CADF

La Fabbrica dell'Acqua

Modello
di Organizzazione e di Gestione
ex decreto legislativo
8 giugno 2001 n. 231

PARTE SPECIALE "E"

DELITTI INFORMATICI
E TRATTAMENTO DATI
E DELITTI IN MATERIA DI
VIOLAZIONE DEL DIRITTO D'AUTORE

CADF S.P.A.

Modello di Organizzazione e di Gestione ex decreto legislativo 8 giugno 2001 n.231

PARTE SPECIALE "E"

DELITTI INFORMATICI E TRATTAMENTO DATI E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

Natura del documento: Edizione definitiva

Approvazione: Consiglio d'Amministrazione

Data Approvazione: 08/09/2020

Tabella Edizioni e revisioni

2	0	10/07/2020	Aggiornamento contenuti con estensione perimetro di prevenzione	08/09/2020
1	0	01/09/2015	Prima emissione	01/09/2015
Edizione	Revisione	Data Revisione	Motivazione	Data approvazione Consiglio d'Amministrazione

INDICE

PARTE SPECIALE "E"
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

E.1 LE TIPOLOGIE DEI DELITTI INFORMATICI E TRATTAMENTO DATI (art. 24-bis del Decreto) E DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (art. 25-novies del Decreto)

I "Delitti informatici e trattamento illecito di dati", di cui all'art. 24-bis D.Lgs. n. 231/2001 ed i "Delitti in materia di violazione del diritto d'autore" di cui all'art. 25-novies D.Lgs n. 231/2001 (d'ora in poi anche "Decreto"), sono indicati ed analizzati all'interno del Capitolo dedicato, inserito nel documento "GEN03 Elenco Reati Presupposto", allegato e parte integrante del MOGC Parte Generale di CADF S.P.A. (di seguito "CADF" o la "Società"), cui si rimanda per i relativi approfondimenti.

E.2 AREE A RISCHIO

In relazione ai reati di cui agli artt. 24-bis e 25-novies, D.Lgs n. 231/2001 e in base all'attività di analisi dei rischi svolta, le aree ritenute maggiormente a rischio per CADF, risultano essere, ai fini della presente Parte Speciale del Modello, quelle di seguito indicate.

- *Per i Delitti informatici e trattamento illecito di dati (art. 24-bis D.Lgs. n. 231/2001):*
  1) Gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT;
  2) Gestione della sicurezza fisica dei sistemi informativi e telematici della società;
  3) Gestione della sicurezza logica (accessi a sistemi informativi o telematici e reti di dati);
  4) Gestione e trattamento di dati personali;
  5) Tutte le attività aziendali svolte dai destinatari tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso ad internet;
  6) Gestione dei flussi informativi elettronici con la pubblica amministrazione;
  7) Gestione di reti di telecomunicazione;
  8) Gestione della sicurezza fisica delle sedi aziendali.
- *Per i Delitti in materia di violazione del diritto d'autore (art. 25-novies D.Lgs n. 231/2001):*
  1) Gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT;
  2) Tutte le attività aziendali svolte dai destinatari tramite l'utilizzo dei sistemi informativi aziendali, del servizio di posta elettronica e dell'accesso ad internet;
  3) Gestione dei flussi informativi elettronici con la pubblica amministrazione.

Per un'individuazione analitica di aree, processi e attività risultanti più a rischio per la Società si rinvia alla Mappatura delle Aree a Rischio – rispettivamente - Delitti informatici e trattamento illecito di dati e Delitti in materia di violazione del diritto d'autore, allegate alla presente Parte Speciale.

Eventuali integrazioni delle Aree a Rischio potranno - su proposta dell'Organismo di Vigilanza, anche su segnalazione delle funzioni interessate - essere disposte dal Presidente del Consiglio d'Amministrazione, al quale viene dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.

