



Casa di Cura Città Di Bra S.p.A.

Incontro formativo sul D.lgs. 231/01, sul D.lgs. n. 24/23 (c.d. «Whistleblowing») e sul Reg. UE n. 679/16

Avv. Cristiano Burdese



DECRETO 231: LA RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI (PRESUPPOSTI E PRINCIPI GENERALI)

La responsabilità amministrativa dell'ente:

- va a sommarsi a quella della persona fisica che ha commesso il reato;
- è autonoma rispetto alla tradizionale responsabilità penale personale;
- è accertata mediante meccanismi del processo penale;
- è legata alla commissione di un reato, ricompreso nel catalogo dei reati presupposto del Decreto;
- presuppone un reato commesso nell'interesse o a vantaggio dell'ente da parte di soggetti funzionalmente collegati al medesimo;
- l'ente risponde per un deficit organizzativo (la c.d. COLPA DI ORGANIZZAZIONE)
- coinvolge il patrimonio dell'ente ed il libero svolgimento della sua attività sociale (sanzioni pecuniarie ed interdittive)

DECRETO 231: CRITERI DI IMPUTAZIONE SOGGETTIVA

Art. 5 co. 1 del D.lgs. 231/2001:

La società risponde per i reati commessi nel suo interesse o vantaggio da soggetti **funzionalmente collegati all'ente** ed in particolare:

1. da persone che rivestono funzioni di rappresentanza, di amministrazione o direzione dell'ente o di una unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. **SOGGETTI APICALI**);
2. Da persone sottoposte alla direzione o vigilanza di uno dei soggetti di cui al punto 1 (c.d. **SOGGETTI SOTTOPOSTI**).

DECRETO 231: CRITERI DI IMPUTAZIONE SOGGETTIVA

- Per il reato commesso da SOGGETTI APICALI vige una presunzione assoluta di colpevolezza dell'ente in quanto questi ultimi sono considerati l'espressione della volontà della società;
- Per il reato commesso dai SOTTOPOSTI l'ente risponde solo se la commissione del reato è stata resa possibile dalla inosservanza degli obblighi di direzione e vigilanza.

DECRETO 231: CRITERI DI IMPUTAZIONE SOGGETTIVA

Soggetti apicali...presunzione di colpevolezza:

L'ente non risponde solo se prova (inversione onere della prova):

1. **ADOZIONE ED EFFICACE ATTUAZIONE**, prima della commissione del fatto, di un modello di organizzazione e gestione **idoneo** a prevenire il reato;
2. Nomina dell'**ORGANISMO DI VIGILANZA** dotato di autonomi poteri di iniziativa e di controllo con il compito di vigilare sull'osservanza, funzionamento e aggiornamento del modello;
3. Che **non vi è stata omessa o insufficiente vigilanza** da parte dell'organismo di vigilanza;
4. I soggetti apicali hanno commesso il reato **eludendo fraudolentemente** il modello.

La condotta fraudolenta dei soggetti apicali (caso Monte dei Paschi di Siena)

Il concetto di **elusione fraudolenta** necessita di una connotazione decettiva con caratteristiche tipiche dell'aggiramento di un vincolo, quindi una condotta «ingannevole, falsificatrice, obliqua, subdola».

Per tale ragione, l'**elusione fraudolenta del Modello 231** si espliciterebbe in una condotta di dissociazione da parte dei soggetti apicali rispetto alla politica dell'ente, frutto di una scelta personale e non riconducibile ad un difetto organizzativo.

La condotta fraudolenta dei soggetti apicali (caso Monte dei Paschi di Siena)

In particolare:

«L'aver, dunque, costoro approfittato dello spazio di autonomia tollerabilmente lasciato loro dal modello organizzativo in ragione del loro ruolo e, sì d'intesa tra loro, ma in completo spregio dei dati elaborati e loro offerti dalle competenti strutture tecniche della Società, l'aver alterato questi ultimi e divulgato ai mercati informazioni inveritiere non rappresenta – ad avviso del Collegio – una mera violazione delle prescrizioni del Modello.

Una siffatta condotta, invero, risulta munita di efficacia decettiva nei confronti degli altri organi dell'ente, non soltanto perché tenuta senza il rispetto del procedimento di comunicazione previsto dal modello, ma altresì in quanto frutto di un accordo estemporaneo e tale, perciò, da rendere impossibile ogni interlocuzione da parte di qualsiasi altro organo sociale».

DECRETO 231: CRITERI DI IMPUTAZIONE OGGETTIVA

INTERESSE: esprime la finalità dell'attività delittuosa che deve pertanto perseguire un'esigenza diretta dell'ente e non della persona fisica che lo commette.

VANTAGGIO: si considera il successivo ritorno economico o beneficio che la società riceve in seguito alla realizzazione del reato nel suo interesse e il suo accertamento comporta un giudizio ex post avente ad oggetto il risultato conseguito dall'ente.

Rileva anche il vantaggio indiretto, inteso come acquisizione per la società di una posizione di privilegio sul mercato derivante dal reato commesso dal soggetto apicale.

DECRETO 231: CRITERI DI IMPUTAZIONE OGGETTIVA

INTERESSE e VANTAGGIO NEI REATI COLPOSI: nei reati colposi l'interesse ed il vantaggio devono essere necessariamente riferiti alla **condotta e non all'esito anti giuridico (evento)**...è ben possibile che una condotta caratterizzata dalla violazione della disciplina cautelare e, quindi, colposa, sia posta in essere nell'interesse dell'ente e determini comunque il conseguimento di un vantaggio (Cass. Pen., S.S. U.U. 24/4/14 n. 38343, Thyssen).

L'ente non ha infatti alcun interesse nel causare lesioni ad un proprio dipendente, ma può certamente avere interesse a risparmiare sui costi per la predisposizione delle misure di sicurezza. Il vantaggio è dato naturalmente dal risparmio ottenuto o nel maggior profitto realizzato.

DECRETO 231: CRITERI DI IMPUTAZIONE OGGETTIVA

Rientra nel concetto di vantaggio il risparmio economico.

Nei reati colposi, l'interesse e/o il vantaggio vanno letti, nella prospettiva patrimoniale dell'ente, come risparmio di risorse economiche conseguente alla mancata predisposizione dello strumento di sicurezza ovvero come incremento economico conseguente all'aumento della produttività non ostacolata dal pedissequo rispetto della normativa prevenzionale.

Cass. Pen., sez. IV del 23/6/15 n. 31003:

Il risparmio non valutato necessariamente in termini economici, dal momento che può benissimo intendersi come risparmio sui tempi della produzione.

I DESTINATARI del Modello di Organizzazione Gestione e Controllo

SONO DESTINATARI:



Tutti coloro che sono legati alla Società da un **rapporto organico** con essa e dunque soggetti apicali (es. amministratori, direttori generali, institori, procuratori generali e speciali, sindaci)



Tutti coloro che sono legati alla Società da un **rapporto di lavoro subordinato** di qualsiasi genere e/o natura a prescindere dal loro inquadramento contrattuale (es. dirigenti con o senza deleghe, impiegati, quadri, lavoratori somministrati)



Tutti coloro che, a prescindere dalla tipologia del rapporto giuridico che li lega alla Società', subiscono in concreto, secondo l'organizzazione aziendale, il potere di direzione e vigilanza da parte di un qualsiasi soggetto apicale di essa.

