferire rilevanza al dato fattuale, in modo da ricomprendere, tra gli autori dei reati da cui può derivare la responsabilità della società, non soltanto l'amministratore di fatto (ovvero colui che esercita in concreto, senza averne la qualifica, poteri corrispondenti a quelli dell'amministratore), ma anche, ad esempio, il socio azionista di maggioranza, che sia in grado di imporre la propria strategia aziendale e il compimento di determinate operazioni, anche nell'ambito di una società controllata, comunque agendo, attraverso qualsiasi forma idonea di controllo, sulla gestione concreta dell'ente.

Calata nell'organizzazione aziendale di Lepida, la locuzione "soggetti sottoposti all'altrui direzione o vigilanza" indica tutti gli altri dipendenti della Società, operanti nell'ambito dei Dipartimenti/Divisioni/Progetti o Aree aziendali.

2.4 Interesse o vantaggio per l'Ente

L'Ente **può essere ritenuto responsabile dell'illecito se il reato è stato commesso nel suo interesse o a suo vantaggio** (art. 5, co. 1). Al contrario, lo stesso non risponde di azioni compiute dai soggetti sopraindicati qualora le stesse nell'interesse esclusivo proprio o di terzi (art. 5, co. 2).

Da tali indici normativi, si desume che se un interesse dell'Ente - sia pure parziale o marginale - sussisteva, l'illecito dipendente da reato si configura anche se non si è concretizzato alcun vantaggio per l'impresa, la quale potrà al più beneficiare di una riduzione della sanzione pecuniaria.

Secondo l'impostazione elaborata con riferimento ai **reati dolosi**, la nozione di *interesse* si riferisce alla sfera volitiva della persona fisica e sarebbe valutabile al momento della condotta, mentre il *vantaggio* si identificherebbe nel complesso di benefici, economici e non, tratti dall'Ente.

Per i **reati colposi**, come quelli in materia di salute e sicurezza sul lavoro o ambientale, dovrebbe verificarsi se la condotta sia stata o meno determinata da scelte rientranti nell'interesse dell'ente: tale, ad esempio, sarebbe il risparmio di costi per la sicurezza ovvero il potenziare la velocità di esecuzione delle prestazioni o l'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici.



2.5 Condizioni di esenzione

In caso di reato commesso da un soggetto in posizione apicale e/o subordinato, l'Ente **non risponde del reato ove riesca a dimostrare** (art. 6, comma 1 del Decreto):

- che l'organo dirigente ha **adottato e attuato efficacemente**, prima della commissione del fatto, **un Modello di organizzazione e di gestione idoneo** a prevenire i reati verificatisi (lett. a);
- di aver **affidato a un Organismo di Vigilanza interno**, dotato di autonomi poteri di iniziativa e di controllo, **il compito di vigilare sul funzionamento e l'osservanza del Modello**, nonché di curarne l'aggiornamento (lett. b);
- che il reato è stato commesso da persone fisiche mediante **elusione fraudolenta del Modello di Organizzazione e di Gestione** (lett. c);
- che **non vi è stato un omesso o insufficiente controllo da parte dell'Organismo di Vigilanza** (lett. d).

Ne deriva che la Società non verrà sanzionata qualora le misure organizzative adottate e descritte nel Modello risultino:

- idonee a garantire lo svolgimento delle attività aziendali nel rispetto della legge e il monitoraggio e la successiva eliminazione tempestiva delle situazioni di rischio;
- efficaci, cioè proporzionate rispetto alle finalità normative e periodicamente aggiornate in relazione ad eventuali nuove esigenze individuate a seguito di cambiamenti nell'organizzazione o nelle attività svolte. Condizione necessaria per l'efficacia è l'introduzione di un sistema sanzionatorio volto ad individuare le sanzioni per il mancato rispetto delle misure organizzative stabilite.

2.6 Sanzioni

Come esplicitato all'art. 9 del Decreto, molteplici sono le sanzioni previste dal Decreto a fronte della commissione di un reato:

- **sanzione pecuniaria (artt. da 10 a 12)**, sempre prevista, e variabile nel suo ammontare secondo una valutazione discrezionale del giudice, nei limiti previsti per ciascun reato, da un minimo di 100 a un massimo di 1000 quote, in funzione dei seguenti elementi:
 - o gravità del fatto;
 - o grado di responsabilità della Società;
 - o attività svolta dalla Società per limitare/eliminare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

L'importo di ciascuna quota può variare fra i 258,00 € e i 1.549,00 € ed è stabilito in base alle condizioni economiche e patrimoniali della Società;

- **sanzioni interdittive (artt. da 13 a 17)** (*interdizione dall'esercizio della attività; sospensione/revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi*), esplicitamente prevista, per una serie di reati, a rafforzamento della sanzione pecuniaria e applicata (da un minimo di 3 mesi ad un massimo di 2 anni) qualora si verifichi almeno una delle seguenti condizioni:



- o profitto da reato di rilevante entità e reato commesso da soggetti in posizione apicale, o da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- o reiterazione degli illeciti.

Sono previste inoltre talune ipotesi di interdizione permanente dall'esercizio dell'attività (art. 16). L'interdizione dall'esercizio delle attività, anche temporanea, si applica soltanto quando l'irrogazione di altre sanzioni interdittive risulti inadeguata;

- **confisca del prezzo o del profitto del reato (art. 19)**, sempre disposta, anche per equivalente (può avere ad oggetto anche beni o altre utilità di valore equivalente);
- **pubblicazione della sentenza di condanna (art. 18)**, prevista solo per alcune fattispecie di reato.

La sanzione pecuniaria e la confisca sono pertanto sempre previste. A queste possono però aggiungersi le sanzioni interdittive (anche più di una, congiuntamente) e la pubblicazione della sentenza.

3. Quadro normativo di riferimento di Lepida

Al fine di rappresentare il contesto nel quale Lepida opera, si ritiene opportuno richiamare le principali previsioni normative che la Società è chiamata ad osservare; naturalmente, oltre a non poter essere inteso come esaustivo, l'elenco deve essere letto alla luce delle eventuali innovazioni che dovessero essere apportate all'ordinamento vigente.

L'elencazione è effettuata per materia e, all'interno di ciascuna materia, ordinata secondo un criterio di gerarchia delle fonti.

Società per azioni:

- Codice civile: artt. 2325 e ss. (*Società per azioni*), 2602 e ss. (*Dei consorzi per il coordinamento della produzione e degli scambi*) e 2615-ter (*Società consortili*) c.c.;

Società a partecipazione pubblica:

- Testo unico in materia di società a partecipazione pubblica (D.Lgs. 175/2016);

Legislazione regionale Emilia-Romagna regolante l'attività di Lepida:

- Razionalizzazione delle società in house della Regione Emilia-Romagna (L.R. 1/2018);
- Promozione degli investimenti in Emilia-Romagna (L.R. 14/2014);
- Sviluppo regionale della società dell'informazione (L.R. 11/2004).

Normativa generale in materia di attività amministrativa:

- Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi (L. 241/1990);
- Codice dell'amministrazione digitale (D.Lgs. 82/2005);
- Testo unico delle leggi sull'ordinamento degli Enti locali (D.Lgs. 267/2000);
- Modifiche al sistema penale (L. 689/1981);
- Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (D.P.R. 445/2000).



Normativa giuslavoristica e CCNL applicato:

- Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D.Lgs. 81/2008);
- Contratto collettivo nazionale di lavoro per i dipendenti da aziende del terziario distribuzione e servizi TDS;
- Contratto Integrativo Aziendale - Lepida.

Normativa relativa alla contrattualistica pubblica:

- Codice dei contratti pubblici (D.Lgs. 36/2023);
- Regolamento di esecuzione e attuazione del decreto legislativo 12 aprile 2006, n. 163, recante «Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE» (D.p.R. 207/2010).

Normativa relativa all'anticorruzione, incompatibilità e inconfiribilità degli incarichi:

- Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (L. 190/2012);
- Disposizioni in materia di inconfiribilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190 (D.Lgs. 39/2013).

Normativa in materia di trasparenza:

- Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni (D.Lgs. 33/2013).

Normativa in materia di protezione dei dati personali:

- Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (c.d. GPDR);
- Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (D.Lgs. 196/2003);
- Principali provvedimenti del Garante per la protezione dei dati personali.

Normativa in materia di identità digitale:

- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS - Electronic Identification Authentication and Signature);
- DPCM 24 ottobre 2014 *"Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese"*;



- Regolamento AgID recante le regole tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014);
- Linee guida AgID contenenti le Regole Tecniche per la sottoscrizione elettronica di documenti tramite SPID ex art. 20 del CAD approvate con Determinazione n. 157 del 23/03/2020;
- Regolamento AgID approvato con Determinazione n. 75/2023 che disciplina l'adesione al sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) da parte dei soggetti aggregatori.

Normativa in materia di comunicazioni elettroniche:

- Attuazione della direttiva 1999/5/CE riguardante le apparecchiature radio, le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità (D.Lgs. 269/2001);
- Codice delle comunicazioni elettroniche (D.Lgs. 259/2003);
- Testo unico dei servizi di media audiovisivi e radiofonici (D.Lgs. 177/2005);
- Approvazione del piano nazionale di ripartizione delle frequenze (D.M. 8 luglio 2002);
- Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti e ai servizi di telecomunicazioni (D.M. 28 maggio 2003);
- Specifiche tecniche delle interfacce radio regolamentate (D.M. 10 gennaio 2005).

Normativa in materia di Cybersicurezza

- Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (D.P.C.M. 30 luglio 2020, n. 131);
- Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", convertito con modificazioni dalla L. 4 agosto 2021, n. 109 (D.L. 14 giugno 2021, n. 82);
- Attuazione della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;
- Legge 90 del 28 giugno 2024: "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
- Decreto legislativo 4 settembre 2024, n.138 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148".

4. Modello di Organizzazione e di Gestione

4.1 Caratteristiche del Modello

Il Decreto prevede (art. 6) che il Modello Organizzativo debba avere determinate caratteristiche per fungere da elemento scriminante rispetto all'insorgere della responsabilità della Società, in caso di commissione di uno dei reati presupposto; tali caratteristiche guidano



l'implementazione stessa del Modello Organizzativo:

- *Mappatura dei Rischi*: analisi del **contesto aziendale**, di processi e prassi, per evidenziare le aree di attività a rischio e le modalità di commissione dei reati contemplati dal Decreto;
- *Progettazione del sistema di controllo*: **valutazione del Sistema di governance della Società** in termini di capacità di contrastare e/o ridurre efficacemente i rischi identificati, operando l'eventuale adeguamento del sistema stesso;
- *Definizione di un appropriato Sistema disciplinare e sanzionatorio*: da applicare nel caso di mancato rispetto delle disposizioni previste dal Modello Organizzativo;
- *Previsione degli obblighi di informazione dell'Organismo di Vigilanza*: previsione di specifiche e aggiornate modalità informative dell'OdV, per assicurare un controllo costante sulla Società;
- *Previsione di un'attività di monitoraggio sistematico*: diretta a far sì che periodicamente il funzionamento del Modello Organizzativo venga opportunamente verificato;
- *Previsione di un'attività di comunicazione e diffusione* del Modello Organizzativo.

4.2 Procedimento di adozione e modifica del Modello organizzativo

Il Modello Organizzativo di Lepida è adottato dal CdA; tutte le modifiche sostanziali del Modello Organizzativo derivanti, ad esempio, dall'introduzione di nuovi reati o attinenti alla valutazione del rischio, sono di competenza del CdA.

È compito dell'OdV portare all'attenzione del CdA le modifiche al Modello Organizzativo che si rivelino necessarie.

Le modifiche alla Mappatura dei Rischi, ad eccezione del metodo di calcolo del livello di rischi (illustrato al paragrafo 3.5), sono concordate fra l'OdV e il Responsabile dell'area/funzione aziendale interessata.

L'interpretazione del presente Modello Organizzativo è affidata a:

- OdV;
- CdA.

4.3 L'elaborazione del Modello

4.3.1 Principi generali

<p>Specificità</p>	<p>Pur considerando che l'idoneità del Modello Organizzativo debba essere parametrata a standard, best practice e linee guida disponibili in materia, le azioni di risk assessment e di gestione del rischio in senso lato devono aderire specificatamente all'organizzazione, al sistema di controllo esistente, nonché alle aree di attività e ai processi censiti e considerati "sensibili" ai reati presupposto individuati dalla normativa.</p>
---------------------------	--



	<p>Invero è lo stesso art. 6 del D.Lgs. 231/2001 che dispone che l'efficacia del modello organizzativo è subordinata alla previsione "di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire".</p>
Adeguatezza	<p>Si considera adeguato il Modello che consenta di prevenire i reati presupposto "applicabili". La giurisprudenza ha nel tempo individuato elementi che rappresentano evidenze marginali di adeguatezza del modello, come ad esempio:</p> <ul style="list-style-type: none"> • l'espressa indicazione nel Modello delle fattispecie illecite rispetto alle quali l'esposizione della Società risultata particolarmente sensibile e quelle per le quali si ritiene trascurabile; • opportuno bilanciamento tra presidi esplicitati nel Modello e rinvio all'impianto documentale esistente (soprattutto per quelle procedure ove siano dettagliati opportuni processi di controllo), al fine di garantire un idoneo livello di dettaglio nell'illustrazione delle cautele adottate dall'Ente al fine di prevenire il potenziale rischio di commissione dei reati presupposto; • protocolli/divieti presenti nel MOG e richiamo a procedure e regolamenti; • coordinamento, con riferimento ai reati previsti nel Modello, tra i controlli di linea di primo livello (insiti nelle procedure operative), di secondo livello (compliance, risk management, antiriciclaggio, ove applicabile) e di terzo livello (Internal Audit o Revisione Interna) previsti dal Modello e le procedure cui lo stesso rinvia; • coordinamento e integrazione del Modello con gli altri sistemi di gestione e controllo aziendale, con conseguente adeguamento dei suoi contenuti alla specifica realtà operativa di riferimento ai fini della concreta applicabilità delle prescrizioni in esso contenute.
Attuabilità e condivisione	<p>I protocolli e le misure organizzative siano aderenti alla struttura organizzativa dell'Ente e ai processi e macro aree censiti. È pertanto necessario prevedere un flusso informativo costante in seno all'organizzazione.</p>
Efficienza	<p>Deve esserci coerenza tra il Modello, i processi censiti, i punti di controllo, le procedure previste e la complessità strutturale dell'Ente.</p>
Dinamicità	<p>L'art. 7 del Decreto dispone che l'efficacia del Modello è certamente subordinata ad <i>"una verifica periodica e l'eventuale modifica dello stesso [...] quando intervengono mutamenti nell'organizzazione o nell'attività"</i> dell'Ente".</p>
Unità	<p>Il censimento dei processi e la correlata analisi dei rischi considera l'organizzazione nella sua interezza, anche ai fini della sensibilizzazione diffusa in ordine all'attuazione del Modello.</p>
Coerenza	<p>Il Modello deve assicurare coerenza con i processi censiti, il sistema dei controlli, il Codice Etico e di Comportamento, le sanzioni previste e coordinarsi con le determinazioni di cui al Piano triennale di prevenzione della corruzione e della trasparenza.</p>



Neutralità

La neutralità del Modello si persegue assegnando, ai soggetti che definiscono le procedure di controllo, un adeguato livello di autonomia nella rilevazione di eventuali carenze organizzative e le aree di rischio su cui intervenire strutturando gli opportuni meccanismi preventivi.

Il percorso di implementazione del Modello, conclusosi con l'approvazione del "Modello di organizzazione e di gestione" mediante specifica delibera del CdA, si è articolato nelle seguenti fasi:

Fase 1: analisi dei rischi e informativa al CdA

Sono verificate le potenziali modalità di commissione del reato, in relazione all'attività operativa, alla struttura organizzativa e ai processi effettivamente in essere all'interno dell'Ente, individuando, di conseguenza, le funzioni e le aree aziendali coinvolte nello svolgimento delle singole attività.

La necessità di un simile approccio è affermata dallo stesso Decreto 231 (art. 6, comma 2, lett. a), il quale, come in precedenza osservato, impone di *"individuare le attività nel cui ambito possono essere commessi i reati"*. Sono, conseguentemente, considerati:

- aree/funzioni coinvolte, al fine dell'individuazione del process owner e dei soggetti che intervengono nello svolgimento delle diverse attività, anche mediante interviste; a riguardo, anche in occasione dell'aggiornamento del MOG per l'anno 2024, l'Area Affari Legali, Societari & Privacy in collaborazione con l'OdV ha provveduto a somministrare apposito questionario ai Direttori dei Dipartimenti, Divisioni e Progetti e ai Responsabili di Area, al fine di acquisire una valutazione dei rischi reato quale base di lavoro per l'individuazione di nuovi eventuali presidi procedurali e/o per l'implementazione di quelli esistenti mediante integrazione delle norme di condotta, dei principi, delle policies e delle procedure di Lepida.

Alla rilevazione hanno partecipato 56 soggetti tra Responsabili di Area, Direttori di Dipartimenti, Divisioni e Progetti. Dalla disamina dei riscontri ricevuti si evince complessivamente una conoscenza diffusa del Modello e dei principi del Codice Etico e di Comportamento, così come delle procedure e dei regolamenti aziendali.

I riscontri acquisiti sono stati valorizzati nell'ambito dell'aggiornamento del Modello e saranno valutati anche ai fini dell'elaborazione del prossimo piano di formazione nell'ottica di assecondare i suggerimenti emersi verso una ulteriore focalizzazione concreta, nella realtà lavorativa quotidiana, delle condotte che possono assumere rilevanza ai fini della responsabilità amministrativa da reato;

- modalità di attuazione dell'illecito, con approfondimento relativo non solo ai reati direttamente realizzabili, ma anche a reati e attività *"strumentali"*;
- sistema di controllo interno e presidi di prevenzione esistenti;
- livello di rischio in relazione alla possibile commissione di reati-presupposto;
- valutazione dell'eventuale introduzione di nuove procedure di controllo e di mitigazione del rischio per indurre lo stesso alla condizione di *"accettabile"*;
- predisposizione del MOG per il CdA e condivisione dei risultati.

Fase 2: definizione Modello Organizzativo e delibera del CdA



Solo in un momento successivo all'analisi dei rischi e alla conseguente informativa nei confronti del CdA, si è dato seguito a:

- istituzione dell'Organismo di Vigilanza;
- definizione di: modello di organizzazione e di gestione; codice etico e di comportamento; sistema disciplinare;
- delibera del CdA per l'approvazione del modello e dell'OdV istituito.

Fase 3: aggiornamento Modello Organizzativo

Trattandosi di un documento da ritagliare sulla base dell'organizzazione e dell'attività aziendale, lo stesso è soggetto a periodica revisione, solitamente annuale, e approvazione da parte del CdA.

4.4 Metodo di analisi dei rischi adottato e attività svolte

L'analisi dei rischi è stata condotta con l'obiettivo di individuare i processi, le attività aziendali e le unità organizzative in corrispondenza delle quali si potrebbero configurare i reati previsti dal Decreto legislativo, causando una responsabilità in capo alla Società.

Tale attività è stata compiuta a partire da un'analisi preventiva del contesto in cui opera la Società e della documentazione aziendale ritenuta di interesse:

- Statuto di Lepida;
- Piano triennale di prevenzione della corruzione e della Trasparenza - Misure integrative al MOG di Lepida (P.T.P.C.T.);
- Contratto di servizio 2024-2026 e relative integrazioni tra la Regione Emilia-Romagna e la Società Lepida;
- Convenzione-Quadro per l'esercizio del controllo analogo congiunto su "LEPIDA s.c.p.a.";
- Contratto collettivo nazionale di lavoro per i dipendenti da aziende del terziario distribuzione e servizi TDS e Contratto Integrativo Aziendale;
- Norme di trasparenza di gestione Lepida;
- Procura speciale conferita al Direttore Generale e specifici mandati conferiti dal Consiglio di Amministrazione;
- Regolamenti interni della società pubblicati sulla Intranet aziendale;
- Declaratorie della struttura organizzativa;
- Piano Industriale Pluriennale 2024-2026;
- Politiche e procedure della società pubblicate sulla Intranet aziendale;

Nella presente revisione è stato considerato l'organigramma di Lepida adottato a partire dal 1/1/2024 che vede la riorganizzazione di alcuni Dipartimenti con conseguente modifica della struttura societaria.

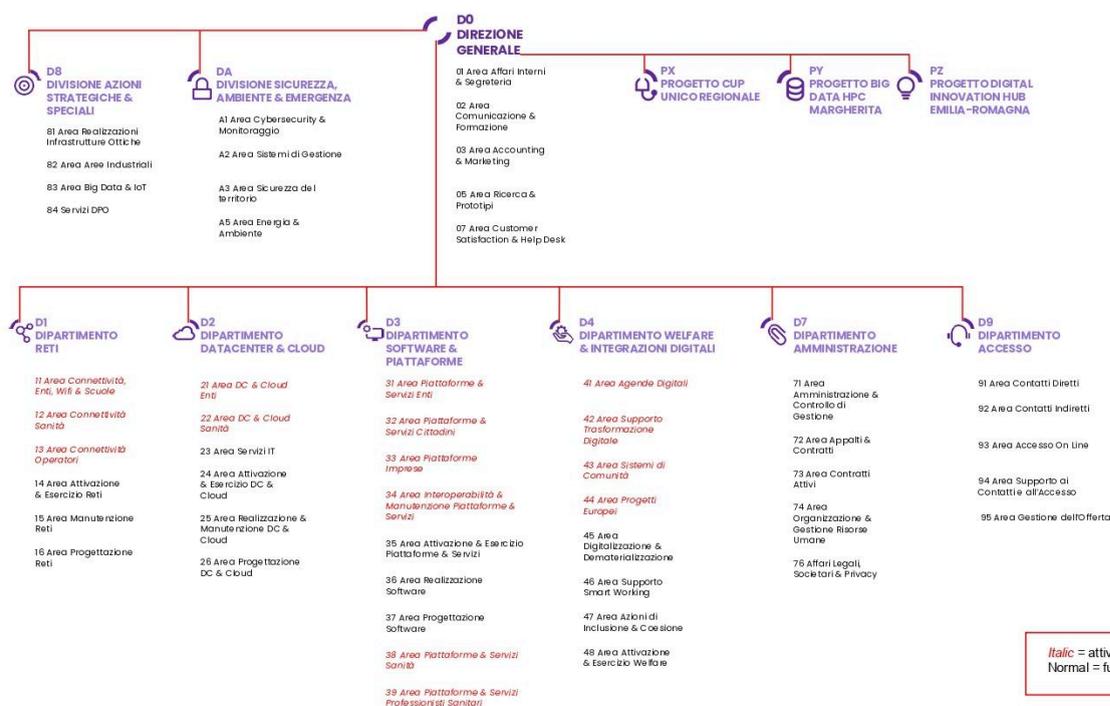
Di seguito, il nuovo organigramma di Lepida come integrato e modificato a partire dal 1/1/2024:

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali



- D7 - Dipartimento Amministrazione
- D8 - Divisione Progetti Strategici & Speciali
- D9 - Dipartimento Accesso
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

Organigramma di Lepida



La struttura societaria operativa a partire dal 1/1/2024 ha comportato la fusione dei Dipartimento Integrazioni Digitali (D4) e del Dipartimento Welfare Digitale (D5), ora uniti nell'unico Dipartimento Welfare & Integrazioni Digitali (D4).

La nuova organizzazione non innova in modo determinante rispetto all'impostazione precedente. Nonostante ciò, ai fini della mappatura e censimento delle aree a rischio, anche per l'anno 2024, è stata condotta un'analisi puntuale che tiene conto della nuova organizzazione aziendale.

Si dà atto che il Piano industriale triennale 2025 - 2027 già approvato dal Consiglio di Amministrazione della Società in data 18 ottobre 2024, che verrà portato all'approvazione dell'organo espressione del controllo analogo congiunto, il Comitato Permanente di Indirizzo e



Coordinamento ed, infine dell'Assemblea Ordinaria dei Soci, contempla alcune variazioni all'organigramma aziendale che saranno efficaci con decorrenza dal 1° gennaio 2025. L'analisi dei rischi per l'anno 2025 sarà, pertanto, condotta anche con riferimento a tali modifiche, per appurare se vi siano impatti determinanti ai fini dell'individuazione dei presidi aziendali di prevenzione di fattispecie rilevanti ai sensi del D.Lgs. 231/2001.