E.3 DESTINATARI E OBIETTIVO DELLA PARTE SPECIALE

La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, sindaci, liquidatori, dirigenti e dipendenti ("Esponenti Aziendali") della Società, nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito tutti definiti i "Destinatari").

Obiettivo della presente Parte Speciale è che tutti i Destinatari, come sopra individuati, si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento di attività nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di CADF – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi di Delitti informatici e trattamento illecito di dati e di Delitti in materia di violazione del diritto d'autore.

In particolare, la presente Parte Speciale ha la funzione di fornire:

a) un elenco dei principi generali e delle procedure specifiche cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;

b) all'Organismo di Vigilanza (d'ora in poi anche "ODV"), e ai responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica previste.

E.4 PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE DEL PROCESSO DECISIONALE NELLE AREE DI ATTIVITÀ A RISCHIO

E.4.1 Regolamentazione

In relazione alle rispettive funzioni, oltre alle regole di cui al presente Modello, gli Esponenti Aziendali devono in generale conoscere e rispettare tutte le regole, procedure e principi - che si devono intendere come attuativi ed integrativi del Modello - contenuti nei seguenti documenti:

- Codice Etico;
- Statuto Sociale;
- Regolamento interno per l'utilizzo del sistema informatico e telecomunicazioni;
- Sistema di autoregolamentazione inerente la corporate governance, la struttura organizzativa, la gestione amministrativa, contabile e finanziaria, il sistema di controllo interno della Società (Regolamenti, manuali, procedure aziendali, istruzioni operative e ogni altra disposizione);
- Whistleblowing – Procedure per la segnalazione di illeciti;

- Ogni altra documentazione relativa al sistema di controllo interno in essere nella Società;
- Norme inerenti il sistema informativo e il trattamento dei dati diffuse dalla Società;
- Normativa applicabile;
- Organigramma aziendale.

L'insieme organico di tali documenti - che determina, per le diverse aree di intervento, le regole a cui gli Esponenti Aziendali nonché i soggetti esterni, in funzione del rapporto che li lega a CADF, devono conformarsi – deve regolamentare rispettivamente:

- il governo della sicurezza delle informazioni (relativo ad esempio, alla determinazione dei Piani di Sicurezza dei sistemi informativi, alla segnalazione e risposta agli incidenti di sicurezza delle informazioni, alla formazione e sensibilizzazione per la sicurezza delle informazioni, etc.);
- i controlli di sicurezza specifici per tipologia di asset informativo (relativi ad esempio alla selezione di contromisure per piattaforme e sistemi, applicazione, database, etc.);
- i controlli di sicurezza indipendenti dalla tipologia di asset, volti ad indirizzare i comportamenti e le azioni operative degli Esponenti Aziendali (ad esempio in relazione all'uso accettabile delle risorse informative, alla gestione dei diritti di accesso alle risorse, alla tracciabilità degli eventi, etc.).

E.4.2 Divieti

La presente Parte prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, e a carico dei Collaboratori esterni e Partner, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la Società - di:

- porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino - direttamente o indirettamente - le fattispecie di reato previste dagli artt. 24-bis e 25 novies del Decreto (anche solo nella forma del tentativo);
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- violare le prescrizioni della presente Parte Speciale;
- porre in essere comportamenti non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

E.4.3 Principi generali

Nell'espletamento delle rispettive attività, oltre alle previsioni di legge esistenti in materia, i principi generali e i criteri di condotta disposti dal Codice Etico e alle prescrizioni contenute nella Parte Generale del presente Modello, i Destinatari sono tenuti ad attenersi ai seguenti principi generali di condotta:

a) tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività che comportano l'utilizzo di apparecchiature informatiche e telematiche;

b) osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità delle informazioni contenute nei sistemi informatici e non danneggiare e/o distruggere i dati in essi contenuti;

c) rispettare le regole in materia di trattamento dei dati personali in attuazione del Regolamento UE 2016/679 (c.d. GDPR) e del D.Lgs. 196/03 (c.d. Legge Privacy), come aggiornato dal D.Lgs. n. 101/2018;

d) selezionare con particolare attenzione e in base ad apposita procedura, le controparti destinate a fornire servizi di IT (Information Technology), valutandone l'affidabilità ex ante;

e) installare e utilizzare prodotti software nel rispetto degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano il diritto d'autore.