NON SONO DESTINATARI:



tutte le persone fisiche e/o giuridiche che **intrattengono rapporti commerciali con la SOCIETÀ' nell'ambito del proprio oggetto sociale**, ma che, in concreto secondo l'organizzazione aziendale, **non subiscono l'esercizio del potere di direzione e vigilanza da parte di uno e/o più soggetti apicali** di essa (es. fornitori, clienti, consulenti)

Le SANZIONI previste dal D. Lgs. 231/01

Pecuniaria:

è sempre prevista l'applicazione di una sanzione pecuniaria, commisurata alla gravità del fatto, al grado di responsabilità dell'ente, alla condotta successiva alla commissione del reato nonché alle condizioni economiche dell'ente. La sanzione pecuniaria viene applicata per quote da 100 a 1000 ed ogni quota va da un minimo di Euro 258 ad un massimo di Euro 1549 (quindi minima Euro 25.800 e massima Euro 1.549,000).

Interdittive:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca di autorizzazioni, licenze, o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la PA (salvo che per ottenere la prestazione di un pubblico servizio);
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Le SANZIONI previste dal D. Lgs. 231/01

Confisca: del prezzo o del profitto del reato (ovvero somme di denaro equivalenti): è sempre disposta nei confronti dell'ente, salvo che per la parte che può essere restituita al danneggiato; sono fatti salvi i diritti acquisiti dai terzi in buona fede.

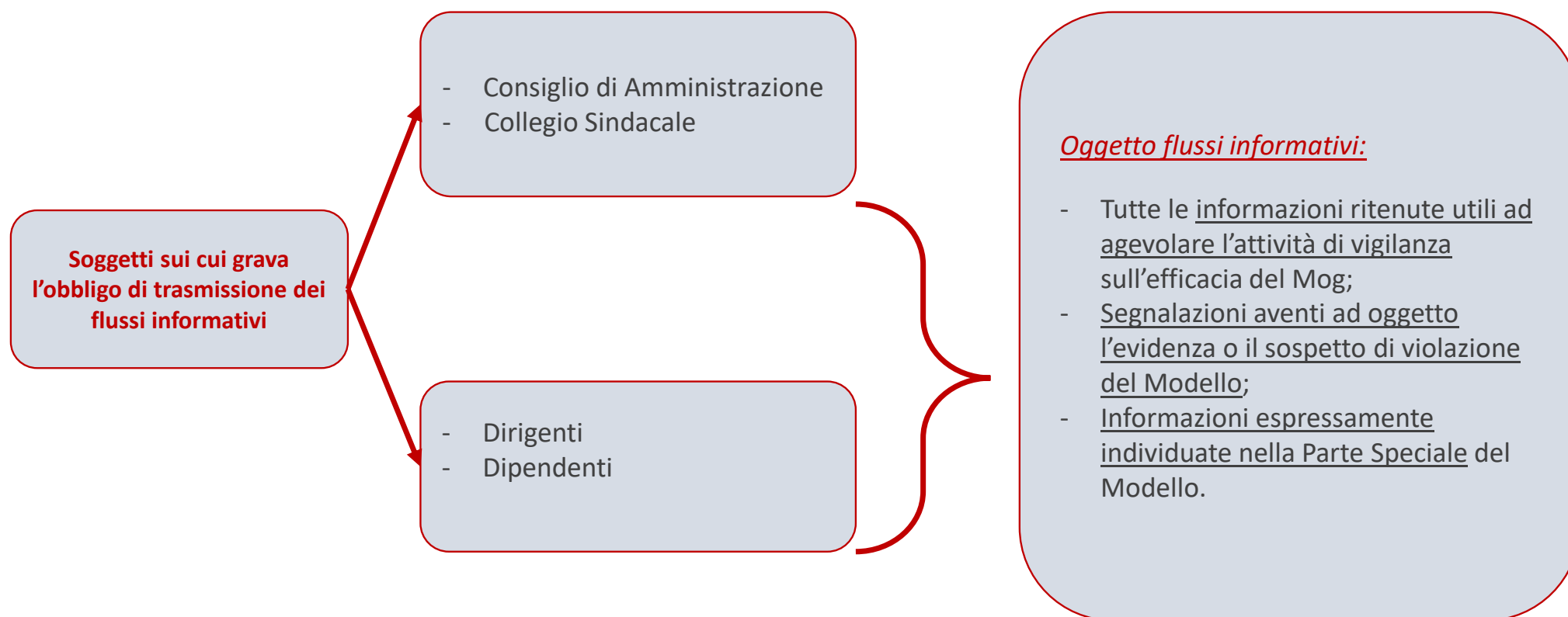
Pubblicazione della sentenza su quotidiano a tiratura nazionale

L'ORGANISMO DI VIGILANZA

L'art. 6 del D.Lgs. 231/01 affida il compito di vigilare sul funzionamento e sull'osservanza del Modello, nonché di curarne l'aggiornamento, ad un Organismo di Vigilanza che deve essere dotato dall'ente di autonomi poteri di iniziativa e di controllo. I compiti dell'OdV sono:

- **vigilare sull'effettività del Modello**: ossia verificare che i comportamenti posti in essere all'interno della Società siano conformi ai contenuti del Modello e al Codice Etico adottati
- **verificare l'efficacia del Modello**: ossia verificare che il Modello sia concretamente idoneo a prevenire il verificarsi dei reati rilevanti
- **proporre aggiornamenti del Modello** al fine di adeguarne il contenuto ai mutamenti ambientali ed alle eventuali modifiche della struttura aziendale, dei processi operativi della Società nonché alle novità legislative
- **raccogliere informazioni e condurre indagini** in merito alle violazioni del Modello, sia a fronte di eventuali segnalazioni esterne, sia come conseguenza dell'attività di vigilanza propria dell'OdV

I FLUSSI INFORMATIVI – Soggetti destinatari dell'obbligo



Flussi informativi – ESEMPI

- Devono esser raccolte eventuali segnalazioni relative: i) alla commissione, o al ragionevole pericolo di commissione, dei reati richiamati dal D.lgs. 231/01; ii) a «pratiche» non in linea con le norme di comportamento emanate dalla Società; iii) comportamenti che, in ogni caso, possono determinare una violazione del Modello;
- provvedimenti o notizie provenienti dagli organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D.lgs. 231/01 riguardanti la Società e i destinatari del Modello, direttamente o indirettamente;
- visite, ispezioni e accertamenti avviati da parte degli enti competenti (a titolo meramente esemplificativo: ASL, INPS, INAIL, Guardia di Finanza, etc.) e, alla loro conclusione, eventuali rilievi e sanzioni comminate;
- le notizie relative ai procedimenti disciplinari ed alle sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Flussi informativi – ESEMPI

- Violazioni del Codice Etico;
- Anomalie o criticità riscontrate dai responsabili nello svolgimento delle attività sensibili per l'applicazione del D.lgs. n. 231/01.

