# PARMAINFANZIA S.P.A.

Sede Legale in Parma (PR), Strada Budellungo n. 45/A

## MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

**Parte Speciale B**

**Delitti informatici e trattamento illecito dei dati**

**&**

**Delitti in materia di violazione del diritto d'autore**

ai sensi del art. 24-bis e 25-novies ex Decreto Legislativo 8 giugno 2001, n. 231
sulla "Responsabilità Amministrativa delle Imprese"

Il presente "Modello di organizzazione, gestione e controllo" (di seguito il "Modello") di ParmaInfanzia S.p.A. (di seguito la "Società" o "ParmaInfanzia") è stato redatto in attuazione dei dettami di cui agli artt. 6 e 7 del D. Lgs. 231 del 2001 e ss. mm. e ii. (di seguito il "Decreto").
Esso è stato adottato dalla Società con delibera del Consiglio di Amministrazione del 26 Marzo 2021 ed aggiornato in data 27/03/2024 e sarà efficacemente attuato attraverso la sua progressiva implementazione (ivi compresi gli adeguamenti che si renderanno necessari anche in conseguenza delle modifiche e novità legislative in merito) da parte del Consiglio di Amministrazione medesimo e dell'Organismo di Vigilanza.
Il "Modello" rappresenta il riferimento gestionale diretto, atto a costituire lo strumento predisposto ai fini della prevenzione degli illeciti penali previsti dal Decreto, in ossequio alla politica di etica aziendale adottata dalla Società.

**INDICE**

**PREMESSA**

La presente Parte Speciale è dedicata alla trattazione dei reati di natura informatica e alla violazione dei diritti d'autore.

Ai fini della trattazione complessiva, la presente Parte Speciale analizza le tipologie di condotta criminosa e le misure di prevenzione adottate da ParmaInfanzia S.p.A. sia in riferimento ai reati informatici che a quelli di violazione dei diritti d'autore.

In senso stretto sia i retai informatici e trattamento illecito dei dati (previsti dall'art. 24-bis del D. Lgs. 231/2001, inserito dalla L. 18/3/2008 n. 48 all'art. 7) sia i delitti in materia di violazione del diritto d'autore connessi alla sfera dell'utilizzo di strumenti informatici, (previsti dall'art. 25-novies del D. Lgs. 231/2001, aggiunto dalla L. 23 luglio 2009, n. 99 all'art. 15).

Di seguito viene riportato l'elenco delle fattispecie criminose prese in considerazione dalle disposizioni citate, le modalità attraverso le quali queste fattispecie criminose possono essere compiute nonché le "macro aree" sensibili, i ruoli aziendali coinvolti e i protocolli di prevenzione attuati all'interno della Società.

## 1. LA TIPOLOGIA DEI DELITTI TRATTATI

Per quanto riguarda la presente Parte Speciale, si riporta di seguito una breve descrizione dei reati contemplati negli sopra menzionati:

- art. 24-bis – Delitti informatici e trattamento illecito di dati:
  - Documenti informatici (art. 491-bis c.p.)
  - Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
  - Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
  - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]
  - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
  - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]
  - Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
  - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
  - Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
  - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
  - Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
  - Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

- Art. 25-novies – Delitti in materia di violazione del diritto d'autore:
  - Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
  - Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
  - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
  - Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
  - Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti

analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941) [modificato dalla L. n. 93/2023]

- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

L'art. 24-bis ex D. Lgs. 231/2001 cita quanto segue:
*1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*

*2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.*

*3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, ((e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105,)) si applica all'ente la sanzione pecuniaria sino a quattrocento quote.*

*4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).*

L'art. 25-novies ex D. Lgs. 231/2001:
*1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.*
*2. Nel caso di condanna per i delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941.*

I delitti in oggetto sono reati comuni dolosi realizzabili da "chiunque". Ai fini della configurabilità della responsabilità amministrativa dell'ente il soggetto agente deve ricoprire una delle posizioni individuate nell'art. 5:

- persona che riveste funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persona che esercita, anche di fatto, la gestione e il controllo dello stesso;
- persona sottoposta alla direzione o alla vigilanza di uno dei soggetti di cui alla lett. a).