Ai Destinatari che intrattengono rapporti negoziali per conto di CADF con soggetti terzi deve essere formalmente conferita una delega in tal senso (con apposita procura scritta, qualora debbano essere compiuti atti idonei ad impegnare la Società).

Accanto al rispetto dei principi generali di condotta, dei principi procedurali specifici di cui al successivo paragrafo E.5, tutti i Destinatari sono tenuti al rispetto dei principi di comportamento contenuti nei documenti organizzativi aziendali al fine di prevenire la commissione dei Reati di cui agli artt. 24-bis e 25-novies del Decreto.

Infine, per ciò che concerne i rapporti con Partner, Fornitori e con eventuali altre Controparti coinvolte in attività a rischio, anch'essi Destinatari della presente Parte Speciale, ai medesimi deve essere resa nota l'adozione del Modello e del Codice Etico da parte di CADF, la cui conoscenza e il cui rispetto costituirà obbligo contrattuale a loro carico.

E.5 AREE DI ATTIVITA' A RISCHIO: ELEMENTI FONDAMENTALI DEL PROCESSO DECISIONALE

E.5.1 Responsabile interno

Per tutte le operazioni a rischio che concernono le attività sensibili individuate nel paragrafo E.2 di questa Parte Speciale, i protocolli di prevenzione individuano un Responsabile Interno per l'attuazione dell'operazione, che corrisponde, salvo diversa indicazione da parte del Presidente della Società o di un dirigente da questi incaricato, al responsabile della funzione competente per la gestione dell'operazione a rischio considerata.

Il Responsabile Interno:

- è soggetto referente e responsabile dell'operazione a rischio;
- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che si occupano o si sono occupati dell'operazione a rischio;

- informa tempestivamente l'ODV di qualunque criticità sorta durante lo svolgimento dell'operazione a rischio;
- trasmette un'informativa periodica all'ODV, mediante compilazione di apposita Scheda di evidenza;
- può interpellare l'Organismo di Vigilanza in tutti i casi di inefficacia, inadeguatezza o difficoltà di attuazione dei protocolli di prevenzione o delle procedure operative di attuazione degli stessi o al fine di ottenere chiarimenti in merito agli obiettivi e alle modalità di prevenzione previste dal Modello.

E.5.2 Principi procedurali specifici

Si indicano qui di seguito i principi procedurali specifici che in relazione ad ogni singola Area a Rischio (come individuate nel paragrafo E.2) i Destinatari sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte dell'Organismo di Vigilanza.

Ai fini dell'attuazione dei principi generali indicati al paragrafo E.4, oltre che delle prescrizioni della Parte Generale del presente Modello, nell'adottare procedure relative alle attività sensibili dovranno essere osservati anche i principi di riferimento di seguito indicati.

Costituiscono parte integrante del Modello le procedure aziendali che danno attuazione ai principi e alle misure di prevenzione indicate nel Codice Etico e nel Modello per prevenire i Delitti informatici e trattamento illecito di dati e i Delitti in materia di violazione del diritto d'autore.

Le procedure devono essere monitorate e mantenute aggiornate.

Per la prevenzione delle fattispecie di reato, anche tentato, rientranti tra quelle richiamate dagli artt. 24-bis e 25-novies del Decreto i Destinatari (cioè, Esponenti Aziendali nonché altri Soggetti esterni eventualmente autorizzati), oltre quanto indicato in precedenza, sono tenuti a rispettare le seguenti prescrizioni.