Sono stati valutati i processi e le attività aziendali nell'espletamento dei quali si potrebbero configurare i reati previsti dal Decreto.

Nell'analisi dei rischi e nell'identificazione delle fattispecie di reato di più probabile realizzazione, si è tenuto conto dei seguenti elementi:

- i reati rilevanti ex D.Lgs. 231/2001 sono normalmente di tipo doloso (è pertanto necessaria la volontà di compiere il fatto), salvo alcune ipotesi specifiche di reato colposo espressamente indicate;
- il reato deve essere commesso, in tutto o in parte, nell'interesse della Società o con l'obiettivo di farle ottenere un vantaggio (i comportamenti illeciti posti in essere per conseguire un vantaggio esclusivamente personale non fanno sorgere alcuna responsabilità dell'Ente);
- il reato deve essere commesso da persone che dirigono/controllano l'azienda (cc.dd. soggetti in posizione apicale) o che sono sottoposte alla vigilanza di queste.

L'analisi preventiva ha pertanto portato a identificare i reati configurabili nel concreto contesto operativo di Lepida e ad escludere metodologicamente alcune classi e/o specifiche fattispecie di reato.

La metodologia adottata prevede di affrontare il problema con una strategia di tipo bottom-up, consistente in:

- identificazione degli elementi di rischio (attività e reati);
- valutazione degli elementi in termini di correlazione attività/rischio-reato;
- calcolo del rischio potenziale (o assoluto);
- valutazione dell'impatto dei sistemi di controllo esistenti sul rischio potenziale;
- definizione del rischio residuo.

Mentre il **rischio potenziale** è quello ontologicamente correlato alle attività censite, il **rischio residuo** è quello riscontrabile a valle dell'applicazione degli strumenti di prevenzione e controllo messi in atto dalla Società.

4.4.1 Identificazione delle macroattività a rischio reato

L'art. 6 del D.Lgs. 231/2001 presuppone l'analisi delle attività svolte nell'ambito della Società al fine di individuare quelle che, in aderenza al Decreto, possono considerarsi a rischio di illeciti. Pertanto, sono state analizzate le attività svolte dai singoli Dipartimenti/Divisioni/Progetti, rilevati i profili di omogeneità che caratterizzano ciascuna di queste e, sulla scorta di questi, sono state declinate le macroaree rilevanti ai fini dell'analisi del "rischio reato", così come richiesto dalla normativa in questione.



4.4.2 Calcolo della gravità del reato

Ai fini della valutazione della gravità di un reato, sono stati considerati esclusivamente profili oggettivi, derivanti dalla valutazione del “peso” afferente alle pene pecuniarie e alle pene interdittive.

4.4.2.1 Le sanzioni interdittive

Queste ultime al momento sono costituite da:

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

Ad ogni sanzione è stato assegnato un determinato indice di gravità, tenendo in debita considerazione la natura di società in house di Lepida. Tale perno di valutazione produce effetti significativi - rispetto, ad esempio, a quanto accade per enti sostanzialmente privatistici - sulla valutazione fatta, come si può dedurre dall'aver assegnato un indice di gravità equivalente alla sanzione di cui alla lettera C) e a quella di cui alla lettera A). Specificatamente:

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

4.4.2.2 Le sanzioni pecuniarie

La sanzione pecuniaria, come noto, è invece misurata dal legislatore sulla base di quote, da applicarsi in numero non inferiore a 100 né superiore a 1.000, e il cui importo unitario è compreso tra i 250 e i 1.500 euro. Il numero minimo di quote applicabili è naturalmente 0. Conseguentemente, le pene pecuniarie sono state suddivise in 4 differenti fasce, con riferimento al numero massimo di quote previsto per il singolo reato presupposto:



Sanzioni pecuniarie	livello
100-325	1
326-550	2
551-775	3
776-1000	4

4.4.3 L'indice di gravità del reato

Nonostante, in concreto, le pene pecuniarie e interdittive possano essere applicate anche congiuntamente, nel valutare la gravità del singolo illecito presupposto, le stesse sono state considerate e pesate separatamente.

Il Modello, come riferito, tiene in debita considerazione la natura di società in house di Lepida e, pertanto, si è ricollegato alla comminatoria di sanzioni di tipo interdittivo un impatto decisamente più grave di quello riscontrabile nel caso di sanzioni esclusivamente pecuniarie. Da ciò consegue che, ai fini del calcolo dell'indice di gravità del reato, è necessario soppesare i livelli di impatto delle due tipologie di sanzioni in aderenza a quanto rappresentato nel periodo precedente.

I pesi sono, quindi, determinati come segue:

- **Sanzione interdittiva: 0,8**
- **Sanzione pecuniaria: 0,2**

L'indice di Gravità del Reato è quindi l'output che deriva dalla seguente formula:

$$GR = 0,8 \cdot Si + 0,2 \cdot Sp$$

L'indice di gravità è poi normalizzato a 100.

4.4.4 Indice di correlazione del reato

L'indice di correlazione tra attività e reato è il prodotto delle valutazioni effettuate sui seguenti parametri qualitativi:

- Semplicità di commissione del fatto di reato: ovverosia più è semplice commettere il reato, maggiore sarà l'indice di correlazione;
- Frequenza con cui l'attività è espletata: ovverosia più l'attività è frequente, più aumenta la probabilità di commissione e conseguentemente più alto è l'indice;
- Autonomia, livello e potere del soggetto responsabile dell'attività: ovverosia all'aumentare del potere e dell'apicalità di coloro che operano sull'attività aumenta l'indice.

I suddetti parametri sono stati declinati come segue:

Semplicità commissione reato	Livello
non semplice	1



poco semplice	2
semplice	3
molto semplice	4
Frequenza attività	Livello
non frequente	1
poco frequente	2
frequente	3
molto frequente	4
Autonomia, livello e potere del soggetto responsabile dell'attività	Livello
no autonomia	1
poca autonomia	2
media autonomia	3
molta autonomia	4

L'indice è costituito dalla somma dei 3 parametri sopraindicati, normalizzati a 100.

4.4.5 Calcolo del rischio potenziale (o assoluto)

Il rischio potenziale si ottiene a mezzo del prodotto tra l'indice di gravità del reato e l'indice di correlazione del reato:

$$RP: GR*ICR$$

Anche tale valore viene normalizzato a 100.

I livelli di rischio sono classificati come segue:

Rischio potenziale		
Valore	Livello	Descrizione
0	0	Nulla
>0 & <35	1	Basso
>=35 & <75	2	Medio
>= 75	3	Alto

Tale output costituisce, a tutti gli effetti, il ranking delle attività in base al rischio connesso alla loro esecuzione.



4.4.6 Calcolo dell'efficacia dei controlli

Una volta individuati i controlli posti in essere dalla Società si è scelto di assegnare loro un peso massimo sulla base della seguente tabella.

Elenco Controlli	Codice ID	Peso massimo
Piano triennale di prevenzione della corruzione e della trasparenza	C1	0,075
Codice Etico e di Comportamento	C2	0,075
Regolamenti aziendali	C3	0,075
Politiche e Procedure aziendali	C4	0,075
Poteri autorizzativi e segregation of duty	C5	0,100
Audit interni	C6	0,075
Audit di terza parte	C7	0,075
Sensibilizzazione e formazione del personale	C8	0,100
Tracciabilità e accountability delle operazioni	C9	0,100
Modello di Organizzazione e Gestione	C10	0,100
Norme di Trasparenza di Gestione	C11	0,100
Sistema di Gestione integrato	C12	0,050
TOTALE		1,000

L'effettiva capacità, dei controlli posti in essere, di ridurre il rischio potenziale per ciascun reato viene valutata assegnando all'insieme dei controlli applicati a quel reato un valore di efficacia non superiore al peso massimo dei controlli applicabili.

4.4.7 La valutazione del rischio residuo

Riducendo il valore del rischio potenziale sulla base della valutazione dell'efficacia dei controlli applicati si ottiene il rischio residuo. Questo è considerato accettabile solo se "NULLO" o "BASSO".

Rischio residuo

Valore

<35

ACCETTABILE



>=35	NON ACCETTABILE
------	--------------------

All'emergere di livelli di rischio "NON ACCETTABILE", la Società ha predisposto o, in mancanza, predisporrà specifici controlli aggiuntivi (ad esempio l'introduzione di una specifica Procedura) al fine di riportare il suddetto livelli di rischio nel cluster del rischio "ACCETTABILE".

4.5 L'analisi dei rischi

La valutazione preventiva della realtà aziendale ha consentito di identificare, mediante successive approssimazioni, attività e processi a particolare rischio di reato, al fine di meglio individuare controlli e strategie di riduzione dello stesso.

FASE 0 - IDENTIFICAZIONE DEI REATI DA ESCLUDERE EX ANTE, ovvero dei **reati** che, pur essendo ricompresi nel catalogo del D Lgs. 231/2001, siano da ritenersi **non configurabili già a livello astratto**, in considerazione degli elementi costitutivi della fattispecie, dell'attività svolta da Lepida e/o dall'impossibilità di configurare un vantaggio per la Società ([§ 4.5.1 Identificazione dei reati esclusi ex ante](#)).

*

FASE 1 - VALUTAZIONE DI ACCETTABILITÀ DEL RISCHIO REATO, A FRONTE DEGLI STRUMENTI DI CONTROLLO PREDISPOSTI A LIVELLO SOCIETARIO CENTRALE

In un primo momento, l'esame della realtà aziendale si è mantenuto ad un livello generale, che ha permesso di valutare il complesso dei flussi di lavoro e identificare i punti di maggior rischio di verifica degli illeciti. Concordemente, in questa prima fase, ad essere analizzati sono gli strumenti di tutela aventi portata generale (lo svolgersi dell'attività all'interno della singola Divisione/Area è invece rimandato alla successiva **FASE 2**). In particolare, si sono susseguiti due momenti:

1. **DETERMINAZIONE DELL'INDICE DI GRAVITÀ DEI REATI**: si è anzitutto proceduto a valutare l'**Indice di gravità** dei reati astrattamente configurabili ([§ 4.4.3](#));
2. **IDENTIFICAZIONE DELLE MACROATTIVITÀ INTERESSATE E DETERMINAZIONE DELL'INDICE DI CORRELAZIONE**: è stata successivamente effettuata una prima valutazione delle macroattività aziendali ([§ 4.5.2 Identificazione delle macroattività a rischio](#)), al fine di desumere, rispetto alle stesse, gli elementi qualitativi (semplicità di commissione, frequenza dell'attività e autonomia decisionale) necessari a determinare il cd. **Indice di correlazione** ([§ 4.4.4](#)) e, conseguentemente, il **Rischio potenziale** derivante dalla commissione del singolo reato ([§ 4.4.5](#));
3. **VERIFICA DELL'EFFICACIA DEI CONTROLLI PREDISPOSTI A LIVELLO CENTRALE RISPETTO AI SINGOLI FLUSSI DI LAVORO**: la prima fase d'analisi è terminata con la determinazione di un **Rischio residuo** ([§ 4.4.7](#)) "di primo grado", mediante l'interconnessione tra flussi di



lavoro e controlli centrali predisposti, così identificando, in relazione ai singoli processi societari:

- a. ipotesi di reato con un rischio residuo di primo grado ACCETTABILE;
- b. e ipotesi di reato a rischio residuo di primo grado NON ACCETTABILE.

*

FASE 2 - CONTROLLI PERIFERICI E ATTIVITÀ IN CUI RESIDUA UN MAGGIOR RISCHIO CONCRETO

Solo una volta conclusa la prima fase di analisi (**FASE 1**), si è proceduto ad innestare nel quadro fino a quel momento delineato gli strumenti predisposti in relazione a specifiche attività riconducibili a determinate Divisioni/Aree, al fine di comprendere se l'esame delle specifiche attività svolte permettesse di riscontrare l'esistenza di ulteriori strumenti di sicurezza implementati a livello periferico in modo da ottenere, per attività particolarmente critiche, un rischio residuo "di secondo grado" questa volta ACCETTABILE.

1. Si è, pertanto, proceduto ad individuare e incrociare:
 - a. le **MACROATTIVITÀ PARTICOLARMENTE SENSIBILI**, ovvero nell'ambito delle quali è più probabile la realizzazione di illeciti presupposto ex D.Lgs. 231/2001 ([§4.5.3 Identificazione delle Macroattività particolarmente sensibili](#));
 - b. con le **FATTISPECIE DI REATO A MAGGIOR RISCHIO POTENZIALE**, la cui realizzazione determinerebbe le conseguenze più gravi per la continuità della vita societaria ([§4.5.4 Identificazione delle Fattispecie di reato a maggior rischio potenziale](#)).

Si è ritenuto, in tal modo, di poter individuare i punti di maggiore criticità dell'attività societaria, al fine (1) di verificare l'esistenza di specifiche procedure o tutele in grado di limitare ulteriormente il rischio reato o, in alternativa, (2) di programmare l'elaborazione di specifici strumenti di tutela e prevenzione.

2. Si è, pertanto, proceduto a **verificare l'efficacia degli ulteriori strumenti di sicurezza implementati a livello periferico** in modo da ottenere, per le attività e i processi aziendali particolarmente critici, un rischio residuo "di secondo grado" questa volta ACCETTABILE.

FASE 3 - PREDISPOSIZIONE DI CONTROLLI SPECIFICI ED ULTERIORI: l'incrocio compiuto nella fase di cui al punto precedente, costituisce la base conoscitiva indispensabile alla predisposizione della PARTE SPECIALE del presente Modello organizzativo e di gestione.

In essa, infatti, sono elencate, per ciascuna Macroattività particolarmente sensibile ([§4.5.3](#)), le Divisioni societarie maggiormente esposte e le Fattispecie di reato a maggior rischio potenziale ([§4.5.4](#)): il ruolo centrale, tuttavia, è naturalmente svolto dall'analisi delle specifiche misure di controllo e di contrasto predisposte dalla Società al fine di scongiurare il rischio di commissione degli illeciti considerati.



Ove non presenti strumenti adeguati – per l’assenza o insufficienza di quelli presenti – Lepida individua già nel MOG le misure di più urgente adozione al fine dell’ulteriore contenimento del rischio reato.

I risultati esposti non possono considerarsi come un dato definitivo e immutabile, ma, al contrario, sono sottoposti ad una continua attività di controllo e revisione, anche in ragione dei mutamenti strutturali o di attività che Lepida si trova ad affrontare. La Società programma, pertanto, specifici momenti di verifica dell’aggiornamento dell’analisi svolta.

4.5.1 Identificazione dei reati esclusi ex ante

Alcune delle fattispecie di reato presupposto, pur essendo previste dal D.Lgs. 231/2001, non si ritengono concretamente attuabili nell’ambito dell’organizzazione di Lepida.

L’elemento oggettivo dei reati in considerazione – alla luce dei peculiari elementi costitutivi richiesti dal legislatore al fine del perfezionamento della fattispecie – si è ritenuto di scarsissimo se non nullo rilievo concreto, in considerazione delle attività sociali poste in essere da Lepida; ciò, anche a considerare la clausola generale della responsabilità per colpa (art. 40, co. 2 c.p.), il mero tentativo di reato (art. 56 c.p.) o la forma plurisoggettiva eventuale (art. 110 e ss. c.p.).

L’analisi sul punto ha tenuto conto del *bene giuridico* tutelato dalla previsione, della *titolarità* dello stesso; del *soggetto attivo* e di quello *passivo* del reato; della specifica *condotta* richiesta, anche alla luce del principio di frammentarietà del diritto penale; infine, dell’*evento naturalisticamente considerato*, oltre che di quello *giuridico* necessari al perfezionamento della fattispecie criminosa.

Disposizione del D.Lgs. 231/2001	Riferimenti normativi specifici	Valutazione
<p>24 ter (Delitti di criminalità organizzata)</p>	<ul style="list-style-type: none"> • Sequestro di persona a scopo di estorsione (art. 630 c.p.); • Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DpR 309/1990); • 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 	<p>Tenuto conto della natura dell’attività e dell’oggetto sociale di Lepida, si esclude ex ante la possibilità che tali fattispecie di reato possano trovare applicazione nell’ambito delle attività di Lepida stessa e, nell’interesse o a vantaggio della stessa Società.</p> <p>Nello specifico, è la stessa condotta tipica descritta nelle singole fattispecie di reato qui elencate a precludere la possibilità che tali ipotesi delittuose possano essere</p>



	<p>armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), n. 5) c.p.p.).</p>	<p>realizzate nell'interesse o a vantaggio di Lepida.</p>
<p>25 bis.1 (Delitti contro l'industria e il commercio)</p>	<ul style="list-style-type: none"> • Turbata libertà dell'industria o del commercio (513 c.p.); • Illecita concorrenza con minaccia o violenza (513-bis c.p.); • Frodi contro le industrie nazionali (514 c.p.); • Frode nell'esercizio del commercio (515 c.p.); • Vendita di sostanze alimentari non genuine come genuine (516 c.p.); • Vendita di prodotti industriali con segni mendaci (517 c.p.); • Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (517-ter c.p.); • Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (517-quater c.p.). 	<p>Lepida, quale società in house providing, non opera in concorrenza con altre imprese private. Inoltre, non svolge attività di produzione di beni materiali o di natura industriale. Considerata la platea dei destinatari delle attività del proprio core business - Enti Soci - non può dirsi configurabile un interesse all'utilizzo di privative e/o titoli di proprietà industriale, marchi e/o segni distintivi di soggetti terzi. Pertanto, non si riscontra in Lepida la presenza di rischi rispetto alla concreta configurabilità di tali fattispecie criminose. La rilevanza di condotte implicanti profili di responsabilità inerenti la proprietà intellettuale e il diritto d'autore viene valutata in sede di analisi dei delitti in materia di diritto d'autore.</p>
<p>25 quater (Delitti con finalità di terrorismo o di eversione dell'ordine democratico)</p>	<ul style="list-style-type: none"> • Delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali. 	<p>I reati cui si riferisce l'art 25 quater sono connotati dal riferimento finalistico della condotta; da ciò consegue che la quasi totalità del quadro dei reati previsti dal nostro ordinamento potrebbe essere ricompreso in tale disposizione. A tal proposito, sebbene in un'ottica meramente prudenziale, sono state considerate casistiche</p>



		<p>residuali, ad esempio relative all'utilizzo di fondi a favore di soggetti che intendono porre in essere reati di terrorismo. Si è ritenuto che tali casistiche non siano suscettibili di essere applicate alla realtà societaria di Lepida, considerato che la Società ha rapporti quasi esclusivamente con Enti pubblici e che è sottoposta al controllo analogo dei propri Soci che, evidentemente non operano in territori ad elevata attività terroristica o, comunque, da ritenersi "sensibili" alla categoria di reato sopra rappresentata. In ogni caso Lepida ha informato il proprio Codice Etico e di Comportamento e le proprie policy aziendali a principi e regole di condotta volti ad evitare/stigmatizzare qualsiasi comportamento potenzialmente prodromico alla realizzazione di atti con finalità di terrorismo.</p> <p>Vista comunque l'importanza strategica delle reti di telecomunicazione gestite dalla Società, Lepida ha ritenuto di valutare eventuali profili di rischio attinenti alla commissione di reati in materia di terrorismo o eversione dell'ordinamento democratico all'interno della Parte Speciale del presente Modello.</p>
<p>25 ter (Reati societari)</p>	<p>False o omesse dichiarazioni per il rilascio del certificato preliminare di cui alla normativa attuativa</p>	<p>Lepida in quanto società in house providing della Regione Emilia-Romagna e di altri Enti</p>



	<p>della direttiva (UE) 2019/2121, del Parlamento europeo e del Consiglio, del 27 novembre 2019.</p>	<p>Soci, non potrebbe realizzare operazioni di fusioni transfrontaliere, ovvero, fusioni con società costituite ai sensi di una legge diversa da quella nazionale.</p> <p>Viene meno, dunque, già ex ante, uno degli elementi della fattispecie criminosa oggetto di analisi: l'elemento soggettivo, e in particolare, il dolo specifico costituito dalla finalità, perseguita dal soggetto agente, di rendere false dichiarazioni al fine del rilascio del certificato preliminare necessario, ex art. 29 D.Lgs. 19/2023, per prendere parte all'operazione di fusione transfrontaliera.</p>
<p align="center">25 quater.1 (Pratiche di mutilazione degli organi genitali femminili)</p>	<ul style="list-style-type: none"> • Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.). 	<p>Tenuto conto della natura dell'attività e dell'oggetto sociale di Lepida, si esclude la possibilità che tali fattispecie di reato possano trovare applicazione nell'ambito delle attività di Lepida stessa; ciò anche, tenuto conto degli interventi giurisprudenziali in materia che hanno coinvolto prevalentemente cliniche e strutture sanitarie.</p>
<p align="center">25 quinquies (Delitti contro la personalità individuale)</p>	<ul style="list-style-type: none"> • Riduzione o mantenimento in schiavitù o in servitù (600 c.p.); • Tratta di persone (601 c.p.); • Acquisto e alienazione di schiavi (602 c.p.); • Intermediazione illecita e sfruttamento del lavoro (603 bis c.p.); • Prostituzione minorile (600 bis, co. 1, c.p.); • Pornografia minorile (600 ter, co. 1 e 2, c.p.). 	<p>Anche la commissione di tale famiglia di reati dovrebbe essere preordinata alla realizzazione di un interesse o vantaggio per Lepida che, in tale ambito, non si riscontra, neanche potenzialmente. Tale valutazione è supportata dalla casistica giurisprudenziale in materia che riguarda realtà aziendali operanti nel campo dell'editoria e/o del turismo, nell'ambito delle quali possono</p>



	<ul style="list-style-type: none"> • Prostituzione minorile (600 bis, co. 2, c.p.); • Pornografia minorile (600 ter, co. 3 e 4, c.p.); • Detenzione di materiale pornografico (600 quater c.p.); • Adescamento di minorenni (609 undecies c.p.). 	<p>essere somministrati servizi. aggiuntivi collaterali connessi ai reati di tale categoria (ad es. prostituzione minorile e pedopornografia). Con specifico riferimento, invece, ai reati correlati alla schiavitù, e alle condotte di procacciamento illegale della forza lavoro attraverso il traffico di migrazione anche clandestina, si ritiene che nel contesto di Lepida tali condotte non siano realizzabili, neanche come tentativo, sia per ragioni connesse all'oggetto sociale perseguito sia alle procedure di reclutamento di personale paragonabili a quelle degli Enti pubblici.</p>
<p>25 sexies (Abusi di mercato)</p>	<ul style="list-style-type: none"> • Abuso di informazioni privilegiate (art. 184, D.Lgs. 58/1998); • Manipolazione del mercato (art. 185, D.Lgs. 58/1998). 	<p>Si ritiene di poter escludere tali reati dal novero dell'analisi proprio in quanto Lepida ha natura di Società in house.</p> <p>Ciò comporta, da un lato, l'eterodirezione della Società da parte della Regione Emilia-Romagna e degli altri Enti Soci, che ne controllano l'attività e ne orientano le fondamentali scelte strategiche ed economiche; e, dall'altro, che, ai sensi dell'art. 16 D.Lgs. 175/2016 e dello Statuto sociale, Lepida deve effettuare oltre l'ottanta per cento del proprio fatturato nello svolgimento dei compiti a essa affidati dagli Enti pubblici Soci.</p> <p>Il citato art. 16 D.Lgs. 175/2016 specifica inoltre che la produzione ulteriore rispetto al limite di fatturato di cui sopra - che può essere rivolta anche a finalità diverse - è consentita solo a condizione che la stessa permetta di conseguire</p>



		economie di scala o altri recuperi di efficienza sul complesso dell'attività principale della Società. Infine, i rischi concernenti i reati di abuso di informazioni privilegiate e di manipolazione del mercato non risultano concretamente ipotizzabili, poiché Lepida non è quotata in alcun mercato regolamentato.
Art 25 duodecies (Impiego di cittadini di paesi terzi il cui soggiorno è irregolare)	<ul style="list-style-type: none"> • Disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3-bis e 3-ter D.Lgs. 286/1998); • Disposizioni contro le immigrazioni clandestine (art. 12, co. 5, D.Lgs. 286/1998). 	Le procedure di reclutamento di Lepida prevedono l'esperimento di procedure selettive aventi quale requisito di ammissione, in via alternativa, il possesso di: (1) cittadinanza italiana; (2) di cittadinanza in uno degli Stati membri dell'Unione Europea; (3) per i cittadini di Paesi Terzi, possesso di un regolare titolo di soggiorno.
Art. 25 quaterdecies (Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati)	<ul style="list-style-type: none"> • Frode in competizioni sportive (art. 1, L. 401/1989); • Esercizio abusivo di attività di giuoco o di scommessa (art. 4 L. 401/1989). 	Tenuto conto della natura dell'attività e dell'oggetto sociale di Lepida, si esclude che tali fattispecie di reato possano ricorrere nell'ambito delle attività della Società.
Art. 25 sex-decies (Contrabbando)	<ul style="list-style-type: none"> • Testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi e relative sanzioni penali e amministrative (D.lgs. 504/1995). 	Si esclude che tali fattispecie di reato, in materia di accise, possano ricorrere nell'ambito delle attività svolte dalla Società, considerando la natura, l'attività e l'oggetto sociale di Lepida.
Art. 25-septies decies (Delitti contro il patrimonio culturale)	<ul style="list-style-type: none"> • Importazione illecita di beni culturali (art. 518-decies c.p.); • Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.). 	Stante la natura delle attività di Lepida, anche considerati i presupposti e i requisiti delle condotte tipiche descritte, si esclude che tali fattispecie possano ricorrere nell'ambito delle attività della Società, al



		netto della valutazione in merito al requisito dell'interesse e del vantaggio per la Società.
Art. 25-duodevicies (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici)	<ul style="list-style-type: none"> • Riciclaggio di beni culturali (art. 518-sexies c.p.). 	Attesa la tipicità richiesta dalla fattispecie incriminatrice (piena consapevolezza del valore culturale del bene oggetto di ricettazione e natura necessariamente dolosa del reato presupposto del riciclaggio di beni culturali) considerando anche la giurisprudenza in materia, si ritiene che in relazione alle attività di Lepida non sia configurabile la fattispecie di reato.