Procedura Flussi informativi verso l'Odv

I flussi informativi devono essere inviati all'ODV tramite la seguente casella di posta elettronica dedicata:

organismodivigilanza@ccbra.it

Whistleblowing

In alternativa, i destinatari del Modello 231 che intendano beneficiare delle tutele previste dalla normativa in materia di Whistleblowing di cui al D.lgs. n. 24/23 potranno presentare le segnalazioni di illeciti 231 o di violazioni del Modello (oltreché, le altre segnalazioni rilevanti ai sensi del D.lgs. n. 24/23 espressamente indicate nella Procedura Whistleblowing adottata dalla Società) al **Presidente dell'OdV, avv. Cristiano Burdese (in qualità di Gestore delle Segnalazioni Whistleblowing)** mediante i canali istituiti dalla Società, indicando chiaramente nell'oggetto della segnalazione che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni subite in ragione della segnalazione.

Whistleblowing

OGGETTO DELLE SEGNALAZIONI:

- 1) illeciti rilevanti ai sensi del Decreto 231 o violazioni del Modello 231;
- 2) illeciti commessi in violazione della normativa dell'Unione Europea indicata nell'Allegato I al D.lgs. n. 24/23 e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato); a titolo esemplificativo, e non esaustivo, si tratta di illeciti relativi ai settori dei prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, tutela della vita privata, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- 3) atti od omissioni che ledono gli interessi finanziari dell'Unione Europea come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'Unione Europea (es. frodi, corruzione e qualsiasi altra attività illegale connessa alle spese dell'Unione);

Whistleblowing

4) atti od omissioni riguardanti il mercato interno che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (sono ricomprese le violazioni delle norme UE in materia di concorrenza e di aiuti di Stato, di imposta sulle imprese ed i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle imprese);

5) ulteriori atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione Europea nei settori indicati nei punti precedenti.

di cui il segnalante sia venuto a conoscenza nello svolgimento dell'attività lavorativa.

Whistleblowing

Restano escluse dalle segnalazioni ammissibili:

- contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate, che seguiranno i canali tradizionali;
- segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali indicati dal decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella direttiva;
- segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione Europea.

Whistleblowing

Legittimazione a segnalare:

- i lavoratori subordinati della Casa di Cura Città di Bra S.p.A., a tempo determinato ed indeterminato, compresi i dirigenti;
- i lavoratori autonomi, liberi professionisti e consulenti che prestano la propria attività presso la Casa di Cura;
- i collaboratori che svolgono la propria attività lavorativa presso la Casa di Cura;
- soggetti terzi che forniscono beni o prestano servizi presso la Casa di Cura;
- i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Casa di Cura;
- gli azionisti (persone fisiche) e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso la Casa di Cura.

Whistleblowing

I canali istituiti dalla Società per la presentazione delle segnalazioni *Whistleblowing* (indicati sia nella procedura Whistleblowing adottata dalla Società sia nel MOGC 231 - parte generale) sono:

- **piattaforma informatica Whistleblowing**: piattaforma informatica “trusty”, accessibile via web dal sito www.ccbra.it da qualsiasi *device* con cui è possibile consentire l’accesso non solo ai dipendenti e diretti collaboratori, ma anche a terze parti;
- **segnalazione orale**: contattando l’avv. Cristiano Burdese al numero: 011-533234. Al momento della ricezione della segnalazione, il Gestore documenta la medesima mediante resoconto dettagliato ed il relativo contenuto viene controfirmato dal Segnalante, previa verifica ed eventuale rettifica. Il Gestore deve: a) garantire la riservatezza dell’identità del Segnalante; b) procedere all’archiviazione della segnalazione attraverso idonei strumenti che permettano di garantire la riservatezza dei soggetti tutelati;
- **incontro diretto e riservato con il Gestore del canale di segnalazione interna**, contattando l’avv. Cristiano Burdese al numero: 011-533234.

Cass. Pen. n. 38025 del 7/10/22 (smaltimento illecito di rifiuti)

Il Supremo Collegio ha ritenuto che nonostante gli sforzi posti in essere dell'ente, consistiti nell'aver implementato un Modello 231, istituito un OdV per l'osservanza dello stesso, adottato un sistema sanzionatorio e disciplinare, un codice etico e un manuale integrato di qualità, ambiente e sicurezza sul lavoro, questi fossero insufficienti a rendere idoneo, efficace ed «operativo» il Modello 231.

Un monito per tutti, soprattutto per gli enti, a comprendere come l'idoneità e l'efficacia di modello organizzativo, di un sistema di gestione 231, passi primariamente dall'essere concepito come grimaldello per un miglioramento complessivo della propria struttura, ma con un atteggiamento di sostanziale operatività. Tale approccio deve inevitabilmente comprendere il costante coinvolgimento dell'OdV con l'attivazione dei flussi informativi, l'attuazione di verifiche programmate, la richiesta di training formativi e la ricezione di report da parte delle diverse funzioni aziendali coinvolte in merito ai propri e rispettivi rischi penali costantemente mappati e sottoposti a valutazione.

TRIBUNALE DI MILANO, SEZ. II, n. 1070 del 22/4/24

Il Tribunale di Milano ha escluso la responsabilità di una società in relazione ad un'imputazione di false comunicazioni sociali:

il suo Modello 231 è stato ritenuto idoneo ed è stata pure ravvisata l'elusione fraudolenta di quest'ultimo da parte degli imputati.

Passaggi di rilievo della motivazione:

- **rilevanza sostanziale dei presidi di controllo;**
- **importanza del Whistleblowing** quale strumento per far emergere le violazioni: la sentenza evidenzia che la frode contabile è emersa tramite una segnalazione anonima pervenuta alla società controllante tramite il sistema di «speak up»;
- **rilevanza della formazione del personale che deve essere «intensa e continua»** e non effettuata con iniziative occasionali. Tale ultimo profilo è stato valorizzato anche in una recente sentenza del Tribunale di Milano, questa volta di condanna di una società farmaceutica per fatti di corruzione: in questo caso la sanzione pecuniaria era stata ridotta di un terzo avuto riguardo al comportamento diligente della società la quale aveva erogato corsi di formazione a tutti i dipendenti, compresi ai neoassunti, ed ai soggetti apicali, sia in modalità e-learning sia in presenza.

TRIBUNALE DI MILANO, SEZ. II, n. 1070 del 22/4/24

“In conclusione, ciò che è emerso è che le frodi perpetrate nel corso degli anni ed oggetto di indagine e le manipolazioni contabili che ne sono state la conseguenza siano state il frutto non della mancata adozione di un Modello di gestione del rischio-reato idoneo ed efficace, bensì di una serie di comportamenti fraudolenti posti in essere da «pochi», non evitabili né altrimenti prevedibili, che sono venuti allo scoperto a seguito di una segnalazione anonima (che in ogni caso rappresentava uno dei presidi di controllo previsti nel Modello) ed a seguito della quale sono state avviate approfondite attività di indagine interne ed allontanate le persone responsabili dei comportamenti fraudolenti».