Per documento informatico, in conformità a quanto previsto dall'art. 1 del D. Lgs. 82/2005 (c.d. "codice dell'amministrazione digitale"), si deve intendere " la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Per la configurabilità del reato di accesso abusivo ad un sistema informativo è necessario che lo stesso sia protetto da misure di sicurezza. Sotto questo profilo è sufficiente che il sistema sia dotato di una password per l'accesso.
Il reato è configurabile anche quando i codici di accesso siano utilizzati da un soggetto temporaneamente legittimato (es.: dipendente, socio) ma per finalità diverse da quelle consentite (es.: prelievo dell'archivio clienti per intraprendere un'attività concorrenziale). È evidente che ciò che interessa ai fini della responsabilità amministrativa degli enti, non è il reato commesso ai danni della società ma quello che potrebbe essere commesso nel!' interesse o a vantaggio della società.
Per quanto concerne il reato di danneggiamento di sistemi informatici è sufficiente creare un ostacolo al corretto funzionamento (es.: virus ma anche altre alterazioni o interventi che provochino anche solo un significativo rallentamento della sua funzionalità).
Infine, occorre segnalare che il reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche è configurabile esclusivamente in caso di comunicazioni in fase di trasmissione, atteso che la comunicazione in senso "statico" (per esempio l'e-mail già scaricata dal programma di posta elettronica) è tutelata penalmente dall'art. 616 c.p. in materia di segretezza della corrispondenza, che però non rileva per la responsabilità amministrativa degli enti.
Il reato di frode informatica si riferisce, secondo l'art 24-bis del D. Lgs. 231/2001, anche a parti lese diverse dalla Pubblica Amministrazione, (prevista dall'art. 24 del D. Lgs. 231/200 l). L'aggravante per utilizzo illecito di identità digitali è connessa a condotte illecite di accesso abusivo in generale.
Occorre considerare, nell'ottica della prevenzione del rischio della responsabilità ex D. Lgs. 231/2001, che la presenza di interesse o vantaggio dell'ente nel verificarsi del reato, implica che lo schema comportamentale illecito usualmente riguardi soggetti che utilizzano a benefico del nuovo ente di appartenenza informazioni di illecita provenienza da enti di appartenenza precedente, o comunque terzi.
Di impatto immediatamente non alto il rischio di responsabilità amministrativa derivante di uso illecito di carte di credito o debito nelle operazioni aziendali, visto che i possibili modelli di comportamento illecito, con vantaggio o interesse dell'ente, appaiono relativamente poco frequenti.
Di notevole rilevanza la responsabilità derivante dai reati presupposto, con caratteristica di delitto, relativi all'illecito trattamento dei dati ed alle comunicazioni, e notificazioni al Garante, nonché osservanza dei relativi provvedimenti.
In sintesi (la trattazione del "sistema privacy" richiede naturalmente diversa e più ampia esposizione) l'osservanza delle nonne del codice in materia di protezione dei dati personali, e la sua traduzione in adeguate componenti del modello organizzativo gestionale sono parte essenziale del sistema di prevenzione di reati presupposto e costituiscono la base per le garanzie esimenti la responsabilità dell'ente.

Occorre sottolineare che il delitto di trattamento illecito di dati (art. 167) è strutturato, sotto il profilo dell'elemento soggettivo, come reato a dolo specifico. Ciò significa che non tutte le violazione delle norme speciali richiamate nell'art. 167 rilevano sotto il profilo penale ma solo quelle commesse al fine di trarne per sé o per altri profitto o di recare ad altri un danno.
Il rischio relativo a delitti informatici riguarda le attività nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione. Le attività nelle quali è maggiore il rischio che siano posti in essere i comportamenti illeciti è la gestione e l'utilizzo dei sistemi informatici e delle informazioni aziendali (c.d. "patrimonio informativo") attraverso qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati.
Aggiornamento 2019 :

*Il Decreto Legge 2019 n. 105 ha introdotto nel nostro ordinamento giuridico un'altra ipotesi di reato presupposto, ex D.Lgs. 231/2001 introducendo il Perimetro di sicurezza nazionale cibernetica*
*In particolare la normativa prevede che "Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attivita' ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attivita' ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, e' punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote".*
*Per l'ampliamento dell'elenco dei reati presupposto in materia di sicurezza cybernetica e i dovuti chiarimenti sulla nuova normativa, si dovrà, attendere le indicazioni che saranno contenute nel decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), che sarà adottato entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto.*
*Il primo dei quattro DPCM attuativi del Perimetro di sicurezza nazionale cibernetica, per l'esattezza il Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, "Regolamento in materia di perimetro di sicurezza nazionale cibernetica".*
*Il provvedimento, entrato in vigore il 5 novembre 2020, definisce le regole del Perimetro nazionale di sicurezza cibernetica e stabilisce i parametri con cui sono individuati i soggetti che si occupano di funzioni vitali per l'Italia.*
I reati ai quali fa riferimento l'art. 25-novies sono reati comuni dolosi realizzabili da "chiunque" (anche se in taluni casi nell'ambito dell'esercizio di determinate attività) purché si trovi, rispetto all'ente, in una delle posizioni individuate nell'art. 5 e quindi:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lett. a).