Si segnala altresì l'avvenuta **abrogazione** delle fattispecie di cui al seguente elenco:

Art. 25 ter (Reati societari)	<ul style="list-style-type: none"> • Violazione di obblighi incombenti agli amministratori (2623, co. 1, c.c, abrogato dal DL 78/2009); • Violazione di obblighi incombenti agli amministratori (2623, co. 2, c.c, abrogato dal DL 78/2009); • Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 1, c.c, abrogato dal D.Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D.Lgs. 39/2010); • Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 1, c.c, abrogato dal D.Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D.Lgs. 39/2010).
---	--

4.5.2 Identificazione delle Macroattività a rischio

La predisposizione delle indispensabili misure addizionali di tutela, impone l'analisi dei processi e delle attività aziendali ove è più concreta la verifica delle ipotesi di reato particolarmente allarmanti.

Sono state, pertanto, identificate le macroattività rispetto alle quali appare possibile configurare i reati rilevanti ex D.Lgs. 231/2001, il cui elenco è di seguito riportato:

Macroattività a rischio
A. Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti
B. Attività di selezione del personale e di mobilità interna



C. Gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi
D. Gestione dei servizi, infrastrutture, livelli di servizio
E. Gestione della rendicontazione amministrativa verso gli Enti Soci
F. Bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale
G. Gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale
H. Gestione degli aspetti afferenti la sicurezza e l'igiene sul lavoro
I. Acquisto e utilizzo di valori di bollo
J. Gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale
K. Gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva)
L. Gestione contenzioso legale
M. Gestione rifiuti

Per ricondurre tali ambiti ad un livello di rischio accettabile, la Società ha predisposto una serie di controlli generali da applicarsi alla generalità delle attività poste in essere - quali il Piano triennale di prevenzione della corruzione e della trasparenza, Codice Etico ecc. - organicamente descritti nel successivo § [5. Il Sistema dei controlli](#).

4.5.3 Identificazione delle Macroattività particolarmente sensibili

Fra le macroattività a rischio identificate, **alcune presentano un livello di rischio reato particolarmente forte**. Si tratta, nello specifico di quelle relative a:

- attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti (Macroattività A);
- attività di selezione del personale e di mobilità interna (Macroattività B);
- gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi (Macroattività C);
- gestione dei servizi, infrastrutture, livelli di servizio (Macroattività D);
- gestione della rendicontazione amministrativa verso gli Enti Soci (Macroattività E);
- gestione rifiuti (Macroattività M).

Per ricondurre tali ambiti ad un livello di rischio accettabile è stato necessario definire e adottare sistemi di controllo più stringenti, quali specifiche procedure interne e formazioni specifiche indispensabili per riportare anche tale livello di rischio ad una accettabilità.

4.5.4 Fattispecie di reato a maggior rischio potenziale

Lepida ha condotto un'analisi delle aree di attività a rischio di commissione di Reati che ha portato all'identificazione delle principali, distinte, categorie di reati di possibile commissione di illeciti nell'interesse o a vantaggio della Società:

1) **Reati nei rapporti con la Pubblica Amministrazione:**



- Art. 24 del Decreto;
- Art. 25 del Decreto.

2) Reati informatici e illecito trattamento dei dati:

- art. 24-bis del Decreto.

3) Delitti di criminalità organizzata

- art. 24 - ter del Decreto.

4) Reati societari di cui gli artt. 2621 e ss. del codice civile:

- art. 25-ter del Decreto.

5) Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro:

- art. 25-septies del Decreto.

6) Reati relativi al riciclaggio di denaro e all'autoriciclaggio:

- art. 25-octies del Decreto.

7) Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori:

- art. 25-octies.1 del Decreto.

8) Reati in materia di violazione del diritto d'autore:

- art. 25-novies del Decreto.

9) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

- art. 25-decies del Decreto.

10) Reati ambientali:

- art. 25-undecies del Decreto.

11) Reati tributari:

- art. 25-quinquiesdecies del Decreto.

12) Reati contro il patrimonio culturale:

- art. 25-septies decies del Decreto;
- art. 25-duodevicies del Decreto.

Per le altre fattispecie di reato previste dal Decreto, non comprese nell'elenco sopra indicato, viste anche le attività e la strutturazione aziendali, non sono ravvisati gli estremi o le condizioni per la possibile commissione di queste tipologie di reato.

4.5.5 Parte Speciale

La Parte speciale del presente modello è stata conseguentemente realizzata considerando le **Macroattività a particolare rischio di cui al par. § 4.5.2 e le Ipotesi di reato a maggior rischio potenziale** di cui al successivo **§ 4.5.4**, al fine di individuare i rimedi già posti in essere dalla Società, nonché quelli di opportuna predisposizione ai fini del contenimento del rischio residuo.



5. Il Sistema dei controlli

5.1 Componenti del sistema dei controlli

I principali componenti del sistema di controlli predisposto dalla Società sono i seguenti:

- Piano triennale di prevenzione della corruzione e della trasparenza;
- Codice Etico e di Comportamento: Lepida, al fine di adeguare i propri principi etici e di condotta aziendali ai requisiti previsti dal D.Lgs. 231/2001, si è dotata di un Codice Etico e di Comportamento. Tale documento viene messo a disposizione di tutti i destinatari in forma cartacea o in formato elettronico, in quanto presente anche nel sito internet aziendale e nella intranet aziendale;
- Regolamenti aziendali: la Società dispone di regolamenti formalizzati che normano i principali ambiti aziendali;
- Politiche e procedure aziendali: la Società dispone attualmente di politiche e procedure formalizzate che definiscono i principi e le modalità di svolgimento delle principali attività operative aziendali
- Poteri autorizzativi e segregation of duty: nello svolgimento delle attività aziendali vengono rispettati specifici iter autorizzativi opportunamente formalizzati nelle procedure aziendali. I poteri di firma e rappresentanza sono attribuiti al Presidente della Società, in qualità di Legale Rappresentante, e al Direttore Generale in virtù di apposita procura notarile e specifici mandati conferiti dal Consiglio di Amministrazione. Sono previste adeguate contrapposizioni funzionali per la tutela del requisito di segregazione dei compiti (Segregation of Duties);
- Audit interni: la Società svolge attività sistematiche di audit interno per verificare la corretta attuazione dei controlli interni, delle policy e degli standard adottati.
- Audit di terza parte: la Società viene sottoposta periodicamente a audit per il mantenimento delle certificazioni dei Sistemi di Gestione aziendali e dell'accreditamento come identity provider SPID;
- Sensibilizzazione e formazione del personale: in seguito all'adozione del presente Modello, la Società ha definito un piano per la comunicazione capillare dello stesso Modello a tutti i destinatari e un programma di formazione al personale mirato in base al grado di coinvolgimento nelle aree a rischio reato;
- Tracciabilità e accountability delle operazioni: la Società garantisce, tipicamente tramite sistemi informatici, la tracciabilità e l'accountability delle operazioni effettuate dal personale.
- Modello di Organizzazione e Gestione
- Norme di Trasparenza di Gestione
- Sistema di Gestione Integrato

6. Sistema sanzionatorio

Essenziale per l'effettività del Modello di organizzazione e di gestione - e per l'esclusione di responsabilità della Società che se ne dota - è la predisposizione di un adeguato sistema



sanzionatorio disciplinare da applicarsi in caso di violazione delle previsioni contenute nel Modello stesso, nonché delle disposizioni e dei principi stabiliti nel Codice Etico e di Comportamento e nel Piano triennale di prevenzione della corruzione e della trasparenza: nei confronti dei destinatari del Modello, infatti, la sanzione ha, prima d'ogni altro, lo scopo di dissuadere dal porre in essere comportamenti che possano integrare le fattispecie di reato di cui al D.Lgs. 231/2001.

I comportamenti contrari alle regole comportamentali contenute nel presente Modello risultano qualificabili quali illeciti disciplinari. A titolo meramente esemplificativo, costituiscono violazione del Modello:

- azioni o comportamenti non conformi alle prescrizioni del Modello, nell'espletamento di attività nel cui ambito ricorre il rischio di commissione dei reati contemplati;
- azioni o comportamenti non conformi alle prescrizioni del Modello, ovvero l'omissione di azioni o comportamenti prescritti dal Modello che:
 - espongano la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal D.Lgs. 231/2001 e successive integrazioni;
 - siano diretti in modo univoco al compimento di uno o più reati contemplati;
 - tali da determinare l'applicazione a carico della Società di sanzioni previste.
- la messa in atto di azioni o comportamenti non conformi ai principi contenuti nel Codice Etico e di Comportamento di Lepida.

6.1 Criteri di applicazione delle sanzioni

L'applicazione delle sanzioni è improntata ai principi di proporzionalità e di equità, nonché a quello di tempestività.

Nella determinazione della sanzione si dovrà tenere conto delle concrete circostanze del caso e dell'eventuale reiterazione della violazione. In specie, il tipo e l'entità di ciascuna delle sanzioni saranno determinate in relazione a:

- elemento soggettivo dell'illecito, a seconda del dolo o della colpa;
- rilevanza degli obblighi violati;
- livello di responsabilità gerarchica e/o tecnica del soggetto coinvolto;
- eventuale condivisione della responsabilità con altri soggetti che abbiano concorso nel determinare il reato;
- presenza di circostanze aggravanti o attenuanti, con particolare riguardo alla professionalità, alle precedenti prestazioni lavorative, ai precedenti disciplinari, alle circostanze in cui è stato commesso il fatto.

Non essendovi necessaria coincidenza tra comportamenti di inosservanza del Modello e quelli integranti ipotesi di reato rilevanti ex D.Lgs. 231/01, l'applicazione delle sanzioni disciplinari è autonoma rispetto allo svolgimento e all'esito del procedimento penale eventualmente avviato dall'Autorità giudiziaria.

Gli autori di eventuali violazioni incorreranno pertanto, oltre che nelle responsabilità e nelle sanzioni civili, amministrative, penali o contabili previste per legge, in quelle disciplinari stabilite da Lepida.

Resta naturalmente ferma la possibilità per la Società di agire per il risarcimento dei danni



eventualmente subiti in conseguenza dell'azione commessa.

6.2 Sanzioni per violazioni commesse da dipendenti

Le sanzioni disciplinari derivanti da violazioni commesse da dipendenti saranno coerenti con quanto previsto dalla legge e dalle norme contrattuali applicabili: il rispetto degli obblighi indicati nel Modello, nel Codice Etico e di Comportamento, nel Piano triennale di prevenzione della corruzione e della trasparenza è, infatti, da considerarsi, anche ai sensi dell'art. 2104 c.c., parte integrante degli obblighi derivanti dal rapporto di lavoro.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni rimangono ferme le competenze già attribuite dagli organi della Società. Compete invece all'OdV il compito di condurre le indagini interne in ordine alla violazione del Modello.

I dipendenti della Società sono tenuti ad informare tempestivamente l'Organismo di Vigilanza rispetto ad ogni circostanza che comporti, o che possa comportare, una deviazione dalle norme indicate nel Modello, nel Codice Etico e di Comportamento. Relativamente ai casi di violazione del PTPCT, come sopra indicato (par. 1.3.1.1), si affianca la competenza specifica del Responsabile della Prevenzione della Corruzione e della Trasparenza, che diviene esclusiva nella gestione delle segnalazioni di c.d. whistleblowing.

L'Organismo di Vigilanza dovrà trattare le segnalazioni ricevute con la massima confidenzialità e svolgere successivamente le opportune verifiche e indagini.

Per non compromettere l'integrità e la validità dell'indagine svolta a livello istituzionale, coloro che abbiano segnalato le violazioni dovranno astenersi dal condurre autonomamente indagini in via preliminare.

Durante le fasi istruttorie i dipendenti sono tenuti a cooperare e fornire le informazioni in loro possesso riguardanti le violazioni; la mancata o parziale cooperazione potrà portare all'adozione di provvedimenti disciplinari, ivi incluso il licenziamento.

In conformità con le procedure previste dal CCNL, sempre tenendo conto dell'entità della violazione e delle circostanze in cui essa è stata compiuta, sono applicabili le seguenti sanzioni disciplinari:

- **biasimo in forma orale o scritta.** Tale sanzione è prevista per il lavoratore che commetta lievi mancanze, come nel caso in cui lo stesso violi le procedure interne 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, ecc.) o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una *"non osservanza delle disposizioni portate a conoscenza dall'Ente con ordini di servizio od altro mezzo idoneo"* di cui all'art. 227 del CCNL. Qualora il comportamento sia ripetuto nel tempo, in modo da dare luogo ad una recidiva, il lavoratore è richiamato con una nota di biasimo scritta.
- **multa**, in misura non eccedente l'importo di 4 ore della retribuzione oraria calcolata sul minimo tabellare; applicabile nei confronti del dipendente che:



- o commetta con colpa, negligenza e/o imperizia una violazione non grave dei principi e delle previsioni del Modello, del Codice Etico e di Comportamento, del Piano triennale di prevenzione della corruzione e della trasparenza, delle policy e delle procedure adottate dalla Società da intendersi quali disposizioni per l'esecuzione della prestazione ai sensi dell'art. 2104 c.c.;
 - o violi la riservatezza o si rifiuti di cooperare in caso di avvio di una procedura formale atta a verificare il rispetto dei principi di rispetto della dignità personale e/o di imparzialità, correttezza e trasparenza previsti dal Modello, dal Codice Etico e di Comportamento, dal Piano triennale di prevenzione della corruzione e della trasparenza;
 - o compia atti di ritorsione nei confronti di un collega che abbia lamentato una discriminazione o una lesione dei propri diritti nei casi previsti dal Codice Etico e di Comportamento.
- **sospensione dalla retribuzione e dal servizio** per un massimo di 10 giorni, applicabile nei confronti del dipendente che commetta recidiva nell'anno solare in una delle violazioni sanzionate con la multa o sia responsabile di atti di discriminazione indiretta;
 - **licenziamento disciplinare**, con o senza preavviso, applicabile nei seguenti casi:
 - o violazione dolosa del Modello Organizzativo, Codice Etico e di Comportamento, Piano triennale di prevenzione della corruzione e della trasparenza o del rispetto dei beni aziendali e delle policy e delle procedure adottate dalla Società da intendersi quali disposizioni per l'esecuzione della prestazione ai sensi dell'art. 2104 c.c.;
 - o abuso di informazioni riservate o confidenziali;
 - o falsificazione di documenti, quali scritture contabili, documenti relativi alla Società o documenti relativi a spese di rappresentanza e trasferte;
 - o violazione delle politiche di protezione e delle politiche commerciali della Società, violazione del segreto industriale;
 - o grave violazione anche di una sola tra le indicazioni regolanti:
 - il rispetto delle leggi e normative;
 - i rapporti con i fornitori e con la Pubblica Amministrazione;
 - la sicurezza sul lavoro;
 - la criminalità informatica;
 - o grave omessa divulgazione di informazioni importanti o intenzionale comunicazione di informazioni ingannevoli;
 - o atti gravi di discriminazione diretta e indiretta.

In caso di condotte sanzionabili con il licenziamento disciplinare senza preavviso, la Società potrà disporre la **sospensione cautelare** del dipendente con effetto immediato, per un periodo massimo di 6 giorni; ove il licenziamento venga applicato, esso avrà effetto dal momento della disposta sospensione.



6.3 Sanzioni per violazioni commesse da Dirigenti, membri del CdA o del Collegio Sindacale

Se la violazione è commessa da un componente del CdA o del collegio Sindacale, della stessa sarà data comunicazione ai Soci, al Collegio sindacale e al CdA ai fini della valutazione di una eventuale revoca dalla carica per giusta causa. L'Organismo di Vigilanza deve essere tenuto debitamente aggiornato riguardo ai provvedimenti adottati.

Nei confronti dei Dirigenti che abbiano eluso fraudolentemente Procedure, Policies, regole e/o disposizioni comunque dedotti dal Modello Organizzativo, dal Codice Etico, dal Piano triennale di prevenzione della corruzione e della trasparenza, la Società stabilirà le misure sanzionatorie più idonee, tenendo conto di quanto previsto dalla legge, dal codice civile, dal CCNL applicabile e da eventuali ulteriori normative applicabili. Nel caso in cui tale violazione dovesse determinare, in aggiunta, il venir meno del rapporto fiduciario con la Società, la sanzione è individuata nel licenziamento disciplinare.

6.4 Sanzioni per violazioni commesse da soggetti terzi

Se la violazione è commessa da persona vincolata alla Società da un rapporto di natura differente da quelli sopra indicati, Lepida avrà facoltà di risolvere tale rapporto o comunque di recedere dallo stesso, attraverso decisione assunta da soggetto munito dei necessari poteri.

6.5 Sanzioni connesse all'istituto del Whistleblowing

L'art. 6, comma 2-bis, del Decreto prescrive altresì che i modelli di organizzazione e gestione prevedano "(...) il sistema disciplinare, adottato ai sensi del comma 2, lettera e)".

Sono, pertanto, configurabili le seguenti condotte connesse al whistleblowing rilevanti ai fini dell'irrogazione di sanzioni disciplinari:

- A. violazione dell'obbligo di riservatezza del segnalante;
- B. utilizzo abusivo dei canali di segnalazione – segnalazione infondata o falsa con dolo e colpa grave;
- C. violazione del divieto di atti di ritorsione nei confronti del segnalante.

Va precisato che le sanzioni sono determinate in concreto, nel rispetto del principio della gradualità delle stesse, anche in relazione all'intenzionalità del comportamento o al grado di negligenza, imprudenza o imperizia, con riguardo anche alla prevedibilità dell'evento e all'eventuale concorso nella violazione da parte di più soggetti.

A. Violazione della tutela della riservatezza del segnalante:

Fermi restando eventuali profili di responsabilità previsti dall'ordinamento, in relazione al grado di "colpevolezza" dell'autore della condotta, si ritiene applicabile, a seconda dei casi:

- per il dipendente: dalla sanzione della multa pari a 4 ore della retribuzione oraria calcolata sul minimo tabellare applicabile fino al licenziamento senza preavviso e con trattamento di fine rapporto;
- per il dirigente: dalla lettera di richiamo alla risoluzione del rapporto.



Ove la violazione sia commessa da amministratori o membri del collegio sindacale/OdV, stante la nomina da parte degli Enti Soci, verranno valutati gli opportuni provvedimenti -ivi inclusa la revoca del mandato per giusta causa - in sede di Assemblea dei Soci.

B. Utilizzo abusivo dei canali di segnalazione – segnalazione infondata o falsa con dolo e colpa grave:

La condotta rilevante si sostanzia, di fatto, nel caso di dolo, in una denuncia con intenzionalità ovvero con piena coscienza delle conseguenze della propria azione nella consapevolezza della falsità o infondatezza della denuncia; la colpa grave può dirsi integrata allorquando il soggetto, pur non agendo con l'intenzionalità di arrecare un pregiudizio, abbia agito con straordinaria e inescusabile imprudenza, omettendo di osservare non solo la diligenza del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza richiesto (si può, ad es. prefigurare il caso di una "prova" dell'utilizzo della piattaforma mediante l'inserimento del nominativo del segnalato e la compilazione integrale del form seguita, per una svista, anziché dalla cancellazione, dall'invio della segnalazione stessa. In tal caso può dirsi integrata l'ipotesi di "colpa cosciente" nella misura in cui l'agente si prefigura il rischio che si realizzi l'evento dannoso ma confida sulle proprie capacità e abilità affinché il danno non si verifichi). È, pertanto, applicabile, a seconda dei casi:

- per il dipendente: dalla sanzione della sospensione dal servizio e dalla retribuzione fino al licenziamento senza preavviso e con trattamento di fine rapporto;
- per il dirigente: dalla lettera di richiamo alla risoluzione del rapporto.

C. Violazione del divieto di atti di ritorsione nei confronti del segnalante:

L'eventuale adozione di misure ritorsive nei confronti del whistleblower (trasferimenti, sanzioni disciplinari, mobbing, licenziamento) è astrattamente configurabile solo rispetto al management societario. Fatta salva ogni altra azione legale, ove si ravvisi tale eventualità e risulti provato l'intento effettivamente persecutorio e ritorsivo della misura nei confronti del segnalante, si ritiene irrogabile la più grave sanzione della risoluzione del rapporto.

L'adozione di misure discriminatorie può essere segnalata all'RPCT di Lepida o direttamente all'ANAC sulla base di quanto esplicitato nel sito istituzionale dell'Autorità al link <https://www.anticorruzione.it/-/whistleblowing>.



7. L'Organismo di Vigilanza

7.1 Requisiti dell'Organismo Di Vigilanza

L'articolo 6 del Decreto sancisce che la Società, per risultare esente dalla responsabilità amministrativa ivi prevista, debba, tra l'altro, nominare e affidare ad un organismo preposto la vigilanza sul rispetto del Modello e sul suo funzionamento e aggiornamento. Tale organismo dovrà essere dotato dei caratteri di autonomia, indipendenza funzionale, professionalità e continuità d'azione.

7.1.1 Indipendenza e autonomia

I requisiti di autonomia e indipendenza sono indispensabili affinché l'Organismo di Vigilanza (OdV) non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo.

Per poter garantire all'Organismo l'indipendenza gerarchica, esso riporterà direttamente al CdA e al Presidente della Società, informando della propria attività, su richiesta, il Collegio Sindacale.

La composizione dell'Organismo e la qualifica dei suoi membri devono essere tali da assicurare, sia sotto il profilo oggettivo che sotto quello soggettivo, l'assoluta autonomia e indipendenza delle relative valutazioni e determinazioni.

L'Organismo deve inoltre essere provvisto di una dotazione finanziaria autonoma atta a consentirne la normale operatività.

7.1.2 Professionalità

L'OdV deve avere al suo interno competenze tecnico-professionali compatibili con le funzioni che è chiamato a svolgere. Parimenti, appare opportuno che le persone che lo compongono dispongano di una conoscenza approfondita delle attività della Società. Tali caratteristiche, unite all'indipendenza, conferiscono all'organismo obiettività, autorevolezza e competenza nel giudizio.

7.1.3 Autonomia nei poteri di iniziativa e controllo

L'OdV definisce e svolge in modo autonomo le attività di propria competenza, comprese le attività essenziali di controllo. Le regole di funzionamento dell'OdV sono definite dallo stesso all'interno del proprio Regolamento.

