FONDAZIONE
ENTE CELERI ETS

DOCUMENTO	**PARTE SPECIALE B:** **DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI** **(Art. 24 - bis D.Lgs. 231/01)**
RIFERIMENTI	MOGC D.LGS 231/01
REVISIONE	Rev. 02 del 30/04/2026

SOMMARIO

CONTROLLO DEL DOCUMENTO

TABELLA DI CONTROLLO DELLE REVISIONI		
REV.	DATA	CAUSALE
00	30 febbraio 2014	Prima emissione
01	26 marzo 2019	Aggiornamento MOGC
02	30 aprile 2026	Aggiornamento MOGC

Approvato dal CdA in data 30/04/2026

1. INTRODUZIONE

L'art. 7 della Legge 18 marzo 2008, n. 48 ha introdotto nel D.Lgs. 231/01, l'articolo 24-bis in materia di delitti informatici e trattamento illecito dei dati, ampliando così le fattispecie che possono generare la responsabilità dell'Ente.
Con l'introduzione dei reati sopra citati, il legislatore ha predisposto una duplice tutela che assicura:
- l'integrità dei sistemi informatici, ovvero la non alterabilità dei dati, delle informazioni e dei sistemi medesimi;
- la disponibilità e confidenzialità, ovvero la possibilità, solo da parte dei soggetti autorizzati, di accedere, disporre e conoscere delle informazioni, e del contenuto delle comunicazioni;
- l'autenticità, ovvero la certezza, da parte del destinatario della comunicazione, dell'identità del mittente.
Tuttavia, non tutti i comportamenti correlati all'uso del computer, ancorché penalmente rilevanti, possono rientrare nel novero dei reati informatici, dovendo tale qualifica essere riservata, più correttamente, ai soli casi in cui il sistema informatico o altri beni informatici (quali dati o programmi) costituiscano l'oggetto materiale della condotta criminosa.

2. DESTINATARI

Sono destinatari della presente Parte Speciale del MOGC ai sensi del D.Lgs. 231/01 della Fondazione Ente Celeri ETS (di seguito "Organizzazione") e si impegnano al rispetto del contenuto dello stesso:

- Il Consiglio di amministrazione e i dirigenti dell'Organizzazione (cosiddetti soggetti apicali);
- i dipendenti dell'Organizzazione (cosiddetti soggetti interni sottoposti ad altrui direzione).

In forza di specifica accettazione o in forza di apposite clausole contrattuali possono essere destinatari di specifici obblighi per il rispetto del contenuto del Codice Etico i seguenti soggetti esterni:

- i collaboratori, i consulenti e in generale i soggetti che svolgono attività di lavoro autonomo;

Obiettivo della presente Parte Speciale è che tutti i destinatari, come sopra individuati, adottino regole di condotta conformi a quanto prescritto dalla stessa, al fine di prevenire ed impedire il verificarsi dei reati che ne formano oggetto.

3. TERMINI E DEFINIZIONI

Il presente documento è stato redatto nel rispetto dei principi etici di riferimento espressi nel Codice Etico e tenendo conto delle definizioni riportate nella Parte Generale del MOGC.

Sono riportate di seguito alcune definizioni strumentali alla comprensione della presente Parte Speciale del MOGC:

DOCUMENTO INFORMATICO ai sensi dell'art. 491-*bis* c.p., si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

OPERAZIONE A RISCHIO per la Parte Speciale B, qualsiasi attività aziendale che comporti l'accesso a informazioni, dati o programmi informatici altrui o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

4. LE FATTISPECIE DI REATO

Si riporta di seguito una sintetica descrizione dei reati contemplati nell'art.24 – *bis* del Decreto.