E.5.2.1 Prescrizioni

È vietato:

- connettere ai sistemi informatici della Società, personal computer, periferiche, altre apparecchiature o installare e/o utilizzare software senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
- procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- modificare in qualunque modo la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa e debita autorizzazione;
- acquisire, possedere o utilizzare strumenti software e/o hardware – se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informativi aziendali – che potrebbero

essere adoperati abusivamente per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);

- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;
- divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere abusivamente ad un sistema informatico altrui – ovvero nella disponibilità di altri Dipendenti o terzi – nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- acquisire e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- accedere abusivamente al sito Internet della Società al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, infografica, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;
- comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
- mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- lo spamming come pure ogni azione di risposta al medesimo;
- inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

E.5.2.2 Impegni della Società

La Società si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1) informare adeguatamente i Dipendenti e tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, dell'importanza di:
    a. mantenere le proprie credenziali confidenziali e di non divulgare le stesse a soggetti terzi;

b. utilizzare correttamente i *software* e banche dati in dotazione;

c. non inserire dati, immagini o altro materiale coperto dal diritto d'autore senza avere ottenuto le necessarie autorizzazioni dai propri superiori gerarchici secondo le indicazioni contenute nelle policy aziendali;

2) prevedere attività di formazione e addestramento periodico in favore dei Dipendenti, diversificate in ragione delle rispettive mansioni, nonché, in misura ridotta, in favore di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali, anche con riferimento alla Disciplina Privacy;

3) definire nell'ambito del Codice Etico e delle policy di Information Security i comportamenti accettabili per l'utilizzo corretto dei software e delle banche dati;

4) far sottoscrivere ai Dipendenti, nonché a tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;

5) informare i Dipendenti, nonché tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi, della necessità di non lasciare incustoditi i propri sistemi informatici e di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

6) impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzate per un determinato periodo di tempo, si blocchino automaticamente;

7) limitare gli accessi alle stanze server unicamente al personale autorizzato;

8) proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

9) dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;

10) impedire l'installazione e l'utilizzo di software non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;

11) informare gli utilizzatori dei sistemi informatici che i *software* per l'esercizio delle attività di loro competenza sono protetti dalle leggi sul diritto d'autore ed in quanto tali ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;

12) limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di virus capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti e, in ogni caso, implementare – in presenza di accordi

sindacali – presidi volti ad individuare eventuali accessi o sessioni anomale, previa individuazione degli "indici di anomalia" e predisposizione di flussi informativi tra le Funzioni competenti nel caso in cui vengano riscontrate le suddette anomalie;

13) impedire l'installazione e l'utilizzo, sui sistemi informatici della Società, di software Peer to Peer mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, etc.) senza alcuna possibilità di controllo da parte della Società;

14) qualora per la connessione alla rete Internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i router della stessa e compiere illeciti ascrivibili ai Dipendenti;

15) prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti e di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

16) limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti e di tutti gli altri soggetti – come ad esempio i Collaboratori Esterni – eventualmente autorizzati all'utilizzo dei Sistemi Informativi;

17) provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;

18) prevedere, nei rapporti contrattuali con i Fornitori di servizi software e banche dati sviluppati in relazione a specifiche esigenze aziendali, clausole di manleva volte a tenere indenne CADF da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale di terzi. Prevedere che negli stessi rapporti vengano sottoscritti specifici documenti con cui si impegnino al corretto utilizzo e alla tutela delle risorse informative aziendali con cui entrano in contatto;

19) trattare qualsiasi dato personale relativo alle persone fisiche identificate o identificabili ("Interessati") in conformità alla Disciplina Privacy vigente.