Infatti, mentre l'approvazione del Modello Organizzativo (e i suoi eventuali aggiornamenti) è atto di competenza del CdA, il Regolamento, come espressamente indicato dalle Linee Guida di Confindustria, rappresenta l'autoregolamentazione operativa dell'OdV ed è approvato in piena autonomia dall'OdV stesso alla sua prima seduta.

7.1.4 Continuità di azione

L'OdV deve:

- vigilare che il Modello sia costantemente rispettato utilizzando i necessari poteri



- d'indagine;
- garantire il costante aggiornamento del Modello;
- essere referente qualificato, costante e super partes per tutto il personale della Società e per il Management, promuovendo, anche con il contributo delle competenti funzioni aziendali, la diffusione nel contesto aziendale della conoscenza e della comprensione del Modello.

7.1.5 Acquisizione delle informazioni

Per poter garantire la propria operatività, l'OdV acquisisce le informazioni necessarie attraverso i seguenti canali:

- i flussi informativi definiti dal Regolamento e dallo specifico documento Policy sui flussi di comunicazione con l'Organismo di Vigilanza e dal Modello Organizzativo stesso;
- le richieste dell'OdV stesso verso le strutture interessate;
- le interviste programmate al personale interno e le verifiche documentali;
- la partecipazione di uno dei membri ai momenti decisionali della Società, laddove vengano trattati temi inerenti i rischi di reato di cui al Decreto.

7.1.6 Riporto agli Organi sociali

L'OdV riporta le informazioni acquisite direttamente al CdA.

7.1.7 Qualificazione e ruolo dell'OdV ai fini della normativa sul trattamento dei dati personali

Nel corso del 2020, Lepida ha provveduto a formalizzare nei confronti del proprio Organismo di Vigilanza, collegialmente inteso, l'informativa circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali ex art. 5, co. 2, GDPR (prot. 200862/2020), in conformità all'orientamento, circa la qualificazione e il ruolo ai fini privacy dell'Organismo di Vigilanza, espresso dal Direttivo dell'Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001 in data 21 marzo 2019 nel documento "[Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy](#)".

A seguito del [Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza](#) formalizzato dall'Autorità Garante per la protezione dei dati personali, secondo cui l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongono siano interni o esterni, debba essere considerato "*parte dell'ente*", confermando al contempo l'assunto per cui il medesimo, pur essendo dotato di autonomi poteri di iniziativa e controllo, non può essere considerato né autonomo titolare del trattamento né responsabile inteso come soggetto chiamato ad effettuare un trattamento "*per conto del titolare*", ovvero sia una "*persona giuridicamente distinta dal Titolare, ma che agisce per conto di quest'ultimo*" secondo le istruzioni impartite dal titolare, Lepida ha formalizzato le autorizzazioni al trattamento dei dati personali per ciascun membro dell'Organismo di Vigilanza ai sensi degli artt. 4, n. 10, 29, 32 par. 4 del Regolamento UE n. 2016/679 e art. 2-quaterdecies del D.Lgs. 196/2003 e s.m.i.

7.2 Nomina dei membri dell'Organismo di Vigilanza

Sulla base delle specifiche peculiarità richieste all'OdV, Lepida ha istituito un OdV collegiale,



composto da tre membri, di cui:

- un componente di provenienza esterna alla società, con il ruolo di Presidente dell'OdV;
- due Dirigenti ovvero due Quadri direttivi dell'azienda.

Tale soluzione appare come quella che meglio garantisce il rispetto dei requisiti previsti dal Decreto; da una parte, infatti, la presenza di soggetti interni con particolare preparazione ed esperienza, maturate in posizioni di responsabilità, assicura quel grado di conoscenza dei processi aziendali necessario alla valutazione dell'efficacia dei sistemi organizzativi e di controllo; dall'altra, la presenza di un soggetto esterno che abbia specifica competenza e autorevolezza nell'applicazione dell'impianto giuridico previsto dal Decreto, garantisce quei requisiti d'imparzialità, autonomia, indipendenza e competenza che vengono richiesti dalla legge.

I componenti dell'OdV sono nominati con delibera del CdA.

L'OdV resta in carica per una durata di tre anni dalla data della nomina.

La nomina quale membro dell'OdV è subordinata all'assenza di cause di incompatibilità, e/o ineleggibilità secondo il presente Modello. Il soggetto che verrà individuato quale membro dell'OdV, prima di accettare la nomina, dovrà dichiarare al CdA se esistono a suo carico condizioni di ineleggibilità secondo il presente Modello. In conseguenza di ciò, il CdA potrà riservarsi di valutare tale posizione.

7.3 Rinuncia, revoca e sanzioni

Costituiscono motivi di incompatibilità, ineleggibilità e/o di decadenza dei membri dell'OdV:

- aver attribuito allo stesso funzioni e responsabilità operative incompatibili con i requisiti di autonomia di iniziativa e di controllo, d'indipendenza e continuità di azione propri dell'OdV;
- per uno dei componenti interni alla Società da un rapporto di lavoro subordinato, l'avvio di un procedimento disciplinare per fatti da cui possa derivare la sanzione del licenziamento o in caso di cessazione di detto rapporto indipendentemente dalla causa di interruzione dello stesso;
- non aver partecipato, senza giustificato motivo, a tre o più riunioni consecutive dell'Organismo;
- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con gli amministratori o con i membri del Collegio Sindacale di Lepida;
- intrattenere, direttamente o indirettamente, con esclusione del rapporto di lavoro a tempo indeterminato, relazioni economiche e/o rapporti contrattuali o comunque rapporti da cui possano derivare situazioni di conflitto di interessi o cause di incompatibilità con Lepida e con i rispettivi amministratori, di rilevanza tale da condizionarne l'autonomia di giudizio;
- trovarsi nella condizione giuridica di interdetto, inabilitato, fallito o condannato a una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi;
- essere stato sottoposto a misure di prevenzione disposte dall'autorità giudiziaria, salvi gli effetti della riabilitazione;
- essere stato condannato anche in primo grado, ovvero aver concordato l'applicazione della pena ai sensi degli artt. 444 e ss. c.p.p., salvi gli effetti della riabilitazione, in relazione ad uno dei reati previsti dal D.Lgs. 231/2001 o a reati della stessa indole (in



particolare, reati contro il patrimonio, contro la Pubblica Amministrazione, contro la fede pubblica, contro l'ordine pubblico, reati tributari, reati fallimentari, reati finanziari; ecc.);

- aver svolto, nei tre esercizi precedenti l'attribuzione dell'incarico, funzioni di amministrazione, direzione o controllo in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate;
- aver svolto, nei tre esercizi precedenti l'attribuzione dell'incarico, funzioni di amministrazione o controllo (ovvero essere stato membro del Collegio Sindacale o aver lavorato come revisore esterno del bilancio) in Lepida;
- essere affetti da una grave infermità che renda uno dei componenti dell'Organismo inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, determini l'assenza dal luogo di lavoro per un periodo superiore a sei mesi.

Limitatamente al personale aziendale, rappresentano ulteriori motivi di decadenza dall'incarico:

- la cessazione, per qualsiasi causa, del rapporto di lavoro;
- il cambio di mansione, che determini l'assegnazione della persona a una diversa funzione aziendale incompatibile con lo svolgimento delle funzioni di componente dell'OdV.

Costituiscono cause di revoca dell'incarico di componente dell'Organismo:

- il grave inadempimento dovuto a negligenza o imperizia nell'espletamento delle mansioni affidate all'Organismo;
- l'adozione di reiterati comportamenti ostruzionistici o non collaborativi nei confronti degli altri componenti;
- l'applicazione nei suoi confronti di sanzioni disciplinari;
- l'assenza a tre o più riunioni anche non consecutive senza giustificato motivo nell'arco di dodici mesi consecutivi;
- essere, comunque, titolari di interessi in conflitto, anche potenziale, con la Società tali da pregiudicare la propria indipendenza di giudizio;
- l'aver violato l'obbligo di riservatezza in ordine alle notizie e informazioni acquisite nell'esercizio delle sue funzioni, fatti salvi gli obblighi di informazione espressamente previsti dal Modello ex D.Lgs. 231/2001, o in altri documenti societari ovvero comunque previsti ex lege;
- ogni altra giusta causa.

L'eventuale revoca di uno dei componenti dell'Organismo dovrà essere deliberata dal CdA a maggioranza assoluta, sentiti gli altri membri dell'Organismo e dovrà essere preventivamente comunicata al Collegio Sindacale e, successivamente, all'Assemblea dei Soci in occasione della prima assemblea utile. Egualmente, ove si verifichi una delle cause di decadenza sopra indicate, il CdA di Lepida, esperiti gli opportuni accertamenti, sentito l'interessato e gli altri membri dell'Organismo, stabilisce un termine non superiore a 60 giorni entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, il CdA di Lepida deve dichiarare l'avvenuta decadenza del componente e assumere le opportune deliberazioni.

Qualora la revoca venga esercitata o la decadenza intervenga nei confronti di tutti i



componenti dell'OdV, il CdA di Lepida, sentito il Collegio Sindacale, provvederà a nominare un nuovo OdV.

In caso di applicazione in via cautelare di una delle misure interdittive previste dal D.Lgs. 231/2001, il CdA di Lepida, assunte le opportune informazioni, valuta la sussistenza delle condizioni per la revoca dei componenti dell'Organismo, ove ravvisi un'ipotesi di omessa o insufficiente vigilanza da parte dello stesso.

Il CdA di Lepida, sentito il Collegio Sindacale e gli altri membri dell'OdV, può disporre la sospensione dalle funzioni del membro dell'Organismo che abbia riportato:

- una condanna per un reato diverso da quelli per cui è prevista la revoca;
- l'applicazione provvisoria di una misura di prevenzione;
- l'applicazione di una misura cautelare di tipo personale.

In tal caso, il CdA provvederà, sentiti gli altri membri dell'Organismo, alla nomina di un componente ad interim.

Ove la sospensione sia disposta nei confronti di tutti i membri dell'OdV, il CdA, sentito il Collegio Sindacale, provvederà alla nomina di un Organismo ad interim.

In caso di rinuncia, decadenza o revoca di un componente dell'Organismo, il CdA deve provvedere senza indugio alla sua sostituzione.

7.4 Modalità di funzionamento dell'Organismo di Vigilanza

Le attività poste in essere dall'OdV non possono essere oggetto di sindacato da parte di alcun altro organismo o struttura aziendale; il CdA è, in ogni caso, chiamato a svolgere un'attività di vigilanza, a posteriori, sull'adeguatezza complessiva dell'intervento dell'OdV, in quanto su di esso grava, in ultima istanza, la responsabilità del funzionamento e dell'efficacia del Modello: qualora il CdA rilevi un comportamento dell'OdV non rispondente a quanto descritto nel presente Modello, attiverà le necessarie procedure sanzionatorie previste.

I componenti dell'OdV, nonché i soggetti dei quali esso si avvale, sono tenuti all'obbligo di riservatezza in relazione a tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni o attività, obbligo che perdura per un periodo di cinque anni dalla eventuale cessazione dalla carica e/o dalla funzione.

All'OdV sono attribuiti tutti i poteri e le capacità di indagine necessari per intrattenere relazioni dirette e continuative con tutte le funzioni aziendali, segnatamente nel reperimento di documentazione e informazioni, nei limiti e nel rispetto della legge e delle procedure vigenti (privacy, obblighi di riservatezza, ecc.).

Delle riunioni e dei contenuti dovrà essere dato atto con redazione di apposito verbale.

L'OdV potrà riunirsi anche a mezzo di strumenti informatici e telematici e di comunicazione a distanza, purché sia rispettata la contestualità della riunione e le procedure di autenticazione dei membri.

Al di fuori delle presenti regole l'OdV ha ampio potere di autoregolamentazione della propria attività.

7.5 Funzioni, attività e poteri dell'Organismo di Vigilanza

L'OdV opererà secondo quanto previsto dal proprio Regolamento interno, approvato dall'Organismo stesso e trasmesso al CdA.

L'Organismo svolge le sue funzioni in piena autonomia, non operando alle dipendenze di alcuna altra funzione aziendale e riporta gli esiti delle proprie attività direttamente al CdA.



L'Organismo, quindi, agisce in base alle finalità attribuitegli dalla legge e orienta il proprio operato in vista del perseguimento di tali finalità.

Ai sensi e per gli effetti di cui all'art. 6, comma 1, lett. b) del D.Lgs. 231/2001, l'OdV ha l'obbligo di "vigilare sul funzionamento e l'osservanza dei modelli e curare il loro aggiornamento". Ne consegue che l'Organismo di Vigilanza deve svolgere una serie di attività analitiche e funzionali necessarie a mantenere efficiente e operativo lo stesso, che possono essere raggruppate nelle seguenti macro-aree:

- analisi, vigilanza e controllo;
- aggiornamento del Modello;
- formazione.

All'OdV sono affidati i seguenti compiti, ai quali corrispondono i relativi poteri:

- vigilare sulla corretta applicazione del Modello da parte delle funzioni aziendali. A tal fine, l'OdV provvederà ad effettuare periodicamente le seguenti verifiche:
 - o Verifiche ispettive: consistono nel contattare direttamente i responsabili dei processi strategici aziendali, al fine di monitorare l'attività ordinaria nonché di integrare la mappatura dei rischi aziendali anche richiedendo la documentazione a supporto che l'OdV riterrà utile;
 - o Verifiche procedurali: consistono nel controllare, al fine di prevenire i rischi nei processi strategici aziendali, che le procedure adottate dalle direzioni aziendali siano applicate e siano aggiornate in base alle mutate situazioni;
 - o Verifiche a campione: consistono nell'effettuare dei controlli con metodologie "non sistematiche", al fine di prevenire i rischi nei processi strategici aziendali, atti a rilevare che le procedure adottate dalle direzioni aziendali siano applicate e che le stesse siano aggiornate in base alle mutate situazioni.

Resta salvo il potere discrezionale dell'OdV di attivarsi mediante specifici controlli a seguito di segnalazioni ricevute, ovvero di propria iniziativa:

- esaminare l'adeguatezza del Modello alla realtà aziendale aggiornandolo e proponendo eventuali modifiche qualora lo ritenga necessario;
- valutare l'attitudine del Modello a prevenire la commissione di Reati a fronte dell'evoluzione e dei cambiamenti aziendali attraverso una periodica analisi dei rischi e dei potenziali Reati;
- proporre al Consiglio di Amministrazione le sanzioni stabilite nel sistema disciplinare e sanzionatorio di Lepida per il mancato rispetto delle misure indicate nel Modello;
- attivare le necessarie procedure presso gli Organi Societari competenti per l'irrogazione delle sanzioni derivanti dall'applicazione del D.Lgs. 231/2001;
- supportare iniziative per favorire la conoscenza del Modello, la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello, effettuandone il monitoraggio;
- porre in essere ogni altra attività reputata necessaria e/o utile per il miglior funzionamento del Modello;
- verifiche periodiche sulle operazioni di maggior rilievo (ad esempio per valore economico, coinvolgimento della P.A., livello di rischio, e così via);



- controlli in caso di ispezioni o accertamenti della pubblica autorità;
- interventi con gli organi deputati al controllo contabile e di legalità in prossimità della redazione delle comunicazioni sociali e della redazione del progetto di bilancio;
- interventi con gli organi deputati al controllo contabile e di legalità per controlli sulle operazioni di gestione finanziaria e di tesoreria, al fine di evitare la costituzione di fondi neri o riserve occulte;
- verifiche in ambito antiriciclaggio, sicurezza informatica, modulate in base agli impatti sull'operatività aziendale;
- accertamenti in materia di salute e sicurezza sul lavoro.

A tale scopo, l'OdV:

- effettua il monitoraggio dell'applicazione e del rispetto del Codice Etico e di Comportamento e promuove iniziative per la diffusione della conoscenza e comprensione dello stesso;
- verifica, anche attraverso la rispondenza ai principi generalmente accettati e agli standard di best practice, i criteri e le tecniche utilizzati per l'elaborazione dei dati contabili e delle informazioni a questi afferenti;
- verifica costantemente i previsti flussi informativi verso gli Organi Sociali;
- fornisce la propria collaborazione nella fase di identificazione e classificazione delle Aree aziendali a Rischio attraverso il risk assessment periodico;
- supporta la predisposizione e l'integrazione della normativa interna connessa alla prevenzione rischi e allo sviluppo dei comportamenti corretti nell'ambito delle prescrizioni del Modello e del Codice Etico e di Comportamento;
- segnala alle funzioni competenti le eventuali violazioni delle procedure aziendali o dei principi di riferimento del Modello e del Codice Etico e di Comportamento;
- collabora con il Collegio Sindacale nella valutazione dell'adeguatezza del sistema dei controlli dell'Azienda, nei limiti delle proprie competenze;
- predispone il piano annuale delle verifiche che intende svolgere per verificare l'adeguatezza e il funzionamento del Modello;
- valuta periodicamente l'adeguatezza dei flussi informativi ad esso destinati.

Per lo svolgimento dei compiti suddetti l'OdV:

- ha libero accesso a qualsiasi documento aziendale;
- gode di ampi poteri ispettivi;
- si avvale di risorse economiche stanziare nel budget annuale su sua indicazione; avrà accesso a tali risorse rendicontando di volta in volta al CdA, a seconda delle esigenze derivanti dalla propria attività;
- può avvalersi sia del supporto e della cooperazione delle Funzioni aziendali sia di consulenti esterni di comprovata professionalità;
- può richiedere informazioni o rivolgere comunicazioni al CdA o a singoli membri dello stesso, al Collegio Sindacale e alla società di revisione;
- si avvale della funzione Internal Auditing per pianificare e svolgere l'attività di vigilanza in modo da utilizzare modalità operative già consolidate e risorse con adeguate competenze tecniche, nonché evitare sovrapposizioni di attività.



Gli interventi dell'OdV, inclusi gli incontri con le aree e funzioni aziendali di volta in volta interessate, devono essere verbalizzati.

L'Organismo di Vigilanza si può avvalere, previa richiesta al C.d.A., di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231.

7.6 Obblighi di informazione verso l'Organismo di Vigilanza

Per permettere il regolare funzionamento dell'OdV, i Destinatari sono tenuti al rispetto degli obblighi di informazione previsti:

- dal presente Modello Organizzativo;
- dal documento Codice Etico e di Comportamento, dal Piano triennale di prevenzione della corruzione e della trasparenza;
- dal documento annuale redatto dall'OdV relativamente a specifiche informazioni da trasmettere;
- dalla Mappatura dei Rischi.

La facilitazione dei flussi informativi verso l'OdV costituisce un obbligo in capo a tutti i Destinatari nell'ambito delle attività programmate per la prevenzione dei reati previsti dal Decreto. A tal fine, le informazioni aventi per oggetto i comportamenti non conformi, nonché le informazioni su tutti gli eventi che siano in qualsiasi modo attinenti alle attività a rischio-reato, devono essere trasmesse all'OdV.

L'OdV deve essere tempestivamente informato di ogni cambiamento in essere o pianificato, inerente e/o avente ad oggetto il Modello Organizzativo e/o la struttura/assetto societario in generale rilevante ai fini del Decreto.

L'OdV deve essere informato, attraverso apposite segnalazioni da parte dei Destinatari, in merito ad eventi che potrebbero generare responsabilità per Lepida ai sensi del Decreto.

L'informativa all'OdV avviene per quanto riferibile a tutti gli obblighi relativi alle informazioni di cui al D Lgs. 33/2013 attraverso la sezione Società Trasparente pubblicata sul sito istituzionale dove a mero titolo esemplificativo sono disponibili informazioni relative a: Disposizioni Generali, Organizzazione, Consulenti e Collaboratori, Personale, Selezione del Personale, Performance, Enti Controllati, Attività e procedimenti, Bandi di Gara e Contratti (contenente delibera Cda, delibera Assemblea e riepilogo contratti stipulati), Sovvenzioni, Contributi, Sussidi, Vantaggi economici, Bilanci, Beni immobili e gestione patrimonio, Controlli e rilievi sull'Amministrazione, Pagamenti.

I Direttori di Divisione trasmettono all'OdV eventuali segnalazioni pervenute o comunque evidenziate rispetto alle misure descritte nel Modello Organizzativo e specificatamente:

- verifiche ispettive condotte da Enti Pubblici, Pubbliche Amministrazioni e Autorità Pubbliche di Vigilanza;
- esiti delle certificazioni a standard internazionalmente riconosciuti;
- esiti del controllo analogo svolto dagli Enti Soci.

Devono essere assicurati all'OdV i flussi informativi attivati al verificarsi di particolari eventi, quali ad esempio segnalazioni di violazioni sospette o accertate delle prescrizioni contenute nel Modello ovvero, più in generale, segnalazioni di commissione sospetta o accertata di reati



presupposto, o incidenti di sicurezza di particolare gravità ecc.

Si riportano di seguito alcune prescrizioni di carattere generale che riguardano i flussi di comunicazione verso l'OdV:

- Devono essere comunicate all'OdV tutte le deleghe e/o procure conferite ai vari responsabili e/o soggetti che operano in una delle attività definite a rischio-reato e le modifiche delle stesse;
- Devono essere raccolte da ciascun Responsabile tutte le eventuali segnalazioni relative alla commissione, o al ragionevole pericolo di commissione, dei reati contemplati dal Decreto; o comunque a comportamenti in generale non in linea con i principi contenuti nel Codice Etico e di Comportamento e con le regole di comportamento di cui al presente Modello Organizzativo;
- Ciascun dipendente deve segnalare la violazione (o le informazioni che lasciano presumere l'esistenza di una violazione) del presente Modello Organizzativo, contattando il proprio diretto superiore gerarchico e/o l'OdV;
- L'OdV deve ricevere le notizie relative ai procedimenti disciplinari azionati anche in relazione a notizia di violazione del Modello Organizzativo e alle sanzioni irrogate (ivi compresi i provvedimenti assunti verso i dipendenti), come pure notizie circa l'andamento di tali procedimenti.

L'OdV concorda con il Consiglio di Amministrazione i flussi informativi che ritiene necessario ricevere dalle strutture organizzative interne a Lepida per la verifica delle attività ritenute più sensibili per l'azienda.

L'OdV è tenuto a valutare adeguatamente le segnalazioni ricevute e le conseguenti attività da porre in essere. Eventuali provvedimenti dovranno essere definiti e applicati in conformità a quanto previsto in ordine al sistema sanzionatorio definito nel Codice Etico e di Comportamento.

L'OdV ha facoltà di non prendere in considerazione eventuali segnalazioni anonime.

È impegno preciso dell'OdV assicurare la necessaria e dovuta riservatezza e confidenzialità riguardo all'identità delle persone che effettuano le segnalazioni, al fine di evitare qualsiasi forma di ritorsione, discriminazione o penalizzazione.

Nel caso in cui l'OdV riceva notizie e/o informazioni false, fornite in mala fede e/o con dolo sarà suo dovere segnalare l'accaduto ai soggetti titolari del potere di porre in essere gli eventuali provvedimenti conseguenti.

In ogni caso, in aggiunta ai suddetti obblighi di informazione, è fatto obbligo in capo a qualsiasi dipendente e/o componente degli organi sociali, di fornire tutte le informazioni necessarie a fronte di richieste da parte dell'OdV, o al verificarsi di eventi o circostanze rilevanti ai fini dello svolgimento delle attività dell'OdV, fatti salvi tutti gli obblighi di legge per la tutela dei diritti della Società e delle persone.

Ogni informazione, segnalazione, report, previsti nel Modello sono conservati dall'OdV in un apposito archivio riservato (informatico o cartaceo), al quale potranno avere accesso solamente i componenti dell'OdV medesimo.

7.7 Tipologie di informazioni e segnalazioni verso l'Organismo di Vigilanza

L'OdV, ai sensi del Decreto, deve essere informato dai soggetti tenuti all'osservanza del



Modello, in merito ad eventi che potrebbero determinare la responsabilità di Lepida.