L'ente non risponde se i soggetti sopra indicati hanno agito nell' interesse esclusivo proprio o di terzi.
I reati in esame sono contenuti dalla L. 633/41 (c.d. "legge sul diritto d'autore") e sono stati inseriti tra i reati presupposto ex D. Lgs. 231 dalla L. 99/2009.

La commissione delle fattispecie esaminate prevede per l'ente sanzioni pecuniarie che possono arrivare sino a 500 quote e sanzioni interdittive per la durata massima di un anno.

## 2. AREE DI ATTIVITÀ A RISCHIO RELATIVE ALL'ART. 24-bis

Le attività di rischio si possono vedere sotto una duplice prospettiva:

- secondo organigramma e funzionigramma;
- per processi e ambienti, secondo il tipo di reato.

Di seguito si andranno a schematizzare le aree di rischio suddivise come detto sopra.

### 2.1. Secondo organigramma e funzionigramma

In via generale aree a rischio sono identificabili tutte le aree:

a) in quanto riferite nel Modello organizzativo gestionale;
b) in quanto accedano ai sistemi IT aziendali;
c) in quanto coinvolte nel sistema privacy (norme, processi, dati, asset).

Nel dettaglio si possono configurare le seguenti aree di rischio:

- Corporate governance e direzione generale:
  - gestione documenti informatici;
  - gestione dati riservati;
  - gestione credenziali e certificati digitali.
- Amministrazione – legale – affari societari:
  - gestione documenti in formatici;
  - gestione dati riservati;
  - gestione credenziali e certificati digitali per comunicazioni a uffici pubblici.
- Finanza e controllo:
  - processi di pagamento, incasso e cash management in generale;
  - accesso a sistemi di banche e istituzioni finanziarie, e ai relativi fornitori di servizi telematici e di comunicazione.
- Commerciale e vendite:
  - accesso a sistemi di clienti e partner commerciali;
  - gestione documenti informatici.
- Ricerca e sviluppo:
  - accesso a sistemi esterni;
  - gestione documenti informatici;
  - gestione dati riservati;
  - gestione credenziali e certificati digitali.
- Risorse umane:
  - gestione dati riservati, sensibili.
- Approvvigionamento e acquisti:
  - accesso a sistemi di fornitori e partner commerciali;
  - gestione credenziali e certificati digitali per accesso a gare e processi di e-procurement;
  - gestione documenti informatici;
  - utilizzo di carte di credito e pagamento aziendali per processi di procurement.
- Produzione e logistica:
  - accesso a sistemi di fornitori, clienti e partner commerciali;
  - gestione credenziali e certificati digitali per comunicazioni a uffici pubblici.
- Sicurezza fisica:
  - presidio e protezione fisica infrastrutture ICT.

- Gestione dei sistemi informativi:
  - presidio e protezione logica sistemi IT;
  - gestione documenti informatici;
  - gestione credenziali di accesso ai sistemi IT interni, esterni;
  - gestione procedure assegnazione credenziali e certificati digitali.

**2.2. Per processi e ambienti, secondo il tipo di reato**

Di seguito si elencano le aree di rischio con particolare attenzione ai processi e all'ambiente aziendale ove i reati possono essere commessi:

- Falsità di documenti informatici (art. 491-bis):
  - Presenza di documenti in formatici nei processi:
    - dell'ente;
    - di enti esterni cui vi è prassi di accesso.
- Reati connessi all'accesso (art. 615-ter, art. 615-quater):
  - presenza di ambienti di accesso dall'esterno al sistema da parte di soggetti esterni all'organizzazione dell'ente (es. siti web informativi, di e-commerce; di consultazione ed interazione);
  - presenza di ambienti di accesso dall'esterno da parte di soggetti appartenenti all'organizzazione dell'ente (es. reti private virtuali, o "VPN", che consentono di accedere ai sistemi interni dell'ente);
  - prassi nei processi dell'ente di accesso a ambienti informatici e telematici interni;
  - prassi nei processi dell'ente di accesso a ambienti informatici e telematici esterni.
- Reati di intercettazione, interruzione, impedimento di comunicazioni (art. 611-quater, art. 611-quinquies):
  - i presupposti sono gli stessi dei reati di accesso
- Reati di danno a sistemi informatici e telematici in senso lato (art. 615-quinquies – virus informatici e simili, art. 635-bis, art.635-quater – danneggiamento a soggetti privati e art. 635-ter, art.635-quinquies – danneggiamento a soggetti pubblici o di pubblica utilità):
  - i presupposti sono gli stessi dei reati di accesso;
- Frode informatica:
  - Frode informatica (art. 640-ter):
    - i presupposti sono gli stessi dei reati di accesso;
    - in particolare occorre considerare l'aggravante dell'uso di identità digitali, possibile conseguenza dell'accesso abusivo.
  - Frode informatica del certificatore (art. 640-quinquies):
    - sussistenza dello status di ente certificatore inserito nell'elenco dei certificatori accreditati ai sensi del DPR 28.12.2000 n. 445 e successive modificazioni
      Il reato può essere commesso in concorso.
- Uso illecito di carte di credito o pagamento (art. 55 co. 9 del D. Lgs. 231/2007):
  - utilizzo di carte di credito o pagamento per operazioni aziendali di fornitura o regolamento in generale.
- Trattamento illecito dei dati:
  - Codice in materia di protezione dei dati personali (artt. 167- 172 del D. Lgs. 196/2003 e successive modificazioni):
    - l'intero "sistema privacy": sue norme interne, processi, misure protettive, controlli e procedura di gestione delle controversie e delle interazioni con il Garante.

## 3. AREE DI ATTIVITÀ A RISCHIO RELATIVE ALL'ART. 25-novies

I reati sopra considerati, relativi all'art. 25-novies, hanno come presupposto la violazione dei diritti di autore.

In via generale aree a rischio sono identificabili tutte le aree:

a) in quanto riferite nel Modello Organizzativo Gestionale;
b) in quanto in relazione diretta o indiretta, in ambito produttivo o commerciale, con i diritti di autore.

Di seguito sono indicate le aree aziendali a rischio reato in cui, in assenza di opportune misure e cautele procedimentali, può assumere particolare rilevanza il rischio di esporre la Società a responsabilità ai sensi del Decreto.

Nello specifico si possono configurare le seguenti aree:

- Area legale:
  - utilizzazione economica dell'opera:
    - rapporti contrattuali sottostanti concessioni di diritti di:
      - pubblicazione;
      - riproduzione;
      - trascrizione;
      - esecuzione, rappresentazione e recitazione in pubblico;
      - diffusione;
      - distribuzione;
      - traduzione, elaborazione, pubblicazione in raccolta;
      - noleggio o dazione in prestito;
      - modifica;
  - esistenza dei diritti /procedure adottate per ricerca "novità"/"anteriorità"
    - protezione dei diritti d'autore.
- Area finanziaria:
  - gestione dei flussi finanziari;
  - gestione dei fondi aziendali.
- Area ricerca & sviluppo:
  - tutela dei diritti d 'autore (propri);
  - uso di diritti d'autore (altrui);
  - adempimenti relativi a registrazione – pagamento diritti – SIAE.
- Area della comunicazione esterna:
  - gestione dei sistemi che rendono accessibile dall'esterno l'attività esercitata (e-commerce, siti web aziendali, etc.).
- Area della sicurezza informatica:
  Attività supportate da sistemi informatici e telematici per l'elaborazione, la conservazione e l'archiviazione di dati aziendali riservati.
  Canali multimediali che consentono la diffusione di opere protette da diritti d 'autore tramite sistemi informatici (brani musicali, e-book, podcasting, ecc.).
- Risorse umane:
  - attività relative alla ricerca, selezione, assunzione, formazione, gestione del Personale dipendente;
  - gestione delle risorse umane esterne (Agenti, rappresentanti, collaboratori).