IL SISTEMA DISCIPLINARE

Il “SISTEMA DISCIPLINARE”
costituisce un requisito essenziale del
Modello, ai fini della esenzione di
responsabilità della SOCIETA' e si
rivolge a tutti i suoi Destinatari.

IL SISTEMA DISCIPLINARE

Ai fini dell'applicazione del sistema disciplinare sono considerati, a titolo esemplificativo, comportamenti sanzionabili:

- La commissione di reati previsti dal D.lgs. 231/01, per quanto applicabile alla Società;
- La violazione di disposizioni e procedure interne previste dal Modello e dei principi espressi dal Codice Etico;
- **l'omissione di comunicazione dei flussi informativi/segnalazioni whistleblowing all'OdV;**

- **con riferimento ai soggetti in posizione apicale**, la violazione degli obblighi di direzione o vigilanza di cui all'art. 7 co. 1 D.lgs. 231/01 ovvero il mancato tempestivo intervento per eliminare violazioni del Modello e/o impedire la realizzazione dei reati presupposto;



IL SISTEMA DISCIPLINARE

CODICE
DISCIPLINARE

**SARANNO
APPLICABILI LE
SANZIONI IN MODO
PROPORZIONALE A**

- gravità della violazione/infrazione e/o del fatto commesso;
- natura e intensità dell'elemento soggettivo;

- ruolo aziendale, mansioni e qualifica dell'autore;

- grado di fiducia coesistente alle mansioni assegnate all'autore;
- ogni altra circostanza concreta ritenuta rilevante (eventuale recidiva).

REATI «PRESUPPOSTO» RILEVANTI PER LA SOCIETA'

- **Reati contro la P.A.** – artt. 24 e 25 D.lgs. n. 231/01;
- **Delitti informatici e trattamento illecito di dati, nonché delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori** – art. 24 bis e 25 – octies.1 D.Lgs. 231/01;
- **Delitti di criminalità organizzata** – art. 24 ter D.Lgs. 231/01;
- **Reati societari** – art. 25 ter D.Lgs. 231/01;
- **Delitti contro la personalità individuale** - art. 25 quinquies D.Lgs. 231/01;
- **Omicidio o lesioni gravi o gravissime commesse in violazione delle norme sulla tutela della salute e sicurezza sul lavoro** – art. 25 septies D.Lgs. 231/01;
- **Reati tributari** – art. 25 quinquiesdecies D.Lgs. 231/01;

REATI «PRESUPPOSTO» RILEVANTI PER LA SOCIETA'

- **Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (incluse le fattispecie di ricettazione e riciclaggio di beni culturali)** - art. 25 octies, septiesdecies e duodevicies D.Lgs. 231/01;
- **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori** – art. 25 octies.1 D.Lgs. 231/01;
- **Delitti in materia di violazione del diritto di autore** – art. 25 novies D. Lgs. 231/01
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** – art. 25 decies D. Lgs. 231/01
- **Reati ambientali** – art. 25 undecies D. Lgs. 231/01;
- **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, di procurato ingresso illecito e di favoreggiamento dell'immigrazione clandestina** - art. 25 duodecies D.Lgs. 231/01;
- **Reato di propaganda ed istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa** - art. 25 terdecies D.Lgs. 231/01;
- **Pratiche di mutilazione degli organi genitali femminili** – art. 25 quater.1 D.Lgs. 231/01.

Esempi di condotte illecite che
possono integrare i reati «231»

Reati informatici

Accedere a un sistema informativo, pubblico o privato, al fine di raccogliere informazioni riservate o consentire operazioni illecite a favore della Società.

Sei riuscito a trovare le offerte inviate dai nostri concorrenti?



Eccole!

Reati tributari e corruzione tra privati

Emissione di fatture o altri documenti per operazioni inesistenti

Ho notato che questa fattura fa riferimento ad una consulenza che però non è mai stata effettuata, ma sappiamo che il consulente è il fratello del nostro cliente più importante.....



Lascia stare, va bene così.

Reati tributari

Dichiarazioni fraudolente mediante altri artifici

*Mi raccomando, non inserire
quella voce nel bilancio, per
ora teniamola per noi*



*Ma cosa sta
dicendo?*

Assunzione di cittadini Extra Ue senza permesso di soggiorno

Assenza di verifica dei documenti necessari

Quel lavoratore ha una specializzazione per noi essenziale, se non lo assumiamo subito rischiamo di non rispettare i tempi di consegna della merce con il nostro più grande cliente! Però ha un permesso di assunzione scaduto e non sappiamo se ha ottenuto il rinnovo. Assumiamolo, poi si vedrà..



*Ma c'è
responsabilità
penale per chi firma
il contratto oltre che
dell'Amministratore
Delegato!!!!*

Reati contro la PA

Offrire beni (non di modico valore) o vantaggi a Pubblici Ufficiali al fine di ricevere un vantaggio per la Società:

Prego Ispettore, siamo così contenti che sia venuto a farci visita! La prego di accettare questo «piccolo omaggio». Ah dimenticavo, sua moglie è perfetta per la posizione di responsabile amministrativa della nostra società!



Come siete generosi! A questo punto mi sentirei veramente in difficoltà a negarvi qualcosa in futuro...

Concussione

Ci sarebbero sanzioni per 13.600€...ma se volete potremmo accordarci...



Cosa intendi?

Devo assolutamente avvertire l'OdV!

Salute e sicurezza sul lavoro

Avvalersi di un fornitore che offre DPI non adeguati ma a basso costo

Ho a disposizione dei DPI ad un prezzo stracciato... che ne pensi?



Uno sconto non si rifiuta mai! Con quello che costano i DPI all'azienda...

Strutture sanitarie: centralità delle condotte corruttive e della truffa ai danni dello Stato

Le strutture sanitarie sono a stretto contatto ed interlocuzione con la Pubblica Amministrazione.

Attraverso lo stanziamento di fondi, rimborsi, autorizzazioni ed accreditamento, vigilanza.

Corruzione

- Corruzione ai fini dell'accreditamento;
- Corruzione tra strutture e classe politica al fine di ricevere fondi;
- Corruzione nell'erogazione dei servizi medici.

Truffa ai danni dello Stato

- Fatture «gonfiate»;
- Effettuazione servizi non necessari ai fini di ottenere rimborsi;
- Richieste di rimborso non giustificate;
- Assunzione ed incarichi a soggetti senza i requisiti necessari.

Case Study

Cronaca dei fatti:

I professionisti avrebbero attestato sulle cartelle cliniche di alcuni pazienti fatti e situazioni non rispondenti al vero, allo scopo di procurarsi un indebito rimborso da parte della Regione Lombardia e dal SSN.

Si riportano di seguito i dettagli di provvedimento:

- la Guardia di Finanza ha notificato 24 avvisi di garanzia nei confronti dei dirigenti e dei medici del Policlinico;
- oltre agli avvisi di garanzia, è stato eseguito il sequestro preventivo di 2 milioni di Euro a carico della Società;
- in applicazione del D.lgs. 231/01, ad essere iscritto nel registro degli indagati è anche il Policlinico stesso ed il suo Amministratore, nell'interesse e a vantaggio del quale è stata realizzata la condotta.