I Flussi informativi possono essere:

1. Segnalazioni, che dovranno essere in forma scritta e avere ad oggetto ogni violazione o sospetto di violazione del Modello;
2. Le seguenti Informazioni Rilevanti:
 - copia di tutti gli atti in materia penale, ispettiva e/o tributaria diretti agli Amministratori, Dipendenti, Consulenti della Società o che comunque coinvolgono e possono coinvolgere in dette materie la Società;
 - provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività di indagine per i reati di cui al Decreto, avviate anche nei confronti di ignoti;
 - segnalazioni inoltrate alla Società dai Dipendenti in caso di avvio di procedimento giudiziario a loro carico per uno dei reati previsti dal Decreto;
 - rapporti predisposti dalle strutture aziendali nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto;
 - in via periodica, le notizie relative all'effettiva attuazione del Modello a tutti i livelli aziendali;
 - l'informativa relativa all'avvio di indagini dirette ad appurare, ed eventualmente sanzionare, il mancato rispetto dei principi di comportamento e dei protocolli previsti dal Modello, nonché l'informativa sulle eventuali sanzioni irrogate;
 - violazioni del Codice Etico e di Comportamento;
 - devono essere trasmesse da ciascun responsabile di Funzione eventuali segnalazioni relative alla commissione o al ragionevole pericolo di commissione dei reati contemplati dal Decreto o comunque a comportamenti in generale non in linea con le regole di comportamento di cui al Modello;
 - prospetti riepilogativi degli appalti affidati a seguito di gare o a trattativa privata;
 - le notizie relative a cambiamenti organizzativi;
 - gli aggiornamenti del sistema delle deleghe e dei poteri;
 - le eventuali comunicazioni della società di revisione riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società;
 - le dichiarazioni di veridicità e completezza delle informazioni contenute nelle comunicazioni sociali.

7.8 Raccolta e conservazione delle informazioni

Ogni flusso informativo, verbale, corrispondenza, report previsto nel Modello sarà conservato dall'OdV in un apposito Database informatico e/o cartaceo, ordinato per date e con numero di protocollo, nel rispetto della normativa sulla protezione dei dati personali.

I dati e le informazioni contenute nel database sono poste a disposizione di soggetti esterni all'OdV che ne possano aver diritto, previa autorizzazione dell'organismo stesso e con immediata informazione al CdA di Lepida e al Collegio Sindacale.

Il CdA stabilisce con delibera i criteri e le condizioni con cui è possibile accedere al database.

Al fine di agevolare la comunicazione da e verso l'ODV è stata istituita e comunicata a tutti i dipendenti apposita casella di posta elettronica (odv@lepidait) la cui titolarità è riservata ai



soli membri del ODV. Ai fini dell'archiviazione dei documenti dell'ODV è stata istituita nell'ambito del protocollo di Lepida una sezione riservata proprio all'Organismo di Vigilanza.

8. Comunicazione e diffusione

8.1 Diffusione verso l'interno

È preciso impegno di Lepida dare ampia divulgazione dei principi contenuti nel presente Modello Organizzativo sia all'interno che all'esterno della Società. A tal fine, Lepida pone in essere opportune iniziative atte a promuovere e a diffondere la conoscenza del presente Modello Organizzativo, utilizzando le modalità più opportune a seconda del ruolo, responsabilità e compito in Società dei Destinatari.

Il presente Modello Organizzativo è comunicato formalmente secondo le modalità di seguito descritte.

8.1.1 Comunicazione e formazione in generale

Al fine di assicurare la più completa e ampia diffusione dei principi e delle regole previste dal presente Modello Organizzativo, viene reso disponibile a tutti i dipendenti di Lepida per mezzo della rete intranet aziendale, nonché tramite il portale e il sito Internet della Società.

I dipendenti sono informati della redazione e dei successivi aggiornamenti del Modello Organizzativo.

Per tutti i dipendenti sono realizzate opportune attività di informazione (quali, ad es., invio di email di aggiornamento, di comunicazione, etc.) o iniziative periodiche di formazione ad hoc. La comunicazione riguarda a titolo esemplificativo: (1) il Codice Etico e di Comportamento; (2) i diversi poteri autorizzativi; (3) le linee di dipendenza gerarchica; (4) le Procedure aziendali; (5) i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano.

A seguito dell'approvazione della Ed. 05 del presente Modello, l'Organismo di Vigilanza, in collaborazione con il Dipartimento Amministrazione, ha curato l'ideazione e la realizzazione di un corso di formazione dal titolo *"Il Decreto Legislativo 231/2001: Modello di organizzazione e gestione in Lepida ScpA"*.

Il corso, erogato ai dipendenti tramite piattaforma [SELF](#) (Sistema di E-learning federato per la Pubblica Amministrazione in Emilia-Romagna) a partire dal febbraio 2020, è articolato in 4 moduli: 3 di carattere generale, volti a fornire gli elementi indispensabili per conoscere i presupposti della responsabilità amministrativa degli Enti e il D.Lgs. 231/2001, oltre ad 1 specifico modulo dedicato alla diffusione e all'illustrazione del Modello organizzativo di Lepida.

Il Corso è stato strutturato secondo lo standard SCORM, con brevi video e diapositive, oltre a test di verifica per ciascun modulo e un test finale con relativo attestato rilasciato a ciascun dipendente.

A valle dell'assunzione, nel corso del primo anno di servizio ai neoassunti viene richiesto di seguire le formazioni SELF aventi ad oggetto *"Percorso di formazione generale in tema di prevenzione e sicurezza sul lavoro"*, *"Il Decreto Legislativo 231/2001: Modello di organizzazione e gestione in Lepida ScpA"* e, infine, in materia di privacy, *"La nuova disciplina in tema di*



protezione dei dati personali”.

Nel mese di ottobre 2022, è stato erogato il corso di formazione in materia di anticorruzione e trasparenza ai Direttori e ai Responsabili di Area. Tale contenuti sono stati utilizzati per creare un corso di formazione in modalità FAD da erogare a tutti i dipendenti di Lepida.

Il corso in modalità FAD in materia di anticorruzione e trasparenza è stato messo a disposizione ed erogato a tutti i dipendenti di Lepida a partire dal 1° febbraio al 31 marzo 2024. E' in via di definizione un corso, promosso a cura dell'Organismo di Vigilanza di Lepida, in tema di whistleblowing; tale corso verrà somministrato al personale della Società tra la fine 2024 e l'inizio 2025.

8.1.2 Comunicazione e formazione

I principi, le regole e le disposizioni del presente Modello Organizzativo, anche con riferimento alla tutela della salute e sicurezza dei lavoratori, sono comunicati in maniera più specifica e mirata ai seguenti soggetti aziendali:

- membri del CdA;
- dirigenti;
- tutto il personale.

Il piano delle iniziative di comunicazione e formazione è definito dall'OdV, coadiuvato e in coordinamento con l'Area Amministrazione.

8.2 Diffusione verso l'esterno

Nel rispetto dei principi fondamentali di Lepida legati alla trasparenza, correttezza e integrità, l'adozione del Modello Organizzativo è comunicata e diffusa anche ai soggetti esterni all'azienda, quali clienti, fornitori e terzi in genere. I documenti descrittivi del Modello Organizzativo sono infatti messi a disposizione sul sito internet di Lepida.

L'avvenuta comunicazione e l'impegno formale da parte dei suddetti soggetti esterni al rispetto dei principi del Codice Etico e di Comportamento di Lepida, sono documentati attraverso la predisposizione di specifiche dichiarazioni o clausole contrattuali debitamente sottoposte e accettate dalla controparte.

In merito agli adempimenti circa la comunicazione e diffusione all'esterno, si richiamano in particolare le seguenti responsabilità:

- ciascun Responsabile dell'area/funzione aziendale e ciascun Direttore è responsabile di mantenere la corretta comunicazione sia al proprio interno, sia all'esterno dell'azienda, per ciò che concerne l'adozione e attuazione del Modello Organizzativo;
- l'OdV effettua un'attività di supporto per le informazioni all'esterno di Lepida relative al Modello Organizzativo.



PARTE SPECIALE



Introduzione

La presente parte speciale è elaborata in considerazione del paragrafo di parte generale [4.5.4 Fattispecie di reato a maggior rischio potenziale](#) e dell'identificazione compiuta in relazione alle macroattività a maggior rischio potenziale [4.5.3 Identificazione Macroattività a maggior rischio](#).

Come riferito nella Parte Generale, quella Speciale ha tenuto conto delle fattispecie la cui analisi, in relazione al processo produttivo, ha dato atto della presenza di un rischio potenziale alto v. [4.4.5 Calcolo del rischio potenziale \(o assoluto\)](#).

0. Fattispecie escluse o abrogate

Al riguardo si può fare riferimento alla tabella riportata nel paragrafo [4.5.1 Identificazione dei reati esclusi ex ante](#).

0.1 Principi generali di comportamento

La presente Parte Speciale si riferisce a comportamenti posti in essere da Amministratori, Dirigenti e Dipendenti di Lepida, nonché da Partner e Collaboratori esterni o fornitori con essa operanti sulla base di un rapporto contrattuale, anche temporaneo (qui di seguito, tutti definiti "Destinatari").

Obiettivo della presente Parte Speciale è che i Destinatari adottino regole di condotta conformi a quanto prescritto nel Modello, nonché a quanto previsto nel Codice Etico e di Comportamento di Lepida, al fine di impedire il verificarsi dei reati contemplati nel Decreto.

Pertanto, la presente Parte Speciale sancisce – a carico degli Amministratori, dei Dirigenti e dei Dipendenti in via diretta e altresì a carico dei Partner e di tutti i Collaboratori esterni o fornitori tramite apposite clausole contrattuali – il divieto di:

- porre in essere comportamenti tali da integrare le fattispecie di reato di cui al Decreto identificate nel presente documento;
- porre in essere comportamenti che, sebbene non siano tali da costituire di per sé fattispecie di reato, possano comunque potenzialmente diventarlo;
- porre in essere qualsiasi situazione di conflitto di interessi, anche solo potenziale, nei confronti della Pubblica Amministrazione in relazione alle riferite ipotesi di reato.

Segnatamente è fatto divieto di:

- creare situazioni ove i Destinatari coinvolti in transazioni siano, o possano apparire, in conflitto con gli interessi di Lepida, ovvero creare situazioni che possano interferire con la loro capacità di assumere, in modo imparziale, decisioni nel migliore interesse di Lepida;



- compiere azioni o tenere comportamenti che siano o possano essere interpretati come pratiche di corruzione, favori illegittimi, comportamenti collusivi, sollecitazioni, dirette o mediante terzi, di privilegi per sé o per altri;
- effettuare o promettere ovvero tentare di effettuare o promettere, in favore di pubblici funzionari italiani ed esteri o di loro parenti, anche per interposta persona, elargizioni in denaro, distribuzioni di omaggi o regali, ovvero benefici di qualsivoglia natura, tali da influenzare l'indipendenza di giudizio dei pubblici funzionari stessi ovvero indurli ad assicurare indebiti vantaggi;
- effettuare o promettere, in favore dei Soci, prestazioni che non trovino adeguata giustificazione alla luce del rapporto associativo con essi costituito;
- riconoscere oppure tentare di riconoscere, in favore dei collaboratori esterni, compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alla prassi vigente nel settore di attività interessato;
- presentare o tentare di presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire finanziamenti, contributi o erogazioni di varia natura oppure per ottenere un indebito beneficio o qualsiasi altro vantaggio per Lepida;
- destinare o tentare di destinare le somme ricevute da detti organismi pubblici a scopi diversi da quelli per i quali erano stati concessi;
- alterare il funzionamento di un sistema informatico ovvero manipolare i dati in esso contenuti al fine di ottenere un indebito vantaggio a danno di terzi.

0.2 Principi generali di controllo

Costituiscono principi generali di controllo, da applicarsi con riferimento a tutti i processi aziendali individuati come a rischio:

1. CHIARA IDENTIFICAZIONE E RESPONSABILITÀ DI CIASCUNA OPERAZIONE/PROCESSO

La responsabilità di ogni operazione/processo aziendale deve essere chiaramente definita e conosciuta all'interno dell'organizzazione.

2. SEGREGAZIONE DI FUNZIONI/ATTIVITÀ ALL'INTERNO DI CIASCUNA OPERAZIONE/PROCESSO

Lo svolgimento delle diverse attività in cui si articola ciascuna operazione/processo deve essere svolta da soggetti diversi. Il coinvolgimento di esponenti aziendali diversi disincentiva infatti la commissione di reati o irregolarità e, comunque, consente una puntuale individuazione del soggetto cui ascrivere specifiche responsabilità.

3. TRACCIABILITÀ DI ATTI E OPERAZIONI

Ogni operazione o fatto gestionale posto in essere con riguardo ai processi sensibili deve venire documentato, in forma scritta, in modo che sia sempre possibile verificare l'iter in cui si è articolata ciascuna attività e individuare, ove necessario, i soggetti responsabili.

4. EVIDENZA FORMALE DEI CONTROLLI

I controlli che vengono effettuati all'interno di un processo devono lasciare una traccia documentale, così che si possa, anche in un momento successivo, verificare lo svolgimento del controllo, identificare colui che lo ha posto in essere e valutarne l'operato.

5. SISTEMA DI DELEGHE E PROCURE



In ambito aziendale deve essere adottato un sistema di deleghe interne, per mezzo del quale a ciascun esponente aziendale siano attribuiti compiti e responsabilità nell'ambito della gestione delle diverse attività. Esiste altresì un sistema di procure, finalizzate al conferimento di poteri di firma e di spesa in capo a esponenti aziendali individuati dal CdA.

6. ADOZIONE E IMPLEMENTAZIONE DI SPECIFICHE PROCEDURE/PROTOCOLLI

Le attività emerse come sensibili sono disciplinate da procedure/protocolli, che diano completa attuazione dei principi di controllo di cui al presente e ai successivi paragrafi.

7. COMUNICAZIONE CONTINUATIVA ALL'ORGANISMO DI VIGILANZA DELLE INFORMAZIONI CONCERNENTI LE OPERAZIONI A RISCHIO

La Società individua taluni soggetti qualificati come Responsabili Interni, i quali sono tenuti, tra l'altro, a inviare con cadenza periodica all'Organismo di Vigilanza le informazioni relative alle operazioni sensibili e all'attuazione del Modello Organizzativo.

8. INFORMATIVA TEMPESTIVA ALL'ORGANISMO DI VIGILANZA DI ANOMALIE O VIOLAZIONI DEL MODELLO ORGANIZZATIVO

Tutti i dipendenti e coloro che operano a nome o nell'interesse di Lepida sono tenuti a comunicare per iscritto e in modo tempestivo all'Organismo di Vigilanza la notizia circa comportamenti anomali, anche se non ancora di rilevanza penale, tenuti in ambito aziendale, ovvero le vere e proprie violazioni del Modello Organizzativo di cui siano venuti a conoscenza.

9. UTILIZZO DI SISTEMI INFORMATICI CON RIFERIMENTO ALLE OPERAZIONI SENSIBILI

Per quanto possibile, la Società ricorre all'utilizzo di sistemi informatici con riferimento alle operazioni sensibili, in modo che siano garantite tracciabilità e gestione uniforme delle diverse attività.

10. MONITORAGGIO DA PARTE DELL'ORGANISMO DI VIGILANZA DELL'ATTUAZIONE DEL MODELLO ORGANIZZATIVO

L'Organismo di Vigilanza pone in essere un'attività continuativa di monitoraggio sull'osservanza e sull'attuazione del Modello Organizzativo. Tale attività, opportunamente documentata, è finalizzata alla individuazione di interventi da apportare al Modello Organizzativo, nonché alla promozione di procedimenti disciplinari a carico di coloro che abbiano violato le misure preventive adottate dalla Azienda.

11. INDIVIDUAZIONE DEI SOGGETTI AZIENDALI AUTORIZZATI A INTRATTENERE RAPPORTI CON PUBBLICHE AMMINISTRAZIONI

Fermi restando i poteri di firma attribuiti con procura, in ambito aziendale devono essere espressamente individuati i soggetti autorizzati a intrattenere rapporti con soggetti pubblici.

12. PREVISIONE DI CLAUSOLE AD HOC NEI CONTRATTI CON COLLABORATORI ESTERNI, CONSULENTI, FORNITORI

Nei contratti stipulati con collaboratori esterni, consulenti, e fornitori devono essere inserite specifiche clausole con cui gli stessi attestino di essere a conoscenza del Codice Etico e di Comportamento e del presente Modello Organizzativo e si impegnino a uniformarsi ai principi e alle procedure in essi contenuti. I contratti devono altresì prevedere che comportamenti violativi dell'obbligo così assunto consentano la risoluzione del contratto e la richiesta di risarcimento dei danni da parte di Lepida (clausola risolutiva espressa, penale, etc). Ai collaboratori esterni, ai consulenti, e



Fornitori che intrattengono rapporti con la P.A. per conto di Lepida, deve esser formalmente conferito potere in tal senso (con apposita clausola inserita nel contratto). Gli stessi soggetti devono sottoscrivere una dichiarazione in cui si attesta la conoscenza del Codice Etico e di Comportamento e del presente Modello Organizzativo e l'impegno di uniformarsi ai principi e alle procedure in essi contenuti.

13. RIUNIONI TRA ORGANISMO DI VIGILANZA, COLLEGIO SINDACALE E SOCIETÀ INCARICATA DELLA REVISIONE LEGALE DEI CONTI

L'Organismo di Vigilanza e il Collegio Sindacale (qualora non rivesta le funzioni di OdV) organizzano riunioni semestrali con la Società incaricata della revisione legale dei conti per la condivisione in merito al monitoraggio e all'esito dei controlli effettuati ciascuno nell'ambito delle attività di propria competenza.

1. Reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

1.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

1.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)), sono state le seguenti fattispecie:

<p>Art. 24 - Indebita percezione di erogazioni, truffa in danno dello stato o di un Ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un Ente pubblico</p>	<ul style="list-style-type: none"> - Malversazione a danno dello Stato (316-bis c.p.); - Indebita percezione di erogazioni a danno dello Stato (316-ter c.p.); - Truffa aggravata in danno dello Stato o di altro Ente pubblico (art. 640, co. 2, n. 1 c.p.); - Truffa aggravata per il conseguimento di erogazioni pubbliche (640-bis c.p.); - Frode informatica (640-ter c.p.) se commesso in danno dello Stato o di altro Ente pubblico; - Frode nelle pubbliche forniture (356 c.p.); - Art. 2 L. 23 dicembre 1986, n. 898; - Turbata libertà degli incanti (art. 353 c.p.); - Turbata libertà del procedimento di scelta del contraente (art. 353 - bis c.p.).
---	--



<p>Art. 25 - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione</p>	<ul style="list-style-type: none"> - Corruzione per l'esercizio delle funzione (art. 318 c.p.); - Pene per il corruttore (321 c.p.); - Istigazione alla corruzione (322, co. 1 e 3, c.p.); - Traffico di influenze illecite (346 bis c.p.); - Peculato (314, co. 1, c.p.), quando sono offesi interessi finanziari UE; - Indebita destinazione di denaro o cose mobili (314 bis c.p.), quando sono offesi interessi finanziari dell' UE; - Peculato mediante profitto dell'errore altrui (316 c.p.), quando sono offesi interessi finanziari UE"; - Corruzione per un atto contrario ai doveri d'ufficio (319 c.p.); - Corruzione in atti giudiziari (319 ter, co. 1 c.p.); - Pene per il corruttore (art. 321 c.p.); - Istigazione alla corruzione (art. 322, co. 2 e 4 c.p.); - Concussione (317 c.p.); - Corruzione per un atto contrario ai doveri d'ufficio aggravata quando dal fatto l'ente ha conseguito un profitto di rilevante entità (319 e 319 bis c.p.); - Corruzione in atti giudiziari (319 ter, co. 2, c.p.); - Induzione indebita a dare o promettere utilità (319 quater c.p.); - Pene per il corruttore (art. 321 c.p.).
---	--

1.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B.** attività di selezione del personale e di mobilità interna;
- C.** gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- E.** gestione della rendicontazione amministrativa verso gli Enti Soci;
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di



revisione, modalità formazione del capitale sociale;

G. gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;

H. gestione degli aspetti afferenti la sicurezza e l'igiene sul lavoro;

I. acquisto e utilizzo di valori di bollo;

J. gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale;

K. gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva);

L. gestione contenzioso legale;

M. gestione rifiuti.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

1.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo *"di primo grado"* non accettabile (FASE 1 - **punto 3**)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento Lepida

(Allegato e parte integrante del presente Modello)

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

(Allegato e parte integrante del presente Modello)

Certificazione ISO 9001

La norma specifica i requisiti di un sistema di gestione per la qualità quando un'organizzazione ha (1) l'esigenza di dimostrare la propria capacità di fornire con regolarità prodotti o servizi che soddisfano i requisiti del cliente e i requisiti cogenti applicabili; e (2) mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del sistema, compresi i processi per il miglioramento del sistema stesso e assicurare la conformità ai requisiti del cliente e ai requisiti cogenti applicabili. Tutti i requisiti sono di carattere generale e previsti per essere applicabili a



tutte le organizzazioni, indipendentemente da tipo o dimensione, o dai prodotti forniti e servizi erogati.

Certificazione ISO 37001

La norma certifica il Sistema di gestione per la prevenzione della corruzione, specificando le misure e i controlli adottati per monitorare le attività aziendali e implementare l'efficacia di prevenzione del fenomeno di corruzione.

Lepida ha ottenuto la Certificazione ISO 37001 in data 23 dicembre 2022.

Certificazione ISO/IEC 27001

La norma UNI EN ISO/IEC 27001 specifica i requisiti necessari a stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Questo standard internazionale include, inoltre, i requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione.

Regolamento [015] Gestione Firme

Il Regolamento definisce le modalità operative per la stesura, verifica, approvazione e sottoscrizione di tutti i documenti prodotti nell'ambito dei processi aziendali per garantire uniformità, completezza e regolarità procedurale nel rispetto del vigente assetto organizzativo e del sistema di deleghe e procure in essere.

In un'ottica di snellimento dei flussi organizzativi e gestionali, sono predisposti per la sottoscrizione del Presidente solo ed unicamente i documenti che richiedano in via indefettibile la firma del legale rappresentante; diversamente, il documento verrà portato alla sottoscrizione del DG.

Qualunque atto alla firma del Presidente deve essere preventivamente vagliato dal DG e dal Direttore di Dipartimento /Divisione proponente, qualora esistente in organigramma, che provvedono a siglarlo in calce.

Laddove invece, come di norma avviene, l'atto debba essere posto alla firma del DG, a valle della stesura da parte dell'estensore - condivisa necessariamente con i Direttori in conformità al Regolamento [010] gestione Direttori - deve recare il vaglio formale del Direttore di Dipartimento / Divisione.

Infine, anche, i documenti predisposti a firma del Direttore di Dipartimento / Divisione devono essere preventivamente visti dal Responsabile estensore.

Reati a rischio residuo "di primo grado" non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 24 - Indebita percezione di erogazioni, truffa in danno dello stato o di un Ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un Ente pubblico</p>	<ul style="list-style-type: none"> - Truffa aggravata per il conseguimento di erogazioni pubbliche (640-bis c.p.); - Frode nelle pubbliche forniture (356 c.p.); - Art. 2 L. 23 dicembre 1986, n. 898; - Turbata libertà degli incanti (art. 353 c.p.); - Turbata libertà del procedimento di scelta del contraente (art. 353 - bis c.p.).
<p>Art. 25 - Peculato, indebita destinazione di</p>	<ul style="list-style-type: none"> - Corruzione per un atto contrario ai doveri



<p>denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione</p>	<p>d'ufficio (319 c.p.); - Corruzione in atti giudiziari (319 ter, co. 1 c.p.); - Pene per il corruttore (art. 321 c.p.); - Istigazione alla corruzione (art. 322, co. 2 e 4 c.p.); - Concussione (317 c.p.); - Corruzione per un atto contrario ai doveri d'ufficio aggravata quando dal fatto l'ente ha conseguito un profitto di rilevante entità (319 e 319 bis c.p.); - Corruzione in atti giudiziari (319 ter, co. 2, c.p.); - Induzione indebita a dare o promettere utilità (319 quater c.p.); - Pene per il corruttore (art. 321 c.p.).</p>
--	--

1.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo "di primo grado" non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

1.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B.** attività di selezione del personale e di mobilità interna;
- C.** gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** Gestione dei servizi, infrastrutture, livelli di servizio;
- G.** gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;
- J.** gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale;
- K.** gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva).