## 4. DESTINATARI DELLA PARTE SPECIALE

La presente parte speciale si riferisce a comportamenti posti in essere dagli amministratori, dirigenti e dipendenti, "Esponenti Aziendali", di ParmaInfanzia S.p.A. nelle aree di attività a rischio sopra elencate, nonché dai Collaboratori esterni e Partner (qui di seguito tutti denominati "Destinatari parte speciale B").

Obiettivo della presente parte speciale è che tutti i Destinatari della parte speciale B come sopra individuati adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di impedire il verificarsi dei reati previsti nel Decreto.

## 5. PRINCIPI GENERALI DI COMPORTAMENTO

A tutti i destinatari è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato richiamate nella presente Parte Speciale;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente divenirlo.

Tutti gli operatori coinvolti nelle aree "a rischio reato" (par. 2 della presente Parte Speciale) sono tenuti, nell'ambito della propria attività, al rispetto dei principi di comportamento definiti sia dal Codice Etico adottato dalla Società (All. 1) che a quanto disposto da ulteriori documenti che verranno menzionati nel paragrafo 6 della presente Parte Speciale.

Sul piano generale si identificano:

- i trattamenti dei dati personali svolti all'interno della struttura;
- le competenze e le responsabilità delle strutture e del personale preposto al trattamento dei dati personali;
- le tipologie e la gravità dei rischi incombenti sul trattamento;
- le misure di sicurezza adottate per contrastare i rischi rilevati;
- i criteri e le procedure per il salvataggio ed il ripristino dei dati;
- la pianificazione degli interventi formativi in materia di trattamento dei dati;
- i trattamenti dei dati personali affidati a strutture esterne.

La predisposizione ed il mantenimento di un adeguato sistema di controllo interno, quale insieme di tutti gli strumenti necessari o utili a indirizzare, gestire e verificare le attività di impresa con l'obiettivo di assicurare il rispetto delle leggi e delle procedure aziendali, di proteggere i beni aziendali, di gestire in modo ottimale ed efficiente le attività, rappresenta la migliore risposta per la prevenzione dei rischi. Con specifico riguardo alle problematiche connesse al rischio informatico, in considerazione dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale, ParmaInfanzia ha definito un sistema di sicurezza atto ad evitare e dissuadere ogni genere di azione che possa minare la sicurezza informatica della struttura.

## 6. PROTOCOLLI SPECIFICI

### 6.1. Norme di comportamento per l'utilizzo degli strumenti informatici aziendali

Le norme di comportamento, da parte dei dipendenti e dei collaboratori di ParmaInfanzia, per l'utilizzo degli strumenti informatici messi a disposizione dalla Società, sono state determinate dal Disciplinare Tecnico e sono supportate da adeguato sistema sanzionatorio che, in applicazione delle procedure di legge e di contratto collettivo, permette di disporre la sospensione o l'esclusione dell'utente dall'uso delle risorse informatiche, applicando nei confronti del lavoratore che ha violato i propri doveri di diligenza, obbedienza e fedeltà, le sanzioni disciplinari commisurate alla gravità della infrazione.

Si rimanda a quanto detto nel disciplinare tecnico REV 00 Maggio 2018.

### 6.2. Sistema di autenticazione

È fondamentale proteggere dall'accesso illecito la propria postazione di lavoro, indipendentemente che sia un personal pc o notebook, mediante l'utilizzo di una o più password segrete e personali. Vi sono differenti categorie di password, ognuna con un proprio ruolo preciso:

- password di accesso al computer per impedire l'utilizzo improprio della vostra postazione;
- password di accesso alla rete per impedire l'accesso non autorizzato a una postazione che renda disponibili tutte le risorse dell'ufficio;
- password per programmi specifici per restringere l'accesso ai dati al solo personale autorizzato;
- password del salva schermo, per impedire che l'assenza temporanea dalla postazione permetta la visualizzazione del vostro lavoro a personale non autorizzato.

Alcune di queste password, per motivi tecnici, possono coincidere e comunque si richiede il medesimo comportamento diligente e la conservazione segreta di tali password.
Al fine della corretta applicazione delle misure minime di sicurezza richieste dalla normativa vigente, le password a protezione di unità che contengono dati sensibili (utenza e/o personale) devono essere cambiate ogni 3 mesi, negli altri casi almeno ogni sei mesi e comunque ogni volta che il lavoratore incaricato all'uso della strumentazione interrompe la propria attività (dimissioni, cambio di servizio, etc…).
Per proteggere i dati riservati dell'azienda, così come per evitare che i soci/dipendenti possano leggere la posta personale altrui, la soluzione richiesta, dalle "misure minime di sicurezza", è l'adozione di password di almeno 8 caratteri (alfanumerici) possibilmente comprendenti caratteri speciali o lettere accentate che ne rendono difficile la decriptazione anche attraverso apposita strumentazione.