Reati e condotte illecite:

Reati:

- Falso ideologico;
- Truffa ai danni del Servizio Sanitario Nazionale.

Condotte illecite:

- Erogazione prestazioni sanitarie non necessarie;
- Falsificazione DRG.

Case Study

Cronaca dei fatti:

Un ente ospedaliero, specializzato in ambito ortopedico, traumatologico e nelle terapie riabilitative, è stato sottoposto ad un procedimento ex D.lgs. n. 231/01, in quanto i medici che vi operano sono stati indagati per truffa ai danni dello Stato, avendo firmato delle **schede di dimissione ospedaliera** falsificate, **atte a gonfiare i rimborsi da richiedere all'ASL regionale**.

La struttura ospedaliera, che operava in forma di S.p.A. mista (49% privato e 51% pubblico) non aveva attuato il Modello 231. La struttura aveva infatti ritenuto che la struttura ospedaliera fosse un ente pubblico e, di conseguenza, che non fosse assoggettata alla normativa di cui al D.lgs. n. 231/01.

Reati e condotte illecite:

Reati:

- Truffa ai danni dello Stato;
- Falso ideologico in atto pubblico.

Condotte illecite:

- Emissione di SDO falsificate ai fini dell'ottenimento di maggiori rimborsi.

IL CODICE ETICO

Rappresenta un insieme di principi comportamentali, adottati spontaneamente dalle Società, riconosciuti, accettati e condivisi, diretti a diffondere, a tutti i livelli aziendali, una solida integrità etica e una forte sensibilità alle leggi e alle regole comportamentali.

CODICE ETICO

PREMESSA

CAPO I DISPOSIZIONI GENERALI

1. Ambito di applicazione e Destinatari
2. Obblighi dei dipendenti

CAPO II PRINCIPI ETICI

3. Principi Etici
- 3.1. Osservanza delle leggi
- 3.2. Imparzialità
- 3.3. Conflitto d'interessi
- 3.4. Trasparenza e affidabilità
- 3.5. Riservatezza
- 3.6. Rispetto della persona e delle risorse umane
- 3.7. Professionalità

CAPO III REGOLE COMPORTAMENTALI

4. Correttezza e trasparenza delle informazioni societarie
5. Antiriciclaggio
6. Omaggi
7. Comportamenti vietati sul lavoro
8. Sicurezza sul lavoro
9. Comunicazioni all'esterno
10. Rapporti con i fornitori
11. Rapporti con Istituzioni e Pubbliche Amministrazioni
12. Rapporti con organizzazioni politiche e sindacali
13. Rapporti con la stampa e comunicazioni esterne
14. Tutela della concorrenza

CAPO IV DISPOSIZIONI SANZIONATORIE

15. Violazioni e conseguenze sanzionatorie

CAPO V DISPOSIZIONI FINALI

16. Approvazione del Codice Etico e relative modifiche

EUROFIDI S.p.A.
Via Perugia, 56
10152 Torino

EUROCONS - C
AZIENDALE
Via Perugia, 56
10152 Torino

I SOGGETTI DESTINATARI DEL CODICE ETICO



IL CODICE ETICO

Al fine di assicurare attuazione alle norme del codice è opportuno:

- Garantire un adeguato supporto interpretativo ove richiesto;
- Prevedere un apparato sanzionatorio ed i relativi meccanismi di attivazione connessi ad un sistema per la raccolta di segnalazioni delle violazioni del codice .

EUROFIDI S.p.A. Via Perugia, 56 10152 Torino	EUROCONS - C AZIENDALE Via Perugia, 56 10152 Torino
	PREMESSA
	CAPO I DISPOSIZIONI GENERALI
	1. Ambito di applicazione e Destinatari
	2. Obblighi dei dipendenti
	CAPO II PRINCIPI ETICI
	3. Principi Etici
	3.1. Osservanza delle leggi
	3.2. Imparzialità
	3.3. Conflitto di interessi
	3.4. Trasparenza e affidabilità
	3.5. Riservatezza
	3.6. Rispetto della persona e delle risorse umane
	3.7. Professionalità
	CAPO III REGOLE COMPORTAMENTALI
	4. Correttezza e trasparenza delle informazioni societarie
	5. Anticorruzione
	6. Conflitti
	7. Comportamenti vietati sul lavoro
	8. Sicurezza sul lavoro
	9. Comunicazioni all'esterno
	10. Rapporti con i fornitori
	11. Rapporti con istituzioni e Pubbliche Amministrazioni
	12. Rapporti con organizzazioni politiche e sindacali
	13. Rapporti con la stampa e comunicazioni esterne
	14. Tutela della concorrenza
	CAPO IV DISPOSIZIONI SANZIONATORIE
	15. Violazioni e conseguenze sanzionatorie
	CAPO V DISPOSIZIONI FINALI
	16. Approvazione del Codice Etico e relative modifiche



La violazione dei doveri contenuti nel codice è fonte di responsabilità disciplinare

LA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI

PERSONALI



Che cos'è la Privacy?



Il termine, inizialmente riferito alla sfera della vita privata, negli ultimi decenni ha subito un'evoluzione estensiva, arrivando ad indicare il **DIRITTO DELLA PERSONA SUI PROPRI DATI PERSONALI**.

Quindi, il significato odierno di privacy è relativo al **DIRITTO DELLA PERSONA DI CONTROLLARE CHE LE INFORMAZIONI CHE LA RIGUARDANO VENGANO TRATTATE** da altri solo in caso di necessità ed in modo corretto.

Principali Definizioni del Regolamento Europeo

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. «interessato»)



Identificabilità

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un dato come:

il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Particolari Categorie di Dati e Dati Giudiziari

Particolari Categorie di Dati (art. 9 Regolamento)

Dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati Giudiziari (art. 10 Regolamento)

Dati relativi alle condanne penali ed ai reati nonché connesse a misure di sicurezza.

Trattamento dei dati personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate ai dati personali o insiemi di dati personali, come:

- la raccolta, registrazione, organizzazione, strutturazione, conservazione
- l'adattamento o la modifica, l'estrazione, la consultazione, l'uso
- la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
- il raffronto o l'interconnessione
- la limitazione, la cancellazione, la distruzione.