1.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Norme di Trasparenza di gestione Lepida

Le Norme di Trasparenza e di Gestione di Lepida costituiscono uno dei documenti fondamentali per l'attività della Società. Il Regolamento è idealmente suddiviso in una *prima sezione* afferente alle Procedure di Acquisto e in una *seconda* relativa agli Incentivi ai Direttori, Procedure Assunzioni e al Conferimento di incarichi professionali per servizi legali.

Il Regolamento ha il taglio di un documento esplicativo rivolto all'esterno e illustra le modalità e le regole con le quali Lepida ha scelto di autovincolarsi, dando applicazione al Codice dei Contratti Pubblici (D.Lgs. 36/2023). I principali riferimenti sono, pertanto, a: Procedura per acquisti di modico valore, per importi non superiori a 1.000 euro; Procedura di Verifica Unicità; Affidamento diretto senza consultazione di operatori economici fino a 5.000 euro; Affidamento diretto previa consultazione di operatori economici mediante procedura con Richiesta di preventivi per importi inferiori a 140.000,00 per servizi e forniture e per importi inferiori a 150.000,00 per lavori; Procedura con Richiesta di Offerta in qualità di Operatore TLC; Procedura sotto soglia comunitaria con Richiesta di Offerta; Procedure sopra soglia comunitaria e, infine, per le Sponsorizzazioni.

La sezione relativa alle Procedure di assunzione ha invece lo scopo di dotare Lepida di procedure volte a disciplinare il processo di ricerca e selezione del personale per assunzioni con rapporto di lavoro subordinato a tempo indeterminato, in attuazione e in conformità all'art 19 del D.Lgs. 175/2016, nel rispetto dei principi indicati dall'art. 35.3 del D.Lgs. 165/2001.

Infine, il Regolamento delinea anche l'affidamento di incarichi di patrocinio legale - intesi come incarichi di assistenza, difesa e rappresentanza in giudizio conferiti da Lepida in occasione di ogni singola vertenza - a professionisti esterni e le principali condizioni giuridiche ed economiche del relativo incarico di patrocinio legale, nel rispetto dei principi di cui 1, 2 e 3 del D.Lgs. 36/2023.

Programmazione degli acquisti

Conformemente a quanto previsto dall'art. 37 , comma 3, del D.Lgs. 36/2023 , Lepida procede alla definizione e successiva pubblicazione di una programmazione triennale, con aggiornamento annuale, degli acquisti di beni e servizi di importo stimato uguale o superiore a 140.000 euro e di un'ulteriore programmazione triennale, con aggiornamento annuale, dei lavori pubblici il cui valore stimato sia pari o superiore a 150.000 euro.

Utilizzo della piattaforma informatica SATER di Intercent-ER

L'utilizzo di strumenti informatici per l'espletamento delle procedure per l'acquisto di beni e servizi costituisce una modalità tipicamente idonea alla prevenzione di fenomeni corruttivi e distorsivi, rendendo l'iter procedurale ancora più trasparente.

Regolamento [014] per Mobilità e Selezione Personale

Il Regolamento, adottato in conformità all'art. 19, comma 2 D.Lgs. 175/2016, è armonizzato con le Norme di Trasparenza e disciplina, a fronte di un fabbisogno di personale, i criteri e la procedura della mobilità interna, preliminare all'indizione della procedura di selezione ad evidenza pubblica, nel rispetto di meccanismi oggettivi e trasparenti.



Regolamento [012] Forniture & Mandati

Il Regolamento disciplina l'iter procedimentale interno relativo alle procedure di acquisizione. Il documento scandisce le fasi procedurali, le competenze dei singoli soggetti e individua i soggetti titolari dei poteri autorizzativi indispensabili all'avvio della procedura.

Condizioni generali di contratto di Lepida

Il documento disciplina le Condizioni generali di contratto che regolano i rapporti contrattuali tra Lepida e gli aggiudicatari contraenti. Oltre all'esatta osservanza delle condizioni stabilite nel contratto di appalto, come definito all'art. 1 "Definizioni", lettera e), con la presentazione dell'offerta, il Partecipante accetta incondizionatamente quanto disciplinato nelle Condizioni generali di contratto di Lepida e quanto indicato nei documenti riferiti alla specifica procedura di acquisto.

Vademecum [022] Conflitto di Interessi

Il Vademecum rappresenta uno strumento di ausilio per il processo di autovalutazione del dipendente - al fine di intercettare situazioni in grado di influenzare negativamente l'esercizio imparziale e obiettivo delle proprie funzioni - nonché una guida per la gestione dell'eventuale conflitto di interessi che costituisce il potenziale presupposto di condotte distorsive e illecite.

Regolamento [023] Incarichi Extra Istituzionali

Il Regolamento disciplina i limiti, i criteri e le modalità per l'autorizzazione preventiva degli incarichi extraistituzionali ai dipendenti quale specifica misura integrativa di prevenzione della corruzione e della trasparenza.

Procedura Gestione del Ciclo attivo

La procedura descrive i processi di elaborazione delle offerte, dei contratti e degli ordini di vendita, di controllo della fase dell'esecuzione dei contratti e degli ordini di vendita e fatturazione, definendo le responsabilità degli attori del processo.

Procedura Gestione del Ciclo passivo

Il documento ha l'obiettivo di descrivere - in conformità al vigente Codice dei Contratti Pubblici e in coerenza con le Norme di Trasparenza di Gestione di Lepida - le procedure di (1) *acquisizione di beni, servizi e lavori*; (2) *esecuzione ed elaborazione degli ordini di acquisto*; e (3) *controllo dell'esecuzione delle forniture e liquidazione*, definendo le responsabilità dei diversi attori coinvolti.

Fatturazione elettronica, Conservazione sostitutiva e accreditamento IPA

A partire dal 01.01.2019, ai sensi dell'art. 1, co. 909, Lepida riceve ed emette fatture unicamente in formato elettronico. A partire dal 15/09/2020, Lepida è accreditata nell'Indice dei Domicili digitali della Pubblica Amministrazione e Gestori dei Pubblici Servizi (IPA), con la conseguente attribuzione di un Codice Univoco Ufficio e ricezione di fatture passive in formato Fattura PA. I documenti fiscali sono ricevuti mediante intermediario NoTI-ER Intercent-ER e inviati in conservazione al ParER.

Protocollo elettronico aziendale



Tutte le comunicazioni e i contratti trasmessi o ricevuti da Lepida vengono registrati nel Protocollo elettronico aziendale, che attribuisce un numero progressivo di protocollazione, al fine di consentirne la tracciabilità.

Regolamento [028] Whistleblowing

Il Regolamento descrive in modo semplificato e procedimentale, richiamando la più estesa Procedura, i presupposti e le modalità con cui segnalare condotte (reati, meri illeciti o irregolarità) che contrastino con l'interesse pubblicistico a cui l'azione di Lepida si conforma.

1.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.

2. Reati informatici e illecito trattamento dei dati personali (art. 24-bis del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

2.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

2.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 24 bis - Delitti informatici e trattamento illecito di dati</p>	<ul style="list-style-type: none"> - Accesso abusivo ad un sistema informatico o telematico (615-ter c.p.); - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater c.p.); - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 quinquies c.p.); Estorsione informatica (art. 629, comma 3, c.p.) - Danneggiamento di informazioni, dati e programmi informatici (635 bis c.p.);
--	--



	<ul style="list-style-type: none"> - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (635 ter c.p.); - Danneggiamento di sistemi informatici o telematici (635 quater c.p.); - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (635 quater 1 c.p.); - Danneggiamento di sistemi informatici o telematici di pubblica utilità (635 quinquies c.p.); - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 quater c.p.); - Falsità in documenti informatici (491 bis c.p.); - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.); - Delitti di cui all'art. 1, co. 11, D.L. 21 settembre 2019, n. 105.
--	--

2.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli enti;

D. Gestione dei servizi, infrastrutture, livelli di servizio.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D8 - Divisione Progetti Strategici & Speciali
- D9 - Dipartimento Accesso
- DA - Divisione Sicurezza, Ambiente & Emergenza



- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

2.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo *"di primo grado"* non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento di Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO/IEC 27001, 27017, 27018

La norma ISO/IEC 27001 specifica i requisiti necessari a stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Questo standard internazionale include, inoltre, i requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione.

La norma ISO/IEC 27017:2015 supporta l'implementazione di controlli sulla sicurezza delle informazioni per fornitori di servizi cloud e per gli utenti degli stessi. La norma ISO/IEC 27018:2019, invece, individua elementi di attenzione, controlli e linee guida necessari ad implementare misure di protezione dei dati personali per un fornitore pubblico di servizi di cloud computing.

Certificazione ISO 37001

Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo *"di primo grado"* non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 24 bis - Delitti informatici e trattamento illecito di dati</p>	<ul style="list-style-type: none"> - Accesso abusivo ad un sistema informatico o telematico (615-ter c.p.); - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater c.p.); - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 quinquies c.p.);
--	--



	<p>Estorsione informatica (art. 629, comma 3, c.p.);</p> <ul style="list-style-type: none"> - Danneggiamento di informazioni, dati e programmi informatici (635 bis c.p.); - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (635 ter c.p.); - Danneggiamento di sistemi informatici o telematici (635 quater c.p.); - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (635 quater 1 c.p.); - Danneggiamento di sistemi informatici o telematici di pubblica utilità (635 quinquies c.p.); - Falsità in documenti informatici (491 bis c.p.); - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).
--	---

2.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo "di primo grado" non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

2.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- D.** gestione dei servizi, infrastrutture, livelli di servizio.



2.2.2 Controlli societari periferici (FASE 2 – punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Modello Organizzativo in materia di protezione dei dati personali

Con il documento Lepida ha definito il proprio ambito di titolarità, delega al Direttore Generale e ai Direttori di Divisioni in materia di tutela dei dati personali, ciascuno per il proprio ambito di competenza, l'attuazione degli adempimenti previsti dalla normativa in materia; ha indicato i compiti assegnati al DPO designato; definito i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità.

Il Documento enuclea ruoli e responsabilità di Titolare del Trattamento, Soggetti Delegati Attuatori, Direttore Generale, Responsabili del Trattamento, Incaricati del Trattamento e Responsabile della Protezione dei Dati (per quest'ultimo, anche con riferimento alle richieste di accesso civico generalizzato di cui all'art. 5, co. 2, D.Lgs. 33/2013).

Regolamento [002] Riservatezza Informazioni e Documenti

Secondo il regolamento in parola, ogni dipendente e collaboratore di Lepida si impegna a mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza nello svolgimento delle proprie attività lavorative, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari allo svolgimento delle proprie attività e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione da Lepida.

L'obbligo in parola - declinato nelle singole previsioni che compongono il Regolamento - sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione delle proprie attività, mentre è da escludersi per i dati che siano o divengano di pubblico dominio. Sia per i dipendenti che per i collaboratori l'obbligo di riservatezza permane per tutta la durata del rapporto di lavoro con Lepida, nonché per i tre anni successivi al termine dello stesso.

Regolamento [019] Videosorveglianza Patrimonio Aziendale

Il Regolamento descrive il sistema di videosorveglianza installato da Lepida presso le proprie sedi aziendali, formalizzando le regole tecniche e organizzative applicate ai trattamenti delle immagini ottenute mediante tali sistemi e fornendo ai dipendenti e collaboratori di Lepida adeguata informativa in ordine al trattamento delle immagini effettuati per mezzo di tali sistemi.

L'utilizzo dei sistemi di videosorveglianza è effettuato in conformità alle vigenti prescrizioni normative in materia di protezione dei dati personali, alle norme a tutela dei lavoratori (L.300/1970), alle disposizioni del Provvedimento in materia di videosorveglianza del Garante per la protezione dei dati personali dell'8 aprile 2010 e agli ulteriori provvedimenti in materia emanati dalla medesima Autorità; la base giuridica del trattamento mediante videosorveglianza viene individuata ai sensi dell' art. 6.1f del Regolamento (UE) 2016/679 GDPR - che ha comportato modifiche al D.Lgs. 196/2003 come emendato dal D.Lgs. 101/2018, - nel legittimo interesse del titolare. Le immagini acquisite sono protette da misure adeguate di



sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità definite in questo regolamento.

Regolamento in materia di Accesso civico e Generalizzato di Lepida

Il documento disciplina i criteri e le modalità organizzative della Società per permettere l'effettivo esercizio da parte della collettività: (1) dell'accesso civico, consistente nel diritto di chiunque di richiedere alle Pubbliche Amministrazioni di pubblicare documenti, informazioni o dati nei casi in cui sia stata omessa la pubblicazione obbligatoria ai sensi di legge; e (2) dell'accesso generalizzato, che comporta il diritto di chiunque di accedere a dati, documenti e informazioni detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria ai sensi del D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'art. 5-bis del citato Decreto.

Disciplinare riguardante l'esercizio dei diritti di cui agli artt. 15-21 del Regolamento UE 2016/679

Inserendosi nell'ambito della suddivisione di competenze fissate dal Modello Organizzativo in materia di protezione dei dati personali, il Disciplinare, unitamente al Modulo per l'esercizio di diritti in materia di protezione dei dati personali, fornisce le regole e le procedure indispensabili fornire riscontro, nei tempi e nei modi previsti dalla legge, ai soggetti che esercitino i diritti di cui agli artt. da 15 a 23 (accesso, rettifica, cancellazione, limitazione del trattamento, portabilità e opposizione al trattamento) del Regolamento UE n. 2016/679.

La Società traccia le istanze pervenute e il relativo seguito in uno specifico Registro delle istanze dell'interessato ex artt. 15 e ss. GDPR.

Procedura per la gestione delle richieste di dati provenienti dall'Autorità giudiziaria o di pubblica sicurezza

Al fine di assicurare la più celere e sicura trasmissione delle informazioni richieste dall'Autorità giudiziaria e dalle Autorità di Pubblica Sicurezza, il Dipartimento Amministrazione, in collaborazione con i Dipartimenti/Divisioni/Progetti interessati, ha adottato una procedura interna di gestione di tali richieste, volta a centralizzare e standardizzare il flusso di lavoro, ad ottenere le necessarie autorizzazioni dai soggetti Titolari del trattamento dei dati richiesti e, infine, alla trasmissione dei dati richiesti con le cautele necessarie ad evitare accessi al dato da parte di soggetti terzi.

La Società traccia le istanze pervenute e il relativo seguito in uno specifico Registro delle richieste dati da Autorità giudiziaria e di pubblica sicurezza.

Manuale Operativo e Guida Utente LepidaID

Il presente manuale illustra l'architettura, le modalità, le procedure adottate dal gestore Lepida per l'erogazione del servizio di Gestione di Identità SPID, come indicato nel DPCM 24 ottobre 2014.

Lepida ID Procedura di cancellazione dei dati del soggetto richiedente

Il documento definisce, in conformità al Regolamento (UE) n. 2016/679 - GDPR, la procedura di cancellazione dei dati e della richiesta di attribuzione di identità digitale in caso di istanza di un soggetto richiedente un'identità LepidaID, qualora l'identità digitale SPID LepidaID non sia stata ancora rilasciata.



LepidaID Modulo di richiesta revoca/sospensione/riattivazione

Il documento definisce le modalità con le quali l'utente titolare di titolare di Identità Digitale SPID LepidaID può chiedere la la revoca, la sospensione o la riattivazione a seguito di una sospensione della propria Identità Digitale.

LepidaID - Procedura blocco/sblocco credenziali (password)

Il documento descrive la procedura di blocco/sblocco credenziali (password) SPID LepidaID di un soggetto in possesso di una identità LepidaID attiva.

Allo stato attuale, Lepida sta provvedendo alle attività di revisione delle procedure relative alla gestione del servizio Lepida ID nell'ottica di implementare i sistemi preposti alla gestione del rilascio e gestione delle identità digitali secondo funzionalità stringenti atte a contenere ed evitare ogni possibile utilizzo indebito o accesso ingiustificato da parte degli operatori preposti.

Procedura Gestione del Ciclo attivo

La procedura descrive i processi di elaborazione delle offerte, dei contratti e degli ordini di vendita, di controllo della fase dell'esecuzione dei contratti e degli ordini di vendita e fatturazione, definendo le responsabilità degli attori del processo. La procedura reca specifiche indicazioni operative riguardanti gli adempimenti in materia di protezione dei dati personali.

Procedura Gestione del Ciclo passivo

Il documento ha l'obiettivo di descrivere - in conformità al vigente Codice dei Contratti Pubblici e in coerenza con le Norme di Trasparenza di Gestione di Lepida - le procedure di (1) *acquisizione di beni, servizi e lavori*; (2) *esecuzione ed elaborazione degli ordini di acquisto*; e (3) *controllo dell'esecuzione delle forniture e liquidazione*, definendo le responsabilità dei diversi attori coinvolti.

Procedura per la gestione degli incidenti di sicurezza

Il documento costituisce il riferimento aziendale per la gestione degli incidenti di sicurezza che possono coinvolgere le attività operative dell'organizzazione, i servizi erogati e le informazioni trattate, anche quando assumono il rilievo di data breach ai sensi del Regolamento UE 2016/679 - GDPR. Lepida traccia gli eventi in uno specifico template di Incident Report.

Disciplinare di sicurezza per utenti dei sistemi informativi

Il disciplinare descrive le regole tecniche e organizzative da applicare per l'utilizzo di strumentazioni informatiche o di servizi del sistema informativo di Lepida. Ciò, al fine di ottimizzare l'impiego delle risorse, introdurre regole di corretto utilizzo nel contesto organizzativo di Lepida, ridurre al minimo i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito di informazioni e dati, compresi i dati personali in relazione ai quali Lepida è Titolare o è designata Responsabile del trattamento, garantire la disponibilità dei servizi e assicurare il rispetto delle norme sul diritto d'autore.

Disciplinare di sicurezza per amministratori di sistema

Il Disciplinare descrive le regole tecniche e organizzative stabilite per gli amministratori di sistema di Lepida al fine di ridurre al minimo i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito di informazioni e dati, compresi i



dati personali in relazione ai quali Lepida è Titolare o è designata Responsabile del trattamento, garantire la disponibilità dei servizi e assicurare il rispetto delle norme sul diritto d'autore.

Disciplinare di sicurezza per applicazioni informatiche

Il Disciplinare descrive gli aspetti tecnici e procedurali richiesti da Lepida per la progettazione, lo sviluppo, il deployment, il test e la gestione di applicazioni sicure al fine di ridurre al minimo i rischi di indisponibilità dei servizi applicativi o di distruzione, perdita, modifica, divulgazione o accesso non autorizzati a dati personali o a dati aziendali riservati. Tali disposizioni garantiscono l'attuazione dei principi di protezione dei dati personali "sin dalla progettazione" (c.d. privacy by design) e "per impostazione predefinita" (c.d. privacy by default) previsti all'Art. 25 del Regolamento (UE) 2016/679 (c.d. GDPR).

Funzionalità specifiche sul sistema LepidaID

Nel corso del 2024, la Società ha implementato alcune specifiche funzionalità tecniche volte ad attuare il principio di minimizzazione dei dati e, quindi, di privacy by design e by default, delimitando, in tal modo, possibili condotte rilevanti ai sensi del D.Lgs. 231/2001 e s.m.i. a titolo di accesso abusivo ad un sistema informatico.

2.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.



3. Delitti di criminalità organizzata (art. 24-ter del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

3.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

3.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 24 ter - Delitti di criminalità organizzata</p>	<ul style="list-style-type: none"> - Associazione per delinquere (art. 416, co. 6, c.p.); - Associazioni di tipo mafioso anche straniere (art. 416 bis c.p.); - Scambio elettorale politico-mafioso (art. 416 ter c.p.); - Delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; - Associazione per delinquere (art. 416, c.p., eccetto comma 6).
---	---

3.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

- A.** Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B.** attività di selezione del personale e di mobilità interna;
- C.** gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- E.** gestione della rendicontazione amministrativa verso gli Enti Soci;
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- G.** gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;



- H. gestione degli aspetti afferenti la sicurezza e l'igiene sul lavoro;
- J. gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale;
- K. gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva);
- L. gestione contenzioso legale;
- M. gestione rifiuti.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D8 - Divisione Progetti Strategici & Speciali
- D9 - Dipartimento Accesso
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

3.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento di Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO/IEC 27001, 27017, 27018

Certificazione ISO 37001

Regolamento [015] Gestione Firme

Vademecum [022] Conflitto di Interessi

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo "di primo grado" non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.



Art. 24 ter - Delitti di criminalità organizzata	Nessuno
--	---------

3.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

3.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- C.** Gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** gestione dei servizi, infrastrutture, livelli di servizio.
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- M.** gestione rifiuti.

3.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Nessuno

3.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, sia pure esclusivamente a livello centrale, non residuano reati con rischio residuo non accettabile.



4. Reati societari di cui agli artt. 2621 e ss. (art. 25-ter del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

4.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

4.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 25 ter - Reati Societari</p>	<ul style="list-style-type: none"> - False comunicazioni sociali (2621 c.c.); - Fatti di lieve entità (2621 bis c.c.); - False comunicazioni sociali delle società quotate (2622 c.c.); - Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 1, c.c., abrogato dal D Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D Lgs. 39/2010); - Illeciti rapporti patrimoniali con la società assoggettata a revisione (2624, co. 2, c.c., abrogato dal D Lgs. 39/2010, ora solo in parte rinvenibile nell'art. 31 D Lgs. 39/2010); - Impedito controllo (2625, co. 2, c.c.); - Formazione fittizia del capitale (2632 c.c.); - Indebita restituzione dei conferimenti (2626 c.c.); - Illegale ripartizione degli utili e delle riserve (2627 c.c.); - Illecite operazioni sulle azioni o quote sociali o della società controllante (2628 c.c.); - Operazioni in pregiudizio dei creditori (2629 c.c.); - Indebita ripartizione dei beni sociali da parte dei liquidatori (2633 c.c.); - Illecita influenza sull'assemblea (2636 c.c.) - Aggiotaggio (2637 c.c.); - Omessa comunicazione del conflitto d'interessi (2629 bis c.c.);
--------------------------------------	---



	<ul style="list-style-type: none"> - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (2638, co. 1 e 2 c.c.); - Corruzione tra privati (2635, co. 3 c.c.) - Istigazione alla corruzione tra privati (2635 bis, co. 1 c.c.).
--	---

4.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

C. gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;

F. bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;

G. gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;

L. gestione contenzioso legale.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D7 - Dipartimento Amministrazione

4.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO 37001

Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).



Reati a rischio residuo “di primo grado” non accettabile

Nonostante l’applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

Art. 25 ter - Reati Societari	nessuno
-------------------------------	---------

4.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell’Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d’esame, in particolare, è stata l’efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo “di secondo grado” questa volta ACCETTABILE.

4.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- F. bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- G. gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;
- L. gestione contenzioso legale.

4.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Revisione Legale dei Conti

Per revisione legale si intende la revisione dei bilanci di esercizio o dei bilanci consolidati effettuata in conformità alle disposizioni del Codice civile e del D.Lgs. 39/2010 (art. 1, D Lgs. 39/2010); si tratta, in altre parole, di un processo complesso di verifiche e procedure svolte, dai revisori persone fisiche e società di revisione iscritti ad uno specifico registro, in conformità ai principi di revisione internazionali (ISA Italia), che consentono al revisore di formarsi un giudizio in merito al fatto che il bilancio, con una ragionevole sicurezza, nel suo complesso non contenga errori significativi, dovuti a frodi o eventi non intenzionali.

Ai sensi dell’art. 3, D.Lgs. 175/2016, nelle società per azioni a controllo pubblico la revisione legale dei conti non può essere affidata al Collegio sindacale: Lepida affida pertanto tale attività ad un Revisore legale o ad una Società di Revisione in conformità alle disposizioni del Codice civile, del Decreto Legislativo 39/2010 e dell’art. 15 (*Collegio sindacale*) dello Statuto sociale, a mente del quale *“la Revisione Legale dei Conti viene affidata ad un Revisore legale*



dei conti oppure ad una Società di Revisione, iscritti nell'apposito Registro, nominati dall'Assemblea Ordinaria su proposta motivata del Collegio Sindacale, e funzionanti ai sensi di legge" (comma 4).