Riferimento	Reato presupposto	Descrizione reato
Art.24 bis D.Lgs. 231/01	art.491-bis c.p. (Documenti informatici)	Documenti informatici - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.
Art.24 bis D.Lgs. 231/01	art. 615-ter c.p. (Accesso abusivo ad un sistema informatico o telematico)	Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni (Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.
Art.24 bis D.Lgs. 231/01	art. 615-quater c.p. (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)	Chiunque, al fine di procurer a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164. La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1). La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.
Art.24 bis D.Lgs. 231/01		

Riferimento	Reato presupposto	Descrizione reato
Art.24 bis D.Lgs. 231/01	art. 617-quater c.p. (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)	Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da quattro a dieci anni se il fatto è commesso: 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma; 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema.
Art.24 bis D.Lgs. 231/01	art. 617-quinquies c.p. (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)	Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater. Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni. Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni.
Art.24 bis D.Lgs. 231/01	art. 635-bis c.p. (Danneggiamento di informazioni, dati e programmi informatici)	Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni. La pena è della reclusione da tre a otto anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.
Art.24 bis D.Lgs. 231/01	art. 635-ter c.p. (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)	Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.La pena è della reclusione da tre a otto anni:1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).

Riferimento	Reato presupposto	Descrizione reato
Art.24 bis D.Lgs. 231/01	art. 635-quater c.p. (Danneggiamento di sistemi informatici o telematici)	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni. La pena è della reclusione da tre a otto anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.
Art.24 bis D.Lgs. 231/01	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.	Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329. La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1). La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.
Art.24 bis D.Lgs. 231/01	artt. 635-quinquies (Danneggiamento di sistemi informatici o telematici di pubblico interesse)	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis ovvero attraverso l' introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni. La pena è della reclusione da tre a otto anni:1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici. La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3).
Art.24 bis D.Lgs. 231/01	art. 640-quinquies c.p. Frode informatica del certificatore di firma elettronica	Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.
Art.24 bis D.Lgs. 231/01	Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)	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 attività 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 attività 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, è punito con la reclusione da uno a tre anni.
Art.24 bis D.Lgs. 231/01	art. 629, comma 3, c.p. Estorsione	Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635 bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità

5. LE ATTIVITÀ SENSIBILI EX ART. 24-bis DEL DECRETO

L'utilizzo degli strumenti informatici, l'accesso ai sistemi informatici aziendali e la gestione di documenti informatici si estende sostanzialmente – a vario titolo – a tutti gli operatori aziendali. Prevalentemente si tratta i documenti di tipo privato. In ragione dei rapporti con le autorità pubbliche, è, tuttavia, teoricamente ipotizzabile che vi possa essere l'accesso a documenti informatici pubblici da parte di operatori aziendali.

In linea generale le attività a rischio di commissione dei reati ex art. 24 –*bis* del D.Lgs. 231/01 posso essere così identificate:

- accesso a sistemi informatici e telematici della PA per inserimento di dati previdenziali, assicurativi, fiscali ed inerenti l'attività dell'Organizzazione (es. ATS, Regione Lombardia, INPS, INAIL, etc.).
- accesso a sistemi informatici e telematici privati es. banca
- utilizzo e detenzione di ID e/o le password di accesso a portali internet per i quali è necessario avere delle specifiche credenziali
- gestione delle firme elettroniche

I dettagli delle attività di analisi dei rischi svolte sono riportati nella **MATRICE DELLE ATTIVITÀ SENSIBILI EX D.LGS 231/01**.
Eventuali integrazioni delle suddette aree di attività a rischio potranno essere disposte dalla Direzione, anche su proposta dell'OdV, al quale è dato mandato di individuare le relative ipotesi e di definire gli opportuni provvedimenti operativi.
La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal Codice Etico adottato dall'Organizzazione alla cui osservanza sono tenuti tutti i destinatari

6. PRINCIPI GENERALI DI COMPORTAMENTO E PROTOCOLLI/PROCEDURE DI CONTROLLO

I destinatari della presente Parte Speciale del MOGC, oltre a rispettare le previsioni di legge esistenti in materia, le norme comportamentali e i principi generali di comportamento richiamati nel Codice etico devono rispettare le procedure e i regolamenti di cui sono responsabili previsti nel presente paragrafo e nell'ulteriore documentazione adottata.