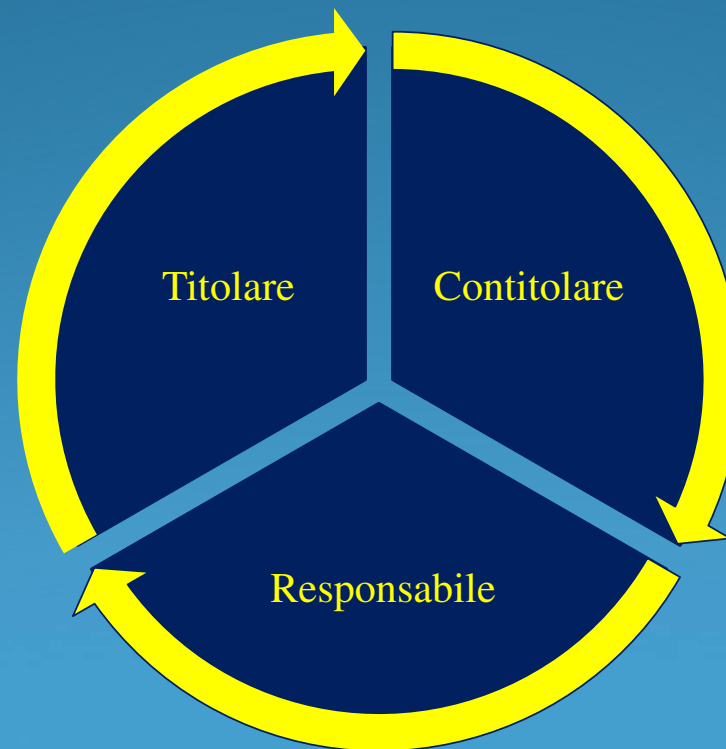
Ambito di applicazione materiale

Il presente regolamento si applica al **TRATTAMENTO** manuale o automatizzato dei **DATI PERSONALI**



PERSONE FISICHE, NON GIURIDICHE

Gli attori ed i ruoli



Il Titolare del trattamento

La **Persona fisica o Giuridica, l'Autorità Pubblica, il servizio od altro organismo** che (singolarmente o insieme ad altri):

DETERMINA le **FINALITA'** ed i **MEZZI** del trattamento di dati personali



Compiti del Titolare

- **adozione misure tecniche ed organizzative** per garantire un livello di sicurezza adeguato al rischio (es. pseudonimizzazione, cifratura, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure adottate);
- **adozione del Registro delle attività di trattamento;**
- **nomina del DPO** nei casi previsti dal Regolamento;
- **notifica delle violazioni** dei dati personali;
- effettuazione di **valutazioni di impatto;**
- **procedure** tempestive di **rilevamento data breach;**
- **essere «accountable»:** dimostrare la conformità del trattamento con misure adeguate, tecniche ed organizzative, procedure, policy, adozione del registro del trattamento.

Poteri del Titolare

Il Titolare **decide** su:

- **Finalità** e mezzi (cfr. art. 4.7)
- **Profilo della sicurezza** (cfr. art. 24.1)

Può **individuare all'interno della sua struttura ruoli subordinati** (dipendenti e collaboratori) a cui affidare operazioni di trattamento, **istruendoli adeguatamente** (Soggetti Autorizzati) e può **esternalizzare attività di trattamento** designando Responsabili di trattamento ed istruendoli adeguatamente.

Il Responsabile del trattamento

La **Persona Fisica o Giuridica, l'Autorità Pubblica, il servizio od altro organismo** che **tratta** dati personali per conto del titolare del trattamento.

Responsabilità del titolare

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che **presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (art. 28).



Nomina del Responsabile del trattamento ex art. 28 del GDPR

I trattamenti effettuati da parte di un Responsabile per conto del Titolare sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati Membri che stipuli:

- la **materia** disciplinata
- la **durata** del trattamento
- la **natura** e le **finalità** del trattamento
- il **tipo di dati** personali
- le **categorie di interessati**
- gli **obblighi** ed i **diritti del titolare** del trattamento



Soggetti Autorizzati al trattamento (ex incaricati)

- Persona fisica (dipendenti e collaboratori) **autorizzata a compiere operazioni di trattamento** dal Titolare o dal Responsabile
- **Chiunque** agisca sotto l'autorità del titolare o del responsabile del trattamento, e che **abbia accesso** ai dati personali **NON può** trattare tali dati **SE NON E' ISTRUITO** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
- la sua **designazione** deve risultare **per iscritto** individuando puntualmente l'area di trattamento consentito (ex art. 29 del GDPR).



Principali compiti del soggetto autorizzato

- Deve **accedere** solo alle **banche dati** cui è **autorizzato**
- Deve **trattare** i dati secondo le **istruzioni impartite** dal titolare o dal responsabile
- Deve **rispettare** le misure tecniche ed organizzative adottate dal titolare



L'autorizzato riceve istruzioni per iscritto nelle quali si prescrive:

- **osservare** scrupolosamente gli **obblighi relativi alla riservatezza**, alla **comunicazione e diffusione** tanto dei dati personali trattati quanto delle credenziali di autenticazione attribuite
- mantenere **segreta la propria credenziale di autenticazione** (la password deve essere composta da almeno 8 caratteri, non deve essere riconducibile a riferimenti personali e deve essere modificata almeno ogni 6 mesi)
- **trattare i dati esclusivamente al fine di adempiere alle obbligazioni nascenti dall'incarico conferito**
- **custodire i dati - in particolare quelli «particolari» - mediante l'adozione di misure di sicurezza** disposte dal titolare al fine di evitare la perdita, la distruzione o l'accesso non autorizzato da parte di terzi

L'autorizzato riceve istruzioni per iscritto nelle quali si prescrive:

- in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, verificare che non vi sia la possibilità da parte di terzi (anche se colleghi o comunque appartenenti alla struttura) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, mediante supporto cartaceo od informatico

salva schermo
con password

ritiro cartelle di lavoro su carta in cassetto



Sistema disciplinare

In caso di mancato rispetto delle istruzioni impartite dal Titolare del trattamento o delle misure di sicurezza adottate



verranno comminate adeguate sanzioni disciplinari a prescindere dall'effettiva realizzazione di un fatto-reato nonché dalla causazione di qualsiasi danno all'ente.





Principi applicabili al trattamento dei Dati Personali





Principali Diritti dell'Interessato (art. 12-22 del Regolamento)



DATA BREACH

(violazione dei dati personali)

Qualsiasi **violazione di sicurezza** che **comporta accidentalmente** (es. smarrimento fascicoli, furto pc) **o in modo illecito** (es. attacco informatico):

la **distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali** trasmessi, conservati o comunque trattati.

Quali rischi per l'interessato?

- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza o qualsiasi altro danno economico e sociale significativo alla persona fisica interessata



Alcuni possibili esempi di Data Breach



Alcuni esempi possibili:

- accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware etc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.



Alcuni possibili esempi di Data Breach

Anche una **perdita temporanea di disponibilità** può costituire una violazione di dati personali:

Esempio

In ambito ospedaliero, se i dati clinici cruciali di un paziente risultano non disponibili, anche solo momentaneamente, questa situazione può mettere a rischio i diritti e le libertà del singolo; un intervento chirurgico, ad esempio, può essere cancellato a rischio della vita.



UK: clinica per l'identità di genere divulga per errore quasi 2000 indirizzi email

Una clinica per l'identità di genere vicino Londra ha inviato una e-mail per un concorso d'arte ai propri pazienti, mettendo in CC quasi 2000 indirizzi email. Accortasi dell'errore, la clinica non è più riuscita ad annullare l'invio.

La violazione, che verrà notificata al Garante UK, è un esempio di data breach imputabile a un errore umano all'interno all'organizzazione.