Procedura per la gestione delle risorse umane

La Procedura si pone l'obiettivo di descrivere alcuni processi cruciali per l'andamento della Società e, più in particolare: (1) Selezione del personale; (2) Formazione del personale; (3) Progressioni e incentivi del personale; (4) Gestione presenze, missioni e trasferte del personale; (5) Gestione presenze e turni di lavoro del personale in specifici servizi; e (6) Preparazione buste paga e pagamento stipendi del personale. Per ciascuno dei processi in questione si indica il responsabile dello stesso, si traccia diagramma a blocchi e una procedura descrittiva dei processi, si definiscono, infine, gli indicatori di processo.

Procedura gestione Ciclo Passivo

Il documento ha l'obiettivo di descrivere - in conformità al vigente Codice dei Contratti Pubblici e in coerenza con le Norme di Trasparenza di Gestione di Lepida - le procedure di (1) *acquisizione di beni, servizi e lavori*; (2) *esecuzione ed elaborazione degli ordini di acquisto*; e (3) *controllo dell'esecuzione delle forniture e liquidazione*, definendo le responsabilità dei diversi attori coinvolti.

4.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.

Nel presente Modello si prevede comunque un flusso comunicativo - mediante incontro con cadenza almeno annuale - tra OdV e soggetti che svolgono controlli e vigilanza quali la Società di Revisione Legale dei Conti incaricata e il Collegio sindacale.



5. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25-septies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§4.5](#), si è evidenziato quanto segue.

5.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

5.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§4.4.5](#)), sono state le seguenti fattispecie:

<p>Art. 25 septies - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro</p>	<ul style="list-style-type: none"> - Omicidio colposo (art. 589 c.p.) commesso con violazione dell'art. 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro; - Omicidio colposo (art. 589 c.p.) commesso con violazione delle norme in materia di tutela della salute e sicurezza sul lavoro; - Lesioni personali gravi (art. 590, co.3, c.p.) commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro.
---	--

5.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. Gestione dei servizi, infrastrutture, livelli di servizio.

Articolazioni interne coinvolte

- D0 - Direzione Generale



- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione sicurezza, Ambiente & Emergenza
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

5.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo “di primo grado” non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di comportamento di Lepida

Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO 37001

Certificazione ISO 45001

Certificazione ISO 45001

Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo “di primo grado” non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 25 septies - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro</p>	<ul style="list-style-type: none"> - Omicidio colposo (art. 589 c.p.) commesso con violazione dell'art. 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro; - Omicidio colposo (art. 589 c.p.) commesso con violazione delle norme in materia di tutela della salute e sicurezza sul lavoro; - Lesioni personali gravi (art. 590, co.3, c.p.)
--	--



	<p>commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro.</p>
--	--

5.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo "di primo grado" non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

5.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- D.** gestione dei servizi, infrastrutture, livelli di servizio.

5.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Documento di Valutazione del Rischio di cui al D.Lgs. 81/2008

L'approvazione e l'aggiornamento del Documento di valutazione del rischio, redatto ai sensi degli artt. 17 e 28, D.Lgs. 81/2008, ha lo scopo di effettuare e tenere monitorata e documentata la valutazione globale di tutti i rischi per la salute e la sicurezza dei lavoratori nell'ambito dell'organizzazione in cui essi prestano la propria attività, al fine di individuare le adeguate misure di prevenzione e protezione e di elaborare il programma di attuazione delle stesse, atto a garantire il miglioramento nel tempo dei livelli di salute e di sicurezza.

Documento di Valutazione del Rischio Biologico

Si tratta di una integrazione del DVR aziendale, riguardante la valutazione del rischio biologico da SARS-CoV-2, la cui redazione è avvenuta facendo riferimento, in particolare, al "Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro" del 14/03/2020, sottoscritto su invito del Presidente del Consiglio dei ministri, del Ministro dell'economia, del Ministro del lavoro e delle politiche sociali, del Ministro dello sviluppo economico e del Ministro della salute all'articolo 1, comma



primo, numero 9), del decreto del DPCM 11 marzo 2020; nonché del successivo Protocollo Condiviso riportato nell'Allegato 6 del DPCM 24/04/2020.

Documento di Valutazione del Rischio da Stress Lavoro-correlato

Si tratta di una integrazione al DVR aziendale, il cui scopo è ottenere una valutazione del rischio da stress lavoro correlato elaborata da Lepida. La relazione, tra le altre cose, tiene conto della distinzione tra *eustress* - ovvero lo stress positivo, che rende più capaci di adattarsi positivamente alle situazioni - e *distress* - all'opposto, una tipologia di stress negativa, in cui la capacità di adattamento richiesta è maggiore di quella effettivamente posseduta dal soggetto interessato, con conseguenze negative di tipo comportamentale e psicologico.

Documento di Valutazione del Rischio Microclima

Si tratta di una integrazione al DVR aziendale, relativa alle condizioni climatiche ambientali presenti all'interno di un locale (stanza 22) sito nella sede di Via Borgo di San Pietro a Bologna, in quanto lo stesso è stato oggetto di un recente cambio di destinazione d'uso volto al posizionamento, al suo interno, di postazioni di call center (e dotato di un impianto di ricambio d'aria dimensionato sull'indice di affollamento previsto).

Documento di Valutazione del Rischio di Esposizione per inalazione a agenti chimici

Si tratta di una integrazione al DVR aziendale eseguita in seguito alla rilevazione della presenza di polveri nei magazzini di Minerbio e Quarto. Sono state fatte misurazioni specifiche nei suddetti magazzini al fine di valutare il livello di esposizione a prodotti chimici aerodispersi (polveri) a cui potrebbero risultare esposti gli addetti al magazzino durante le ordinarie attività.

Documento di Valutazione del Rischio - Datacenter Modena

Si tratta di un DVR specifico della sede aziendale, relativa alle attività svolte dal personale di Lepida presso il Datacenter di Modena, attività che peraltro non prevedono la presenza quotidiana di persone in loco, ma esclusivamente presenze occasionali riconducibili ad interventi di assistenza e/o programmazioni degli apparati presenti.

Documento di Valutazione del Rischio - Datacenter Ravenna

Si tratta di un DVR specifico della sede aziendale, relativa alle attività svolte dal personale di Lepida presso il Datacenter di Ravenna, attività che peraltro non prevedono la presenza quotidiana di persone in loco, ma esclusivamente presenze occasionali riconducibili ad interventi di assistenza e/o programmazioni degli apparati presenti.

Documento di Valutazione del Rischio - Datacenter Parma

Si tratta di un DVR specifico della sede aziendale, relativa alle attività svolte dal personale di Lepida presso il Datacenter di Parma, attività che peraltro non prevedono la presenza quotidiana di persone in loco, ma esclusivamente presenze occasionali riconducibili ad interventi di assistenza e/o programmazioni degli apparati presenti.

Documento di Valutazione del Rischio - Datacenter e sede di Ferrara

Si tratta di un DVR specifico della sede aziendale, relativa alle attività svolte dal personale di Lepida presso il Datacenter di Ferrara, attività che peraltro non prevedono la presenza quotidiana di persone in loco, ma esclusivamente presenze occasionali riconducibili ad



interventi di assistenza e/o programmazioni degli apparati presenti. Inoltre vi sono due locali ad uso ufficio per alcune attività amministrative di call center svolte da Lepida S.c.p.A. a favore della committente Azienda USL di Ferrara. A fronte di ciò si è valutato opportuno effettuare una VALUTAZIONE DEL RISCHIO DA ESPOSIZIONE A CAMPI ELETTROMAGNETICI

Organigramma aziendale per la sicurezza sui luoghi di lavoro 2024

Quale allegato al proprio DVR, Lepida ha adottato un Organigramma aziendale per la sicurezza sui luoghi di lavoro, per permettere di individuare le figure che, ai vari livelli, sono funzionalmente coinvolte secondo le disposizioni di cui al D.Lgs. 81/2008.

5.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.



6. Reati relativi al riciclaggio di denaro e all'autoriciclaggio (art. 25-octies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

6.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

6.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 25 octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio</p>	<ul style="list-style-type: none"> - Ricettazione (648 c.p.); - Riciclaggio (648 bis c.p.); - Impiego di denaro, beni o utilità di provenienza illecita (648 ter c.p.); - Autoriciclaggio (648 ter.1 c.p.).
---	---

6.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. Gestione dei servizi, infrastrutture, livelli di servizio.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna



6.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo *“di primo grado”* non accettabile (FASE 1 - **punto 3**)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

- Codice Etico e di Comportamento Lepida**
- Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)**
- Certificazione ISO 9001**
- Certificazione ISO 37001**
- Certificazione ISO/IEC 27001**
- Regolamento [015] Gestione Firme**
- Vademecum [022] Conflitto di Interessi**

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo *“di primo grado”* non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residuare alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 25 octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio</p>	<p>Nessuno</p>
---	----------------

6.2 Controlli periferici e attività in cui residua un maggior rischio concreto (**FASE 2**)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo *“di secondo grado”* questa volta ACCETTABILE.

6.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - **punto 1**)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:



A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. gestione dei servizi, infrastrutture, livelli di servizio.

6.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Nessuno

6.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, sia pure esclusivamente a livello centrale, non residuano reati con rischio residuo non accettabile.

7. Reati in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1 del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

7.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

6.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 25 octies.1 - Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori</p>	<ul style="list-style-type: none"> - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (493 ter c.p.); - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (493 quater c.p.); - Frode informatica, nell'ipotesi aggravata dalla realizzazione di un trasferimento di
--	--



	<p>denaro, di valore monetario o di valuta virtuale (640ter c.p.);</p> <ul style="list-style-type: none"> - Ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti; - Trasferimento fraudolento di valori (512 bis c.p.).
--	---

7.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

D. gestione dei servizi, infrastrutture, livelli di servizio;

E. gestione della rendicontazione amministrativa verso gli Enti Soci;

F. bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;

I. acquisto e utilizzo di valori di bollo.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- PX - Progetto CUP Unico Regionale
- PY - Progetto Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

7.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO 37001



Certificazione ISO/IEC 27001
Certificazione ISO/IEC 27001
Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 – Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo “di primo grado” non accettabile

Nonostante l’applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

Art. 25 octies.1 - Delitti in materia di strumenti di pagamento diversi dai contanti	Nessuno
--	---------

7.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell’Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d’esame, in particolare, è stata l’efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo “di secondo grado” questa volta ACCETTABILE.

7.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 – punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- E.** gestione della rendicontazione amministrativa verso gli Enti Soci;
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, soci, società di revisione, modalità formazione del capitale sociale.

7.2.2 Controlli societari periferici (FASE 2 – punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Norme di Trasparenza di gestione Lepida

Le Norme di Trasparenza e di Gestione di Lepida costituiscono uno dei documenti fondamentali per l’attività della Società. Il Regolamento è idealmente suddiviso in una *prima sezione* afferente alle Procedure di Acquisto, in una *seconda* relativa agli Incentivi ai Direttori, in una *terza* relativa alle Procedure Assunzioni e in una *quarta* relativa al Conferimento di incarichi professionali per servizi legali.



Il Regolamento ha il taglio di un documento esplicativo rivolto all'esterno e illustra le modalità e le regole con le quali Lepida ha scelto di autovincolarsi, dando applicazione al Codice dei Contratti Pubblici (D Lgs. 36 / 2023). I principali riferimenti sono, pertanto, a: Procedura per acquisti di modico valore, per importi non superiori a 1.000 euro; Procedura di Verifica Unicità; Affidamento diretto senza consultazione di operatori economici fino a 5.000 euro; Affidamento diretto previa consultazione di operatori economici mediante procedura con Richiesta di preventivi per importi inferiori a 140.000,00 per servizi e forniture e per importi inferiori a 150.000,00 per lavori ; Procedura sotto soglia comunitaria con Richiesta di Offerta; Procedure sopra soglia comunitaria; e, infine, per le Sponsorizzazioni .

La sezione relativa alle Procedure di assunzione ha invece lo scopo di dotare Lepida di procedure volte a disciplinare il processo di ricerca e selezione del personale per assunzioni con rapporto di lavoro subordinato a tempo indeterminato, in attuazione e in conformità all'art 19 del D.Lgs. 175/2016, nel rispetto dei principi indicati dall'art. 35.3 del D.Lgs. 165/2001.

Infine, il Regolamento delinea anche l'affidamento di incarichi di patrocinio legale - intesi come incarichi di assistenza, difesa e rappresentanza in giudizio conferiti da Lepida in occasione di ogni singola vertenza - a professionisti esterni e le principali condizioni giuridiche ed economiche del relativo incarico di patrocinio legale, nel rispetto dei principi di cui agli artt. 1, 2 e 3 del D.Lgs. 36 / 2023.

Regolamento [012] Forniture & Mandati

Il Regolamento disciplina l'iter procedimentale interno relativo alle procedure di acquisizione. Il documento scandisce le fasi procedurali, le competenze dei singoli soggetti e individua i soggetti titolari dei poteri autorizzativi indispensabili all'avvio della procedura.

Condizioni generali di contratto di Lepida

Il documento disciplina le Condizioni generali di contratto che regolano i rapporti contrattuali tra Lepida e gli aggiudicatari contraenti. Oltre all'esatta osservanza delle condizioni stabilite nel contratto di appalto, come definito all'art. 1 "Definizioni", lettera e), con la presentazione dell'offerta, il Partecipante accetta incondizionatamente quanto disciplinato nelle Condizioni generali di contratto di Lepida e quanto indicato nei documenti riferiti alla specifica procedura di acquisto.

Procedura Gestione del Ciclo attivo

La procedura descrive i processi di elaborazione delle offerte, dei contratti e degli ordini di vendita, di controllo della fase dell'esecuzione dei contratti e degli ordini di vendita e fatturazione, definendo le responsabilità degli attori del processo.

Procedura Gestione del Ciclo passivo

Il documento ha l'obiettivo di descrivere - in conformità al vigente Codice dei Contratti Pubblici e in coerenza con le Norme di Trasparenza di Gestione di Lepida - le procedure di (1) *acquisizione di beni, servizi e lavori*; (2) *esecuzione ed elaborazione degli ordini di acquisto*; e (3) *controllo dell'esecuzione delle forniture e liquidazione*, definendo le responsabilità dei diversi attori coinvolti.



Fatturazione elettronica, Conservazione sostitutiva, Regime IVA dello Split Payment e accreditamento IPA.

In qualità di società in house providing, Lepida può ricevere e accettare solo fatture in applicazione del regime dello Split Payment di cui all'art. 17-ter, D.P.R. 633/1972, salvo le previsioni applicabili a casi specifici quali Reverse Charge etc...

A partire dal 01.01.2019, ai sensi dell'art. 1, co. 909, Lepida riceve ed emette fatture unicamente in formato elettronico. I documenti fiscali sono ricevuti mediante intermediario NoTI-ER Intercent-ER e inviati in conservazione sostitutiva al ParER. Sempre dallo stesso momento, ai sensi dell'art. 1, co. 916 e 917, L. 205/2017 - come declinata nella Circolare AE n. 8 del 30/04/18 - Lepida non può procedere al pagamento di fatture elettroniche che non riportino i codici CIG e/o CUP di riferimento.

Da ultimo, a partire dal 15/09/2020, Lepida è accreditata nell'Indice dei Domicili digitali della Pubblica Amministrazione e Gestori dei Pubblici Servizi (IPA), con la conseguente attribuzione di un Codice Univoco Ufficio.

Sistema PayER

Payer è la piattaforma per i pagamenti on-line verso gli Enti pubblici realizzata da Lepida per gli Enti Soci. PayER garantisce il riversamento dei pagamenti sul conto corrente della Banca Tesoriera dell'Ente avvalendosi del protocollo PagoPA. La piattaforma viene messa a disposizione dei cittadini e imprese su mandato dell'ente creditore.

7.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, sia pure esclusivamente a livello centrale, non residuano reati con rischio residuo non accettabile.

8. Reati in materia di violazione del diritto d'autore (art. 25-novies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

8.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

8.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

Art. 25 novies- Delitti in materia di violazione	- Delitti in materia di violazione del diritto
--	--



del diritto d'autore	d'autore di cui agli artt: (171, co. 1, lett. a) bis e co. 3, L.633/1941); (171 bis L.633/1941); (171 ter L.633/1941); (171 septies L.633/1941); (171 octies L.633/1941);
----------------------	---

8.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. gestione dei servizi, infrastrutture, livelli di servizio.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto Cup Unico Regionale
- PY - Big Data HPC Margherita
- PZ - Progetto Digital Innovation Hub

8.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla società.

Codice Etico Lepida

Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione 37001

Certificazione ISO/IEC 27001

Regolamento [015] Gestione Firme



(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 – Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo “di primo grado” non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 25 novies- Delitti in materia di violazione del diritto d'autore</p>	<p>- Delitti in materia di violazione del diritto d'autore di cui agli artt: (171, co. 1, lett. a) bis e co. 3, L.633/1941); (171 bis L.633/1941); (171 ter L.633/1941); (171 septies L.633/1941); (171 octies L.633/1941);</p>
---	---

8.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo “di primo grado” non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo “di secondo grado” questa volta ACCETTABILE.

8.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. gestione dei servizi, infrastrutture, livelli di servizio.

8.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Regolamento [005] Sistemi di Comunicazione & Informativi

Tra le altre cose, il Regolamento specifica che sui dispositivi Lepida possono essere utilizzati solo i programmi espressamente autorizzati: l'utente è tenuto a non installare e/o utilizzare programmi senza autorizzazione.

Oltre a ciò, il punto 24 del Regolamento specifica che “Ciascun dipendente o collaboratore, indipendentemente dal fatto che utilizzi un dispositivo proprio o di Lepida, è comunque



responsabile del rispetto di tutte le norme vigenti sul copyright, sulla proprietà intellettuale e relative ai delitti informatici e risponde personalmente per quanto è presente sul proprio dispositivo e quanto provocato dall'accesso alla rete con le proprie credenziali".

Controlli relativi a LepidaTV

LepidaTV rappresenta un progetto condiviso da Giunta e Assemblea legislativa regionali, con la possibilità di ospitare contenuti informativi realizzati dall'Agenzia di Informazione e Comunicazione della Giunta e dal Servizio informazione e comunicazione istituzionale dell'Assemblea legislativa. La linea editoriale di LepidaTV viene definita nell'ambito del Comitato editoriale istituito nel 2020. Gli indirizzi di LepidaTV nel breve e medio periodo sono contenuti nel Piano di comunicazione della Regione Emilia-Romagna (per l'anno 2024, delibera di Giunta regionale n. 540 del 20/03/2024).

I contenuti video veicolati su LepidaTV vengono ceduti di regola a titolo gratuito, a tempo indeterminato non in esclusiva. Regione Emilia-Romagna si impegna ad acquisire le liberatorie necessarie dai soggetti aventi diritto e a fornire a Lepida contenuti video in ottemperanza a quanto previsto dalla normativa sul diritto d'autore.

8.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.

9. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

9.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

9.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 25 decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria</p>	<p>- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.);</p>
--	--



9.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B.** attività di selezione del personale e di mobilità interna;
- C.** gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- E.** gestione della rendicontazione amministrativa verso gli Enti Soci;
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- G.** gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto Cup Unico Regionale
- PY - Progetto HPC PA
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

9.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione 37001

Regolamento [015] Gestione Firme



Vademecum [022] Conflitto di Interessi

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo "di primo grado" non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

Art. 25 decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Nessuno
---	---------

9.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo "di primo grado" non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

9.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B. attività di selezione del personale e di mobilità interna
- C. gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D. gestione dei servizi, infrastrutture, livelli di servizio;
- E. gestione della rendicontazione amministrativa verso gli Enti Soci;
- F. bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- G. gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale.

9.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Nessuno



9.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, sia pure esclusivamente a livello centrale, non residuano reati con rischio residuo non accettabile.

10. Reati in materia ambientale (art. 25-undecies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui §4.5, si è evidenziato quanto segue.

10.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

10.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** (§4.4.5) sono state le seguenti fattispecie:

<p>Art. 25 undecies - Reati ambientali</p>	<ul style="list-style-type: none"> - Inquinamento ambientale (452 bis c.p.); - Disastro ambientale (452 quater c.p.); - Delitti colposi contro l'ambiente (452 quinquies c.p.); - Circostanze aggravanti (452 octies c.p.); - Traffico e abbandono di materiale ad alta radioattività (452 sexies c.p.); - Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (727 bis c.p.); - Distruzione o deterioramento di habitat all'interno di un sito protetto (733 bis c.p.); - Sanzioni penali (137, commi 3, 5, primo periodo, e 13, D.Lgs. 152/2006); - Sanzioni penali (137, commi 2, 5, secondo periodo, e 11, D.Lgs. 152/2006); - Attività di gestione di rifiuti non autorizzata (256, commi 1, lett. a), e 6 primo periodo, D.Lgs. 152/2006);
---	--



	<ul style="list-style-type: none"> - Attività di gestione di rifiuti non autorizzata (256, commi 1, lett. b), 3, primo periodo, e 5 D.Lgs. 152/2006); - Attività di gestione di rifiuti non autorizzata (256, comma 3, secondo periodo, D.Lgs. 152/2006); - Bonifica dei siti (257, commi 1 e 2, D.Lgs. 152/2006); - Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (258, co. 4, secondo periodo, D.Lgs. 152/2006); - Traffico illecito di rifiuti (259, co. 1, D.Lgs. 152/2006); - Attività organizzate per il traffico illecito di rifiuti (artt- 260, co. 1 e 2 D.Lgs. 152/2006, ora 452 quaterdecies c.p.); - Sistema informatico di controllo della tracciabilità dei rifiuti (260 bis, co. 6, 7 secondo e terzo periodo, 8 primo e secondo periodo, D.Lgs. 152/2006); - Sanzioni (279, co. 5, D.Lgs. 152/2006); - Art. 1, co. 1, L. 150/1992; - Art. 2, co. 1 e 2, L. 150/1992; - Art. 6, co. 4, L. 150/1992; - Art. 1, co. 2, L. 150/1992; - Fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996 (art. 3 bis, co. 1, L. n. 150/1992); - Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3, co. 6, L. 549/1993); - Inquinamento colposo (art. 9, co. 1, D Lgs. 202/2007); - Inquinamento doloso (art. 8, co. 1 e 9, co. 2, D Lgs. 202/2007); - Inquinamento doloso (art. 8, co. 2, D Lgs. 202/2007).
--	--

10.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività



A. Attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

D. Gestione dei servizi, infrastrutture, livelli di servizio;

M. Gestione rifiuti.

Articolazioni interne coinvolte

- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D8 - Divisione Azioni Strategiche & Speciali

10.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo *"di primo grado"* non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento Lepida

Piano Triennale Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 37001

Certificazione ISO 9001

Certificazione ISO 14001

Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo *"di primo grado"* non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

<p>Art. 25 undecies - Reati ambientali</p>	<ul style="list-style-type: none"> - Inquinamento ambientale (452 bis c.p.); - Disastro ambientale (452 quater c.p.); - Delitti colposi contro l'ambiente (452 quinquies c.p.); - Circostanze aggravanti (452 octies c.p.); - Sanzioni penali (137, commi 2, 5, secondo periodo, e 11, D.Lgs. 152/2006); - Attività organizzate per il traffico illecito di rifiuti (artt. 260, co. 1 e 2 D.Lgs. 152/2006, ora 452 quaterdecies c.p.).
---	--



10.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili, da un lato, e, dall'altro, ai reati a rischio residuo "di primo grado" non accettabile.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

10.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- M.** gestione rifiuti.

10.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Regolamento [018] Gestione rifiuti

Il Regolamento disciplina, nel rispetto della vigente normativa in materia ambientale, le procedure di gestione dei rifiuti prodotti da Lepida nello svolgimento delle proprie attività. Ciò, a prescindere che l'attività avvenga all'interno di una sede aziendale o all'esterno, come in sede di cantiere mobile. In linea di principio, ogni dipendente della Società è tenuto al rispetto della normativa ambientale in materia di gestione dei rifiuti e degli obblighi in materia di raccolta differenziata, nonché, ove chiamato in relazione alla propria attività, al rispetto delle specifiche istruzioni operative per la gestione dei rifiuti speciali pericolosi e non pericolosi.

Con riferimento alle attività appaltate, si dispone che ove l'onere dello smaltimento sia posto in capo al soggetto affidatario di un determinato contratto, spetta comunque al Referente interno del contratto di Lepida assicurarsi che lo smaltimento avvenga nel rispetto di quanto previsto dalla normativa in materia ambientale.