Per ciò che specificatamente attiene i controlli aziendali, la Società attribuisce alla Funzione responsabile dei Sistemi Informativi i seguenti compiti:

- monitorare centralmente in tempo reale, in collaborazione con le Direzioni/Funzioni interessate, lo stato della sicurezza operativa delle varie piattaforme ICT (sistemi e reti) di processo e gestionali, attraverso strumenti diagnostici e coordinare le relative azioni di gestione;
- monitorare centralmente in tempo reale i sistemi anti-intrusione e di controllo degli accessi ai siti aziendali e gestire le autorizzazioni;
- gestire il processo di identificazione ed autorizzazione all'accesso alle risorse ICT aziendali;

- gestire i processi/procedure di escalation interne ed esterne in occasione di situazioni di emergenza e/o crisi informatiche e in caso di data breach di dati personali, con il supporto delle Direzioni/Funzioni responsabili interessate;
- svolgere analisi degli incidenti avvenuti;
- svolgere analisi di vulnerabilità;
- produrre report a supporto del vertice aziendale.

E.5.3 Contratti

Nei contratti e nelle lettere di incarico con Partner, Fornitori e eventuali altre Controparti coinvolte nelle attività a rischio deve essere contenuta apposita clausola che regoli le conseguenze della violazione, da parte delle controparti stesse, delle norme di cui al Decreto nonché di quanto disposto dal Modello e dal Codice Etico adottati dalla Società.

E.6 ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i Delitti informatici e trattamento illecito di dati e i Delitti in materia di violazione del diritto d'autore di cui agli artt. 24-bis e 25-novies del Decreto, sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati di cui agli artt. 24-bis e 25-novies del Decreto. Con riferimento a tale punto l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti della Società eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme in materia e/o delle disposizioni della presente Parte Speciale, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- proporre e collaborare alla predisposizione e all'aggiornamento delle istruzioni standardizzate (scritte e conservate su supporto cartaceo o informatico) relative a
    - comportamenti da seguire nell'ambito delle Aree a Rischio individuate nella presente Parte Speciale;
    - flussi informativi a favore dell'ODV;
    - compilazione omogenea e coerente delle Schede di Evidenza;
    - limiti entro i quali non è necessaria l'utilizzazione di alcune voci della Scheda di Evidenza;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

- verificare periodicamente il sistema di deleghe in vigore, raccomandando modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli Esponenti Aziendali.

Allo scopo di svolgere le proprie funzioni, l'Organismo di Vigilanza può:

a) partecipare agli incontri organizzati dalla Società tra le funzioni aziendali competenti, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

b) accedere a tutta la documentazione ed a tutti i siti rilevanti per lo svolgimento dei propri compiti.

La Società istituisce a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per esercitare le sue attività di monitoraggio e di verifica dell'efficace esecuzione delle procedure, dei regolamenti e dei controlli previsti dal Modello e, in particolare, dalla presente Parte Speciale.

In particolare, il *Data Protection Officer* (DPO), con cadenza annuale, trasmette all'ODV un apposito flusso informativo avente ad oggetto le misure adottate per garantire un livello di sicurezza adeguato al rischio, ai sensi del Reg. UE 2016/679, le eventuali criticità riscontrate e la formazione erogata in materia.

In ogni caso, l'informativa all'ODV dovrà essere data:

- senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nel paragrafo E.5 della presente Parte Speciale ovvero alle procedure, policy e normative aziendali attinenti alle aree sensibili sopra individuate;
- nel rispetto della periodicità definita per la trasmissione della Scheda evidenza da parte dei responsabili di funzione, indipendentemente dalla presenza o meno di criticità.

Le modalità di informativa all'ODV sono oggetto di speciale procedura aziendale.

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nella presente Parte Speciale deve essere conservata da ciascun Destinatario coinvolto nel processo per le attività di propria competenza e messa a disposizione dell'Organismo di Vigilanza.

I Destinatari sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità e dando atto del processo autorizzativo seguito.

E.7 **ALLEGATI**

Mappatura delle Aree a Rischio di Delitti informatici e trattamento illecito di dati

Mappatura delle Aree a Rischio di Delitti in materia di violazione del diritto d'autore