In caso di VIOLAZIONE DATI PERSONALI (C.D. DATA BREACH)

- Segnalare al titolare del trattamento (o al proprio responsabile gerarchico) eventuali situazioni di rischio per la sicurezza dei dati di cui è venuto a conoscenza (es. violazione della password, il tentativo di accesso non autorizzato ai sistemi)

- **AVVISARE TEMPESTIVAMENTE IL TITOLARE (O IL PROPRIO RESPONSABILE GERARCHICO) QUALORA SI ABBIA EVIDENZA O ANCHE SOLO IL SOSPETTO CHE SIA IN CORSO UNA VIOLAZIONE DI DATI (C.D. «DATA BREACH»)**



Notifica DATA BREACH (art. 33 del Regolamento)

Il **Titolare del trattamento**, non appena viene a conoscenza di un'avvenuta violazione di dati personali, **DEVE NOTIFICARE LA VIOLAZIONE AL GARANTE** ove possibile (e nei casi previsti dall'art. 34 anche all'interessato – rischio elevato per diritti e libertà), **entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che non sia in grado di dimostrare che**, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

Il Titolare del trattamento **DOCUMENTA** tutte le violazioni (a prescindere dalla notifica al Garante) di **dati personali**, ad esempio predisponendo un apposito registro.



Responsabilità connesse al trattamento dei dati personali

Il mancato rispetto degli obblighi previsti dal Regolamento e dal Codice della Privacy

ESPONE IL TITOLARE, IL RESPONSABILE ED I SINGOLI SOGGETTI AUTORIZZATI A RISCHI SUL PIANO DELLE RESPONSABILITA' E DELLE SANZIONI A LIVELLO



CIVILE

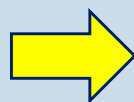
AMMINISTRATIVO

PENALE



Trattamento dei dati in ambito sanitario

Il trattamento dei dati personali in ambito sanitario è disciplinato dal:



Titolo V – Artt. 75 – 92 del Nuovo Codice della Privacy (D.lgs. n. 196/03 così come modificato dal D.lgs. n. 101/2018)

Provvedimenti adottati dal Garante per la protezione dei dati personali in ambito sanitario



Provvedimento n. 55 del 7 marzo 2019:

«Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario»

Trattare «categorie particolari di dati» in ambito sanitario è sempre vietato, **TRANNE CHE PER:**



- a) Motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett.g) del Regolamento ed art. 2 sexies del Codice);
- b) Motivi di interesse pubblico nel settore della sanità pubblica (es. emergenze sanitarie – art. 9, par. 2, lett. i) del Regolamento);
- c) **Finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale** ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura», ex art. 9, par. 2, lett. h) del Regolamento).

Provvedimento n. 55 del 7 marzo 2019

I TRATTAMENTI
NECESSARI
AL PERSEGUIMENTO DI
SPECIFICHE
FINALITA' DI CURA, ossia:

ESSENZIALI PER IL
RAGGIUNGIMENTO DI UNA O
PIU' FINALITA'
DETERMINATE ED
ESPLICITAMENTE
CONNESSE ALLA CURA DELLA
SALUTE

EFFETTUATI DA O SOTTO LA
RESPONSABILITA' DI UN
PROFESSIONISTA SANITARIO
SOGGETTO AL SEGRETO
PROFESSIONALE O DA ALTRA
PERSONA ANCH'ESSA
SOGGETTA ALL'OBLIGO DI
SEGRETEZZA



NON RICHIEDONO
IL CONSENSO
DELL'INTERESSATO

Provvedimento n. 55 del 7 marzo 2019



Adobe Acrobat
Document



**IL CONSENSO
E' SEMPRE
NECESSARIO**
PER I TRATTAMENTI
ATTINENTI IN SENSO
LATO ALLA CURA
E
**NON STRETTAMENTE
NECESSARI**

ESEMPI

CONSULTAZIONE DEL
**FASCICOLO SANITARIO
ELETTRONICO** (D.L. 18/10/12 n.
179, art. 12, co.5)

CONSEGNA DEL **REFERTO
ONLINE** (DPCM dell'8/8/13, art.5)

DOSSIER SANITARIO (Linee
Guida del 4 giugno 2015)



Regione Piemonte,
Prot. 25775/A1416B del
12/12/18: «le soluzioni
aziendali dovranno
acquisire
preventivamente (prima
dell'atto di refertazione)
l'eventuale **volontà**
manifestata dal **paziente**
di **alimentare** il proprio
fascicolo sanitario in
modalità oscurata.



Provvedimento n. 55 del 7 marzo 2019



I tempi di conservazione della documentazione sanitaria non sono stati modificati dalla disciplina sulla protezione dei dati personali e rimangono pienamente in vigore.

Ad esempio:

- le **Cartelle cliniche, unitamente ai relativi referti**, vanno conservate illimitatamente (Circolare del Ministero della Sanità del 19 dicembre 1986 n. 900)
- la **documentazione iconografica radiologica** deve essere conservata per un periodo non inferiore a 10 anni (art. 4, d.m. 14 febbraio 1997).



Sanzioni applicate in ambito sanitario



Il Caso dell'Ospedale dell'Aia

Un'elevata **sanzione, pari a 460 mila euro**, è stata comminata dal Garante privacy olandese all'ospedale di Haga, situato a L'Aia,
per un'insufficiente protezione dei file dei pazienti.



La violazione dell'art. 32 del GDPR è stata rilevata quando è emerso che decine di membri del personale ospedaliero avevano controllato le cartelle cliniche di un noto personaggio olandese, star di un reality televisivo, senza necessità, in quanto non coinvolti nella terapia del paziente.

Per spingere l'ospedale a migliorare la sicurezza dei file dei pazienti, il Garante olandese ha ingiunto all'ospedale l'implementazione di adeguate misure di sicurezza entro il 2 ottobre 2019, pena il pagamento di 100 mila euro ogni due settimane per un massimo di 300 mila euro.

Il Caso dell'Azienda Sanitaria Locale di Alessandria

Un'attività di controllo presso l'Ospedale Santo Spirito di Casale Monferrato quale presidio ospedaliero dell'Azienda Sanitaria Locale di Alessandria ha consentito di accertare che l'Azienda in oggetto ha effettuato, quale titolare, un trattamento di dati personali attraverso il dossier sanitario senza che, alla data degli accertamenti ispettivi effettuati in data 29 e 30 novembre 2017 (quindi prima della data di piena applicazione del Regolamento) fosse resa un'idonea informativa e raccolto uno specifico consenso degli interessati.



E' stata comminata una sanzione pari a 16.000 Euro (ai fini della determinazione della sanzione si è tenuto conto della normativa vigente all'epoca dei fatti e, dunque, del vecchio Codice della Privacy).

Accesso indebito al Dossier Sanitario

Gli accessi indebiti hanno riguardato dati sanitari di dipendenti in cura presso un'azienda ospedaliera. In un caso, l'accesso era stato effettuato con le credenziali di un medico che aveva lasciato incustodita la propria postazione; negli altri due casi uno specializzando ed un tecnico radiologo erano entrati nel dossier sanitario dei loro colleghi.