In relazione alla gestione di sistemi e documenti informatici l'Organizzazione si è dotata del Dossier Privacy con le indicazioni delle contromisure da adottare al fine di annullare o di limitare le vulnerabilità e contrastare le minacce informatiche; tale documento costituisce parte integrante del presente Modello – e viene sottoposto per l'accettazione ad ogni dipendente della società.
Nello specifico nel Dossier sono indicate:

- la gestione degli accessi ai database esterni (sia PA sia privati) ossia chi detiene gli ID e/o le password di accesso a portali internet per i quali è necessario avere delle specifiche credenziali,
- il controllo della gestione delle smart card o business key per la firma digitale impiegata ai fini aziendali.

E' prevista inoltre la distribuzione in forma controllata dei beni informatici aziendali per i quali è mantenuta la rintracciabilità in appositi moduli.

L'Organizzazione ha adottato procedure e istruzioni specifiche finalizzate a descrivere la gestione dei processi a rischio di commissione dei reati; nello specifico riportiamo le procedure identificate per le attività a rischio:

- PROCEDURA PER LA GESTIONE DELLA RENDICONTAZIONE E FLUSSI INFORMATIVI AGLI ENTI PUBBLICI finalizzata a descrivere la gestione della rendicontazione all'ATS o ad altro ente pubblico con l'indicazione delle funzioni preposte al controllo dei dati di rendicontazione e con la descrizione della tipologia di dati inviati, le responsabilità, eventuali deleghe e le modalità di invio dei dati
- GESTIONE DEL PROCESSO DI APPROVVIGIONAMENTO E FORNITORI finalizzata a descrivere la gestione della selezione, qualifica e monitoraggio dei fornitori, a descrivere i criteri di selezione e di controllo dei fornitori in outsourcing a descrivere la gestione degli acquisti, i sistemi di selezione dei fornitori, tra cui aziende che gestiscono le infrastrutture informatiche in outsurcing
- DOSSIER PRIVACY

Si specifica che le procedure aziendali richiamate devono intendersi parti integranti della presente Parte Speciale del Modello.

Si ritiene che in relazione alla modestia del rischio rilevato, possa essere individuata quale efficace e sufficiente misura di prevenzione l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, la stretta osservanza delle regole dettate dal Dossier Privacy e dalle procedure sopra riportate unitamente alla rigorosa applicazione da parte della società del sistema disciplinare.

7. COMPITI DELL'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i reati informatici sono i seguenti:

- proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- svolgere verifiche periodiche sul rispetto delle procedure interne e valutare periodicamente la loro efficacia a prevenire la commissione dei Reati;
- esaminare eventuali segnalazioni specifiche ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

8. FLUSSO INFORMATIVO VERSO L'ODV

Al fine di garantire una maggior efficacia del modello, l'Organismo di Vigilanza predispone una comunicazione continua con l'Organizzazione (tramite l'**ALLEGATO A**), interrogandola su qualsivoglia evento che possa tradursi in una delle fattispecie di reato definite dal D.Lgs.231/01.
Per quanto concerne il flusso informativo riguardante i delitti informatici ex art. 24-bis del Decreto, si riportano, a titolo esemplificativo, i debiti informativi ai quali l'Organizzazione deve provvedere:

- Modifiche o revisioni del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs.231/01;
- Eventuali inosservanze o rilievi relative ad adempimenti in materia di Privacy;
- Modifiche al sistema Privacy;
- Eventuali modifiche al sistema IT, nuovi software, incidenti rilevanti sui sistemi IT, perdite o sottrazione di dati, virus, ecc.;
- Elenco eventuali provvedimenti o notizie da organi di Polizia Giudiziaria per attività d'indagine, anche nei confronti d'ignoti

9. SISTEMA SANZIONATORIO

Il sistema sanzionatorio previsto dal D.lgs.231/2001, per quanto concerne i reati commessi secondo l'art. 24-bis, prevede l'applicazione sia della sanzione amministrativa, con un minimo calcolato in 100 quote e un massimo di 500, sia della sanzione interdittiva, che può variare dai tre ai 24 mesi, a seconda delle fattispecie del reato implicato.