### 6.3. Dati informatici

I dati devono essere protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti (Firewall e Antivirus) da aggiornare con cadenza almeno semestrale; inoltre devono essere aggiornati i programmi volti a prevenire la vulnerabilità dei sistemi elettronici (Antivirus) e a correggerne difetti; questi aggiornamenti devono essere effettuati almeno con cadenza annuale e nel caso si tratti di dati sensibili o giudiziari l'aggiornamento è semestrale.

### 6.4. Utilizzo di strumenti informatici

È consentito l'utilizzo dei soli strumenti informatici posti a disposizione dei destinatari da parte della Società.
È tassativamente vietata l'applicazione di hardware e/o software non fornito dalle competenti funzioni della Società.

### 6.5. Posta elettronica aziendale

L'utilizzo dei programmi di posta elettronica aziendale è concesso al fine esclusivo di condividere informazioni dal contenuto strettamente professionale, nell'esercizio delle mansioni affidate.
Sono vietati i messaggi di contenuto oltraggioso e discriminatorio, idonei a integrare violazioni di sicurezza, a diffondere e/o comunicare senza autorizzazione informazioni a terzi, per compiere o consentire attività di spamming, phishing o altri illeciti.
Non è consentito comunicare a terzi dati o informazioni inerenti il personale o l'Azienda, se ciò non rientra nelle ordinarie mansioni affidate, salvo formale autorizzazione.
Le comunicazioni private non sono consentite.
Per la corrispondenza privata può essere consentito accedere alla propria casella di posta elettronica privata sul Web.

È vietato utilizzare l'indirizzo di posta elettronica aziendale per registrarsi e partecipare a siti e applicazioni Web, forum, rubriche o mailing list, non legati all'attività lavorativa e non preventivamente e formalmente autorizzati.

### 6.6. Navigazione Internet

È consentito l'utilizzo delle risorse internet solo all'interno di siti attinenti al lavoro svolto in società:

- non è consentito navigare in siti che non siano coerenti con lo svolgimento delle mansioni lavorative svolte, soprattutto in quelli che possono rilevare le opinioni politiche, religiose, sindacali o personali del dipendente/collaboratore;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili salvo i casi direttamente autorizzati dall'azienda e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scaricamento (download) di software gratuiti (freeware) e shareware prelevati da siti internet, se non espressamente autorizzati dall'azienda o persona da essa delegata;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all' attività lavorativa;
- non è permessa la partecipazione, per motivi non professionali, a Forum, l'utilizzo di ChatLine, di bacheche elettroniche e le registrazioni in Guest Book anche utilizzando pseudonimi (nickname);
- è vietata la divulgazione di foto o notizie riguardanti il lavoro – senza specifica autorizzazione scritta – tramite web anche utilizzando blog, social network (es.Facebook) e simili. Parimenti è vietata la creazione di "profili utente" al fine di partecipare a blog, social network e simili applicazioni, senza preventiva, specifica autorizzazione;
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o l'invio/ricevimento anche tramite mail;
- non è consentito il download di programmi, file video o musicali, anche se gratuiti, salvo autorizzazione preventiva ed espressa.

## 7. COMPITI DELL'ORGANISMO DI VIGILANZA

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con gli addetti preposti ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.
I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.
Per il perseguimento di tale scopo, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le fattispecie di attività a rischio indicate nella presente Parte Speciale.
In merito ai controlli svolti, l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste dal Modello.
All'Organismo di Vigilanza devono essere tempestivamente comunicati:

- gli aggiornamenti e le modifiche apportati alla struttura societaria, alle figure apicali ed alle altre procedure che definiscono le attività informatiche aziendali;
- le anomalie rilevate nell'ambito delle azioni di monitoraggio svolte sulle procedure informatiche.

Il Responsabile dei Sistemi Informativi trasmette all'Organismo di Vigilanza una relazione periodica concernente gli esiti delle attività di monitoraggio e controllo attuate.