In tutti e tre gli episodi risulta accertato, per stessa ammissione dell'azienda ospedaliera, che gli accessi erano stati effettuati non per erogare prestazioni mediche, ma per esclusive ragioni personali, descritte dall'azienda come «mera curiosità».



Gli accertamenti svolti dal Garante hanno evidenziato che le misure tecniche ed organizzative adottate dall'ospedale, a tutela del dossier sanitario aziendale, non si erano dimostrate idonee ad assicurare un'adequata tutela dei dati personali dei pazienti ed a proteggerli da trattamenti non autorizzati, determinando così un trattamento illecito di dati.

E' stata comminata una sanzione pari a 30.000 Euro.

Uso Illecito dei Dati degli accertamenti medici



Il Garante ha ritenuto **illecito** il trattamento effettuato da un'azienda sanitaria che ha messo a disposizione di una società che fornisce apparecchiature per l'alta diagnostica le immagini Tac dei pazienti determinando così una «**comunicazione di informazioni**» **sulla salute di alcuni pazienti identificati in assenza di un'adeguata base normativa.** Parimenti illecito è stato ritenuto il trattamento svolto dalla società in questione.

La designazione della stessa come «responsabile del trattamento» da parte dell'azienda sanitaria non giustifica l'acquisizione delle immagini della Tac.

Le operazioni eseguite perseguono, infatti, finalità proprie della società (partecipazione alla gara e difesa in giudizio) non riconducibili a quelle per le quali era stata designata **responsabile. Tra queste rientrano, ad esempio, le attività di manutenzione per garantire l'efficienza dell'apparecchiatura e la qualità delle immagini della Tac.**

Il Garante rilevati gli illeciti amministrativi svolti dall'azienda sanitaria e dalla società ha avviato i relativi procedimenti sanzionatori.

Le ultime istruttorie concernenti l'erronea comunicazione dei dati dei pazienti a terzi (conclusesi con ordinanza di ingiunzione in data 27/01/2021)

- 1) Un ospedale toscano ha ricevuto la sanzione pecuniaria di Euro 10.000 per aver spedito, a mezzo posta, al paziente sbagliato, una relazione medica contenente informazioni sulla salute e sulla vita sessuale di un'altra coppia, a causa di un errore nell'imbustamento del documento.
- 2) Un ospedale emiliano ha ricevuto un'analoga sanzione per aver consegnato a dei pazienti cartelle cliniche contenenti dati e referti riferibili ad altre persone, incluso un minore.

In entrambi i casi le sanzioni sono state calcolate tenendo conto del fatto che:

- le strutture sanitarie hanno immediatamente dimostrato un elevato grado di cooperazione con il Garante;
- gli episodi sono risultati isolati e non volontari;
- le strutture hanno non solo cercato di rimediare, in quanto possibile, al danno causato, ma anche pianificato ulteriori misure tecniche e organizzative per cercare di ridurre al minimo l'occorrenza di errori umani.

Le ultime istruttorie concernenti l'erronea comunicazione dei dati dei pazienti a terzi (conclusesi con ordinanza di ingiunzione in data 27/01/2021)

L'ultimo caso, più grave dei precedenti (sanzione di 50.000 Euro), concerne una AUSL dell'Emilia-Romagna, dove una paziente aveva esplicitamente **richiesto che nessun soggetto terzo (neppure i familiari) fosse informato sul suo stato di salute** e chiesto espressamente di essere contattata solo tramite il numero di telefono che veniva inserito all'interno della cartella clinica. Sennonché **l'infermiera di reparto contattava la paziente utilizzando il numero registrato nell'anagrafe aziendale**, cioè quello del **telefono di casa, parlando così con il marito** e comunicandogli **la struttura e reparto ospedaliero** dal quale chiamava.

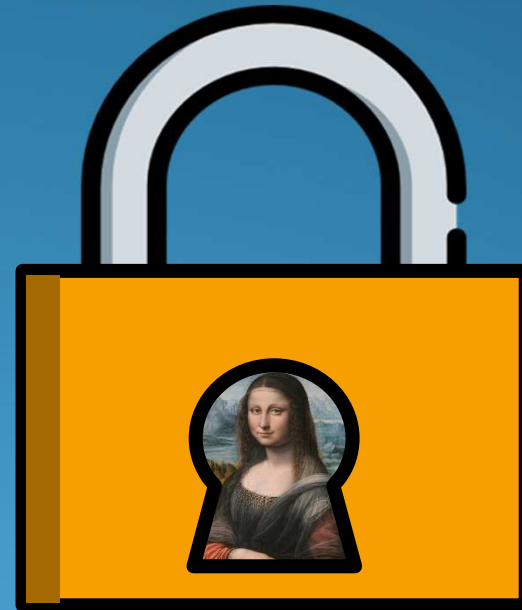
Anche in questo caso, l'Azienda:

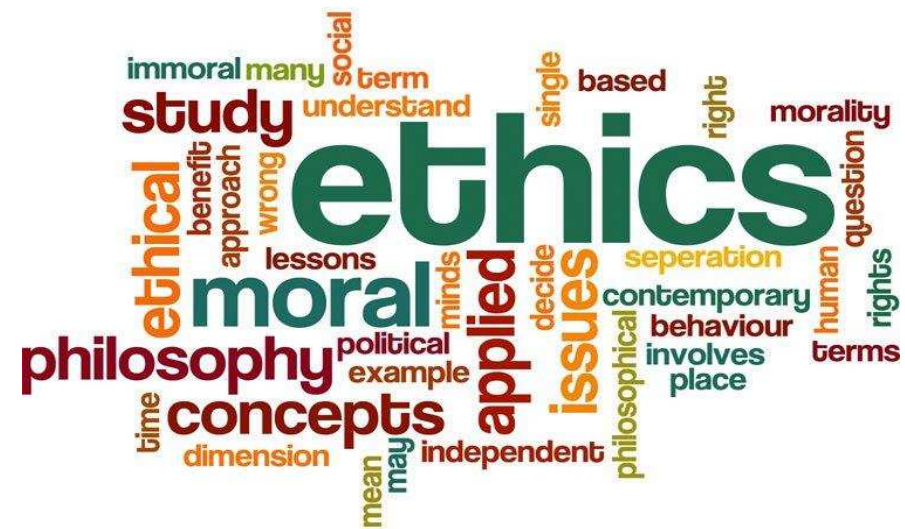
- ha riconosciuto gli errori che hanno causato la violazione;
- si è impegnata ad implementare un sistema informatizzato di gestione dei numeri di telefono dei pazienti ricoverati ed a predisporre una modulistica unica con la quale i pazienti potranno esprimere la loro eventuale volontà di comunicare informazioni sul proprio stato di salute ai terzi, introducendo una specifica policy aziendale.

Il monito dell'Autorità Garante della Protezione dei Dati Personali

Alla luce di questi episodi, il Garante della Privacy ha ricordato che la **disciplina in materia di protezione dei dati personali** prevede, in **ambito sanitario**, che le **informazioni sullo stato di salute dei pazienti possano essere comunicate a terzi solo sulla base di un presupposto giuridico o su indicazione della persona interessata**, previo rilascio di **delega scritta**.

La Privacy è CULTURA





Grazie per l'attenzione