MODELLO
DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 8 GIUGNO 2001 N. 231

COSIMO DE' MEDICI SRL

PARTE SPECIALE B

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI
(ART. 24BIS)

COSIMO DE' MEDICI SRL	PARTE SPECIALE B DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI (ART. 24BIS)	
Revisione	Data	Tipo modifica
0		Prima emissione

LE FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati informatici, richiamati dall'art. 24 bis del D.Lgs.231/2001, ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa della società COSIMO DE' MEDICI SRL Individua inoltre le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di *risk assessment*) specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili".

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto societario di COSIMO DE' MEDICI SRL i seguenti reati:

Art. 24-bis	**Delitti informatici e trattamento illecito di dati**	Articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019
	Documenti informatici (art. 491-bis c.p.)	Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.
	Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	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 e´ 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 *(1)*. *(1) Articolo aggiunto dall´art. 4, L. 23 dicembre 1993, n. 547*

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)	Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna 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 ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell´articolo 617-quater.
Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615-quinquies c.p.)	Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)	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 sei mesi a quattro 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 uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) 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, ovvero con abuso della qualità di operatore del sistema; *3)* da chi esercita anche abusivamente la professione di investigatore privato *(1).* *(1) Articolo aggiunto dall´art. 6, L. 23 dicembre 1993, n. 547*
	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)	Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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 *(1).* *(1) Articolo aggiunto dall´art. 6, L. 23 dicembre 1993, n. 547*
	Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)	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 sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.
	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.)	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 utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. 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 tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.
	Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)	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 uno a cinque anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

	Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)	Se il fatto di cui all´articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

	Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)	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.
	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.

IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti informatici, sono di seguito indicate:

1. Accesso ai sistemi informatici aziendali o di terze parti, che contengono:

- informazioni riservate di enti pubblici;
- informazioni bancarie;
- parametri per l'attivazione di servizi;
- dati di fatturazione o di credito;
- dati relativi a pagamenti.

2. Gestione di strumenti e dispositivi e programmi, da parte di soggetti aziendali e amministratori di sistema, mediante i quali possono:

- essere intercettate informazioni rilevanti di terze parti o impedite comunicazioni;
- danneggiare un sistema informatico o telematico, nell'ambito delle strutture di un concorrente.

3. Falsificazione di documenti informatici relativi ad esempio a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della Società.
4. Acquisizione, detenzione e gestione abusiva di credenziali di accesso (password) a sistemi aziendali o di terze parti.

PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001, del Codice di Comportamento e del

PTPCT adottati dalla Società nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello che, a qualunque titolo, siano stati designati o incaricati alla gestione e manutenzione dei *server*, delle banche dati, delle applicazioni, dei *client* e delle reti di telecomunicazione, nonché a tutti coloro che abbiano avuto assegnate *password* e chiavi di accesso al sistema informativo aziendale sono tenuti ad osservare i seguenti principi di comportamento e controllo:

a) divieto di alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b) divieto di accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c) divieto di accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;

d) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

e) divieto di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

f) divieto di svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

g) divieto di svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

h) divieto di installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

i) divieto di svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

j) divieto di svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

k) divieto di distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;

l) divieto di utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore.

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;

2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione dell'Amministratore di Sistema;

3. segnalare all'Amministratore Delegato il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire al Dirigente l'originale della denuncia all'Autorità di Pubblica Sicurezza;

4. evitare di introdurre e/o conservare negli uffici della Società (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;

5. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;

7. evitare l'utilizzo di *passwords* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile Informatico (o figura analoga);

8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;

10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

11. impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dall'azienda stessa;

12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della società;

15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

PROCEDURE DI CONTROLLO

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati informatici, con particolare riferimento al processo strumentale alla commissione dei reati quale gestione della dell'infrastruttura tecnologica.

In particolare tali principi trovano specifica attuazione nelle procedure adottate dalla Società.

- Gestione delle comunicazioni e dell'operatività:

Lo standard richiede l'esistenza di uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure. In particolare, tale strumento normativo assicura:
a) il corretto e sicuro funzionamento degli elaboratori di informazioni;
b) la protezione da pericoloso;
c) il backup di informazioni e software;
d) la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
e) gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;

f) una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
g) il controllo sui cambiamenti agli elaboratori e ai sistemi;
h) la gestione di dispositivi rimovibili.

- Controllo degli accessi:
Lo standard richiede l'esistenza di uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo prevede:
a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password od altro sistema di autenticazione sicura;

b) le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;

c) una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;

d) la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;

e) la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;

f) l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;

g) la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;

h) la chiusura di sessioni inattive dopo un predefinito periodo di tempo;

i) la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e

j) l'adozione di regole di *clear screen* per gli elaboratori utilizzati;

k) i piani e le procedure operative per le attività di telelavoro.

- Gestione degli incidenti e dei problemi di sicurezza informatica:
Lo standard richiede l'esistenza di uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo prevede:
a) appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;

b) l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;

c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;

d) l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;

e) appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;

f) l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;

g) l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;

h) la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;

i) la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.

- Audit:
Lo standard richiede l'esistenza di uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica.

- Risorse umane e sicurezza:
Lo standard richiede l'adozione di uno strumento normativo che preveda:
a) la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa

applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
b) specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
c) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
d) la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi:
Lo standard richiede l'adozione di uno strumento normativo che definisca:
a) l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
b) la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
c) la confidenzialità, autenticità e integrità delle informazioni;
d) la sicurezza nel processo di sviluppo dei sistemi informativi.