10.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.



Si dà atto che nel corso del 2024 Lepida ha aggiornato il proprio **Regolamento [018] Gestione rifiuti** (Versione 5 del 26.03.2024), con particolare riferimento alla gestione dei rifiuti da cantiere e di altre tipologie di rifiuto gestite nell'ambito delle proprie attività, quale, tra le altre, la polvere assorbente per acido di batterie dei carrelli elevatori.

Lepida provvede ad adeguare tempestivamente le proprie attività agli eventuali nuovi adempimenti normativi in materia; in particolare, è in corso un aggiornamento delle proprie procedure al fine di conformarsi all'obbligo di iscrizione al portale del nuovo Registro Elettronico Nazionale della Tracciabilità dei Rifiuti (RENTRI), che consentirà la gestione informatizzata di formulari, registri carico/scarico e MUD.

I temi della sostenibilità ambientale e della corretta gestione delle risorse energetiche, da sempre al centro dell'attenzione della Società - che ha provveduto ad individuare per tale ambito una specifica collocazione organizzativa nel Dipartimento Sicurezza Ambiente & Emergenza - saranno compiutamente declinati nel Bilancio di sostenibilità a cui la Società sta già lavorando per l'annualità 2025, in conformità agli adempimenti prescritti dalla vigente normativa.



11. Reati tributari (art. 25–quinquiesdecies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§ 4.5](#), si è evidenziato quanto segue.

11.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

11.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 – punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§ 4.4.5](#)), sono state le seguenti fattispecie:

<p>Art. 25 quinquiesdecies – Reati tributari</p>	<ul style="list-style-type: none"> - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, co. 1, D.Lgs. 74/2000); - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, co 2-bis, D.Lgs. 74/2000); - Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 74/2000); - Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, co. 1, D.Lgs. 74/2000); - Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, co. 2-bis, D.Lgs. 74/2000); - Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 74/2000); - Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 74/2000).
--	---

11.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 – punto 2)

Macroattività

A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;

B. attività di selezione del personale e di mobilità interna;

C. gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;



- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- E.** gestione della rendicontazione amministrativa verso gli Enti Soci;
- F.** bilancio, gestione dei rapporti e dei flussi informativi con collegio sindacale, Soci, società di revisione, modalità formazione del capitale sociale;
- G.** gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;
- H.** gestione degli aspetti afferenti la sicurezza e l'igiene sul lavoro;
- I.** acquisto e utilizzo di valori di bollo;
- J.** gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale;
- K.** gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva);
- L.** gestione contenzioso legale;
- M.** gestione rifiuti.

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D3 - Dipartimento Software & Piattaforme
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D7 - Dipartimento Amministrazione Divisione Amministrativa
- D9 - Dipartimento Accesso
- D8 - Divisione Azioni Strategiche & Speciali
- DA - Divisione Sicurezza, Ambiente & Emergenza
- PX - Progetto Cup Unico Regionale
- PY - Progetto HPC PA
- PZ - Progetto Digital Innovation Hub Emilia-Romagna

11.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo *"di primo grado"* non accettabile (FASE 1 - **punto 3**)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla Società.

Codice Etico e di Comportamento e di Comportamento Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione 37001

Regolamento [015] Gestione Firme

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).



Reati a rischio residuo “di primo grado” non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

Art. 25 quinquiesdecies - Reati tributari	nessuno
---	---------

11.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo “di secondo grado” questa volta ACCETTABILE.

11.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- B.** attività di selezione del personale e di mobilità interna;
- C.** gestione delle attività di selezione dei fornitori e degli acquisti e partecipazione a bandi;
- D.** gestione dei servizi, infrastrutture, livelli di servizio;
- G.** gestione dei rapporti con soggetti pubblici in ambito amministrazione personale, previdenziale e fiscale;
- J.** gestione dei rapporti con soggetti pubblici in relazione al conseguimento di contributi destinati alla formazione del personale;
- K.** gestione dei rapporti con gli Enti pubblici nell'ambito dei contratti di servizio (attivazione di contratti, fatturazione attiva).

11.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

Norme di Trasparenza di gestione Lepida

Le Norme di Trasparenza e di Gestione di Lepida costituiscono uno dei documenti fondamentali per l'attività della Società. Il Regolamento è idealmente suddiviso in una *prima sezione* afferente alle Procedure di Acquisto, in una *seconda* relativa agli Incentivi ai Direttori, in una *terza* relativa alle Procedure Assunzioni e in una *quarta* relativa al Conferimento di incarichi professionali per servizi legali.



Il Regolamento ha il taglio di un documento esplicativo rivolto all'esterno e illustra le modalità e le regole con le quali Lepida ha scelto di autovincolarsi, dando applicazione al Codice dei Contratti Pubblici (D.Lgs. 36/2023). I principali riferimenti sono, pertanto, a: Procedura semplificata per acquisti di modico valore, per importi non superiori a 1.000 euro; Procedura di Verifica Unicità; Affidamento i Diretti fino a 5.000 euro diretto senza consultazione di operatori economici fino a 5.000 euro; Affidamento diretto previa consultazione di operatori economici mediante procedura con Richiesta di preventivi Affidamenti con Richiesta di Preventivo per importi inferiori a 140.000,00 per servizi e forniture e per importi inferiori a 150.000,00 per lavori ; Procedura sotto soglia comunitaria con Richiesta di Offerta; Procedure sopra soglia comunitaria Affidamenti con Richiesta di Offerta fino alle soglie europee; e, infine, per le Sponsorizzazioni.

La sezione relativa alle Procedure di assunzione ha invece lo scopo di dotare Lepida di procedure volte a disciplinare il processo di ricerca e selezione del personale per assunzioni con rapporto di lavoro subordinato a tempo indeterminato, in attuazione e in conformità all'art 19 del D.Lgs. 175/2016, nel rispetto dei principi indicati dall'art. 35.3 del D.Lgs. 165/2001.

Infine, il Regolamento delinea anche l'affidamento di incarichi di patrocinio legale - intesi come incarichi di assistenza, difesa e rappresentanza in giudizio conferiti da Lepida in occasione di ogni singola vertenza - a professionisti esterni e le principali condizioni giuridiche ed economiche del relativo incarico di patrocinio legale, nel rispetto dei principi di cui agli artt. 1, 2 e 3 del D.Lgs. 36/2023.

Regolamento [012] Forniture & Mandati

Il Regolamento disciplina l'iter procedimentale interno relativo alle procedure di acquisizione. Il documento scandisce le fasi procedurali, le competenze dei singoli soggetti e individua i soggetti titolari dei poteri autorizzativi indispensabili all'avvio della procedura.

Procedura Gestione del Ciclo attivo

La procedura descrive i processi di elaborazione delle offerte, dei contratti e degli ordini di vendita, di controllo della fase dell'esecuzione dei contratti e degli ordini di vendita e fatturazione, definendo le responsabilità degli attori del processo.

Procedura Gestione del Ciclo passivo

Il documento ha l'obiettivo di descrivere - in conformità al vigente Codice dei Contratti Pubblici e in coerenza con le Norme di Trasparenza di Gestione di Lepida - le procedure di (1) *acquisizione di beni, servizi e lavori*; (2) *esecuzione ed elaborazione degli ordini di acquisto*; e (3) *controllo dell'esecuzione delle forniture e liquidazione*, definendo le responsabilità dei diversi attori coinvolti.

Fatturazione elettronica, Conservazione sostitutiva, Regime IVA dello Split Payment e accreditamento IPA

In qualità di società in house providing, Lepida può ricevere e accettare solo fatture in applicazione del regime dello Split Payment di cui all'art. 17-ter, D.P.R. 633/1972, salvo le previsioni applicabili a casi specifici quali Reverse Charge etc...

A partire dal 01.01.2019, ai sensi dell'art. 1, co. 909, Lepida riceve ed emette fatture unicamente in formato elettronico. I documenti fiscali sono ricevuti mediante intermediario NoTI-ER Intercent-ER e inviati in conservazione sostitutiva al ParER. Sempre dallo stesso momento, ai



sensi dell'art. 1, co. 916 e 917, L. 205/2017 - come declinata nella Circolare AE n. 8 del 30/04/18 - Lepida non può procedere al pagamento di fatture elettroniche che non riportino i codici CIG e/o CUP di riferimento.

Da ultimo, a partire dal 15/09/2020, Lepida è accreditata nell'Indice dei Domicili digitali della Pubblica Amministrazione e Gestori dei Pubblici Servizi (IPA), con la conseguente attribuzione di un Codice Univoco Ufficio.

Fatturazione nei confronti dei Soci - Regime di esenzione IVA ex art. 10, co. 2, DpR 633/1972

Lepida, in qualità di Società Consortile per Azioni - anche a seguito di Interpello all'Agenzia delle Entrate n. 909-844/2017 - può procedere a determinate condizioni a fatturare ai propri Enti Soci, che possiedono i requisiti soggettivi previsti, in regime di esenzione IVA, ai sensi dell'art. 10, co. 2 del D.P.R. 633/72, come modificato dall'art. 9, D.L. 83/2012.

Il regime di esenzione è applicabile qualora, come nel caso di Lepida, almeno il 50% del volume di affari sia svolto nei confronti di Soci che abbiano, come media del triennio precedente, un rapporto tra operazioni IVA imponibili e operazioni totali (tra cui anche le esenti o le escluse) non superiore al 10%.

Il singolo Socio, per usufruire del regime di esenzione, deve: (1) aver registrato, come media del triennio precedente, un rapporto tra operazioni IVA imponibili e operazioni totali (imponibili, esenti ed escluse) non superiore al 10% (requisito soggettivo); (2) fare espressa richiesta di applicazione del regime esentativo di cui all'art. 10, co. 2; (3) inviare annualmente a Lepida una attestazione riguardante il possesso del requisito soggettivo sul triennio precedente.

Protocollo elettronico aziendale

Tutte le comunicazioni e i contratti trasmessi o ricevuti da Lepida vengono registrati nel Protocollo elettronico aziendale, che attribuisce un numero progressivo di protocollazione, al fine di consentirne la tracciabilità.

Revisione Legale dei Conti

Per revisione legale si intende la revisione dei bilanci di esercizio o dei bilanci consolidati effettuata in conformità alle disposizioni del Codice civile e del D.Lgs. 39/2010 (art. 1, D.Lgs. 39/2010); si tratta, in altre parole, di un processo complesso di verifiche e procedure svolte, dai revisori persone fisiche e società di revisione iscritti ad uno specifico registro, in conformità ai principi di revisione internazionali (ISA Italia), che consentono al revisore di formarsi un giudizio in merito al fatto che il bilancio, con una ragionevole sicurezza, nel suo complesso non contenga errori significativi, dovuti a frodi o eventi non intenzionali.

Ai sensi dell'art. 3, D.Lgs. 175/2016, nelle società per azioni a controllo pubblico la revisione legale dei conti non può essere affidata al Collegio sindacale: Lepida affida pertanto tale attività ad un Revisore legale o ad una Società di Revisione in conformità alle disposizioni del Codice civile, del D.Lgs. 39/2010 e dell'art. 15 (*Collegio sindacale*) dello Statuto sociale, a mente del quale *"la Revisione Legale dei Conti viene affidata ad un Revisore legale dei conti oppure ad una Società di Revisione, iscritti nell'apposito Registro, nominati dall'Assemblea Ordinaria su proposta motivata del Collegio Sindacale, e funzionanti ai sensi di legge"* (comma 4).

Condizioni generali di contratto di Lepida

Il documento disciplina le Condizioni generali di contratto che regolano i rapporti contrattuali tra Lepida e gli aggiudicatari contraenti. Oltre all'esatta osservanza delle condizioni stabilite nel



contratto di appalto, come definito all'art. 1 "Definizioni", lettera e), con la presentazione dell'offerta, il Partecipante accetta incondizionatamente quanto disciplinato nelle Condizioni generali di contratto di Lepida e quanto indicato nei documenti riferiti alla specifica procedura di acquisto.

11.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.

12. Reati contro il patrimonio culturale (artt. 25-septies decies e 25-duodevicies del Decreto)

Con riferimento alla presente Categoria di illeciti di cui al Decreto, in esito all'Analisi dei rischi di cui [§4.5](#), si è evidenziato quanto segue.

12.1 Valutazione di accettabilità del rischio reato, a fronte degli strumenti di controllo predisposti a livello societario centrale (FASE 1)

12.1.1 Determinazione dell'indice di gravità dei reati (FASE 1 - punto 1)

Oggetto della valutazione di **Rischio potenziale** ([§4.4.5](#)) sono state le seguenti fattispecie:

<p>Art. 25-septiesdecies</p>	<ul style="list-style-type: none"> - Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.); - Appropriazione indebita di beni culturali (art. 518-ter c.p.); - Uscita o esportazione illecite di beni culturali (art. 518-undecies); - Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies); - Contraffazione di opere d'arte (art. 518-quaterdecies); - Furto di beni culturali (art. 518-bis); - Ricettazione di beni culturali (art. 518-quater).
-------------------------------------	--



Art. 25-duodevices	- Devastazione e saccheggio di beni culturali e paesaggistici (art.518-terdecies del codice penale);
--------------------	--

12.1.2 Identificazione delle Macroattività e articolazioni interne coinvolte (FASE 1 - punto 2)

Macroattività

A. attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti

D. gestione dei servizi, infrastrutture, livelli di servizio

M. gestione rifiuti

Articolazioni interne coinvolte

- D0 - Direzione Generale
- D1 - Dipartimento Reti
- D2 - Dipartimento Datacenter & Cloud
- D4 - Dipartimento Welfare & Integrazioni Digitali
- D8 - Divisione Azioni Strategiche & Speciali

12.1.3 Misure di riduzione del rischio applicate a livello societario centrale e individuazione dei reati a rischio residuo "di primo grado" non accettabile (FASE 1 - punto 3)

Misure di riduzione del rischio

Si sono ritenuti applicabili i seguenti strumenti di organizzazione e controllo predisposti a livello centrale dalla società.

Codice Etico e di Comportamento Lepida

Piano Triennale di Prevenzione della Corruzione e della Trasparenza (P.T.P.C.T.)

Certificazione ISO 9001

Certificazione ISO 37001

(Si vedano le descrizioni di cui alla Sezione di Parte Speciale n. 1 - Reati nei rapporti con la Pubblica Amministrazione).

Reati a rischio residuo "di primo grado" non accettabile

Nonostante l'applicazione degli strumenti di controllo di carattere generale, si sono ritenute residue alcune fattispecie connotate da un rischio reato ancora non accettabile.

Art. 25-septiesdecies	Nessuno
Art. 25-duodevices	Nessuno



12.2 Controlli periferici e attività in cui residua un maggior rischio concreto (FASE 2)

Obiettivo di questa fase dell'Analisi, come riferito nel nel [§ 4.5.1](#), è una verifica di secondo grado con specifico riferimento alle Macroattività ritenute particolarmente sensibili.

Oggetto d'esame, in particolare, è stata l'efficacia degli strumenti di controllo periferici/specialistici predisposti dalla Società al fine di ottenere un rischio residuo "di secondo grado" questa volta ACCETTABILE.

12.2.1 Individuazione delle Macroattività particolarmente sensibili (FASE 2 - punto 1)

Si sono ritenute di particolare rilievo - e, pertanto bisognose di specifiche cautele - in relazione alle fattispecie di reato in considerazione, le seguenti Macroattività:

- A.** attività di progettazione e realizzazione dei servizi, delle infrastrutture e gestione delle milestones contrattuali anche in riferimento all'innovazione e alle integrazioni digitali presso gli Enti;
- D.** gestione dei servizi, infrastrutture, livelli di servizio.

12.2.2 Controlli societari periferici (FASE 2 - punto 2)

Si sono ritenuti applicabili i seguenti, ulteriori, strumenti di organizzazione e controllo predisposti a livello periferico/speciale dalla Società.

PRO-SGQ-001 Procedura per la gestione delle attività operative del Dipartimento Reti

La procedura ha l'obiettivo di descrivere i principali processi adottati dalla Divisione:

- gestione delle iniziative;
- progettazione, realizzazione e attivazione di infrastrutture e servizi;
- gestione, manutenzione ed erogazione di infrastrutture e servizi.

Specifiche tecniche gare infrastrutture

Tali procedure definiscono le caratteristiche e le modalità operative per la fornitura e messa in opera delle reti di telecomunicazioni.

PRO-SGQ-004 Procedura per la gestione delle attività operative del Dipartimento Welfare & Integrazioni Digitali

La procedura delinea le varie fasi di processo relativamente ai progetti e alla gestione ed erogazione di servizi relativi alle integrazioni digitali rivolti alle Pubbliche Amministrazioni della regione Emilia-Romagna.

PRO-SGQ-008 Procedura per la gestione delle attività operative della Divisione Azioni Strategiche & Speciali

La procedura ha l'obiettivo di descrivere i principali processi adottati dall'Aggregato:

- gestione delle iniziative;
- esecuzione delle attività.



Regolamento [018] Gestione rifiuti

Il Regolamento disciplina, nel rispetto della vigente normativa in materia ambientale, le procedure di gestione dei rifiuti prodotti da Lepida nello svolgimento delle proprie attività. Ciò, a prescindere che l'attività avvenga all'interno di una sede aziendale o all'esterno, come in sede di cantiere mobile. In linea di principio, ogni dipendente della Società è tenuto al rispetto della normativa ambientale in materia di gestione dei rifiuti e degli obblighi in materia di raccolta differenziata, nonché, ove chiamato in relazione alla propria attività, al rispetto delle specifiche istruzioni operative per la gestione dei rifiuti speciali pericolosi e non pericolosi.

Con riferimento alle attività appaltate, si dispone che ove l'onere dello smaltimento sia posto in capo al soggetto affidatario di un determinato contratto, spetta comunque al Referente interno del contratto di Lepida assicurarsi che lo smaltimento avvenga nel rispetto di quanto previsto dalla normativa in materia ambientale.

12.3 Illeciti con rischio residuo non accettabile e predisposizione di controlli specifici ed ulteriori (FASE 3)

Dai controlli adottati, tanto a livello centrale quanto a livello periferico, non residuano reati con rischio residuo classificabile come non accettabile.

13. Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater del Decreto)

Con riferimento all'art. 25 quater (*Delitti con finalità di terrorismo o di eversione dell'ordine democratico*) del Decreto, occorre precisare che Lepida - nonostante non consideri probabile il verificarsi di tale fattispecie di reato nel proprio interesse o vantaggio, condizione fondamentale per il sorgere di una responsabilità ai sensi dell'art. 5 del Decreto - ritiene comunque opportuno operare una riflessione in relazione alla possibilità che le reti informatiche e telematiche, al pari delle altre infrastrutture gestite dalla Società, possano rappresentare lo strumento adoperato per la commissione di simili illeciti.

In particolar modo, l'attenzione sul punto deriva dall'emanazione dei seguenti corpi normativi:

1. [Direttiva \(UE\) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento \(UE\) n. 910/2014 e della direttiva \(UE\) 2018/1972 e che abroga la direttiva \(UE\) 2016/1148 \(direttiva NIS 2\)](#), cui il Legislatore italiano ha dato attuazione con il Decreto legislativo 4 settembre 2024, n.138. ;



2. [Legge 28 giugno 2024 n. 90 recante Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.](#)

In materia, comunque, è opportuno segnalare che la società si è dotata di un Sistema di Gestione per la Sicurezza delle Informazioni certificato secondo le norme ISO/IEC 27001, 27017 e 27018.



14. Appendice

La gestione delle procedure finanziate con fondi PNRR

Il coinvolgimento di Lepida nella gestione dei bandi afferenti il Piano Nazionale di Ripresa e Resilienza - [PNRR](#) si è concretizzato, in particolare, nel corso dell'anno 2023 e proseguito anche per l'anno 2024. Lepida, quale società in house providing di Regione Emilia-Romagna e di altri Enti pubblici regionali, è chiamata ad operare principalmente come supporto tecnico-operativo - ai sensi degli artt. 9, co. 2 e 10 del dl 77/2021 e s.m.i. - nel percorso di trasformazione digitale, finanziato con fondi PNRR, che vede negli Enti Soci i soggetti attuatori.

Lepida, inoltre, oltre ad operare direttamente come soggetto realizzatore affidatario di servizi da parte dell'Ente socio, può eventualmente esternalizzare parte delle attività ad operatori economici esterni, sempre in chiave strumentale e nell'interesse dell'Ente socio attuatore.

Relativamente al solo progetto Emilia-Romagna Ecosistema Regionale di Innovazione Digitale (ER2Digit European Digital Innovation Hub (EDIH) della Regione Emilia-Romagna) Lepida collabora, quale soggetto attuatore, con ART-ER e CINECA per favorire il miglioramento dell'offerta di servizi pubblici e l'adozione di soluzioni digitali innovative nella Pubblica Amministrazione e nelle imprese.

Le ingenti risorse messe a disposizione attraverso il PNRR necessitano l'implementazione, per tutti gli Enti coinvolti, di un adeguato sistema di vigilanza affinché i flussi si muovano all'interno di un meccanismo di piena legalità, come già chiaramente indicato da ANAC nel PNA 2022, la quale ha auspicato una mappatura dei processi che coinvolgano la spendita di risorse pubbliche per il raggiungimento degli obiettivi del PNRR e dei fondi strutturali.

Relativamente alla Società, considerata la rilevanza dei progetti PNRR almeno sino al 2026, sono state introdotte azioni *ad hoc* volte a garantire sia l'adempimento degli obblighi di natura documentale e di rendicontazione, sia l'attuazione di misure di prevenzione e controllo dei flussi. Anche nel rispetto di quanto indicato all'art. 22 del Regolamento UE 241/2021, sono stati rafforzati i flussi informativi, anche mediante riunioni di coordinamento con i Soci stessi sull'avanzamento dei progetti PNRR di cui Lepida si è resa parte attrice e al contempo coordinatrice; sono state recepite le indicazioni di ANAC per il controllo degli affidamenti ai fornitori; sono rispettati gli obblighi di trasparenza con riferimento all'implementazione e all'aggiornamento della [sezione "Società Trasparente"](#), ove pubblicare gli atti amministrativi emanati per l'attuazione delle misure di competenza.

Come declinato nelle Linee Guida per lo svolgimento delle attività di controllo e rendicontazione degli interventi PNRR di competenza delle Amministrazioni centrali e dei Soggetti attuatori Vers. 1.0 (agosto 2022), ai fini della prevenzione dei rischi di infiltrazione criminale nell'impiego dei fondi PNRR, occorre valorizzare l'adempimento degli obblighi antiriciclaggio per consentire la tempestiva individuazione di eventuali sospetti di sviamento delle risorse rispetto all'obiettivo per cui sono state stanziare.

Lepida ha già nominato il proprio Responsabile antiriciclaggio ex art. 10, co. 4, D.Lgs. 231/2007 in forza di delibera D1221_33 del 15 dicembre 2021, quale soggetto chiamato a valutare e comunicare all'Unità di Informazione Finanziaria (UIF) le situazioni ritenute sospette, a rispondere ad eventuali richieste di approfondimento provenienti dalla stessa UIF, nonché a



dettare procedure interne funzionali al miglior funzionamento del modello organizzativo di contrasto al riciclaggio. La Società, inoltre, ha provveduto ad individuare il proprio Titolare effettivo, ai sensi dell'art. 20, comma 5 del d.Lgs. 231/2007, giusta delibera del Consiglio di Amministrazione n. D0523_28 del 16 maggio 2023.

La Società, inoltre, presidia l'acquisizione della documentazione amministrativa richiesta dalla normativa PNRR ai fornitori aggiudicatari delle procedure di affidamento (assenza conflitto di interessi, titolare effettivo, rispetto degli obblighi relativi alle Pari opportunità, generazionali e di genere, rispetto del principio Do No Significant Harm - DNSH) e, al contempo, cura essa stessa la produzione della documentazione in favore degli Enti Soci affidanti nell'ambito delle procedure PNRR.

Per quanto attiene ai presidi di natura procedurale, al momento si è ritenuto che l'attuale gestione dei flussi finanziari - così come proceduralizzata - non richieda implementazioni specifiche per le risorse finanziate con fondi PNRR, essendo considerate adeguate ed efficaci le attuali misure a presidio di eventuali condotte distorsive e illecite.

