Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

aias
academy
networkaias

I reati informatici previsti nel Decreto Legislativo n. 231/2001 correlati con la ISO 27001

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

BACKGROUND E FINALITÀ DEL DECRETO

D. Lgs. 231/2001

Disciplina la responsabilità amministrativa di persone giuridiche, società ed associazioni per gli illeciti dipendenti da reati commessi nell'interesse o a vantaggio degli enti

Ha introdotto, per la prima volta nel nostro ordinamento, la responsabilità in sede "penale" degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito

Scopo del Decreto

L'AMPLIAMENTO DELLA RESPONSABILITA' MIRA A COINVOLGERE NELLA PUNIZIONE DI TALUNI ILLECITI PENALI IL PATRIMONIO DEGLI ENTI, CHE PRIMA NON PATIVANO CONSEGUENZE DALLA COMMISSIONE DI REATI DA AMMINISTRATORI E/O DIPENDENTI A VANTAGGIO DEGLI ENTI STESSI

NATURA DELLA RESPONSABILITÀ

LA RESPONSABILITÀ

Ante D.Lgs. 231/2001	Post D.Lgs. 231/2001
Persone fisiche	***Persone fisiche + Enti***

- Si introduce una forma di **responsabilità a carico di società ed altri enti associativi**, di natura formalmente amministrativa, ma **sostanzialmente penale**
  (La responsabilità è accertata e le sanzioni sono irrogate nell'ambito e con le regole del processo penale)
- La responsabilità dell'ente si aggiunge a quella della persona fisica che ha commesso il reato sulla base di specifica imputazione formulata a carico dell'ente.

- **La responsabilità penale è riferibile solo alle persone fisiche** e non può essere imputata ad un ente o ad una società, siano essi dotati oppure privi di personalità giuridica
- Dei reati commessi dai soggetti appartenenti all'ente rispondono penalmente solo tali soggetti e la persona giuridica ha solo una obbligazione civile di garanzia per il pagamento di sanzioni pecuniarie in caso di insolvenza del reo.

PRESUPPOSTI DELLA RESPONSABILITÀ

L'ENTE RISPONDE PER I REATI COMMESSI

- **da persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale**
- **da persone che esercitano anche di fatto, la gestione ed il controllo dell'ente**

c.d. "soggetti apicali"

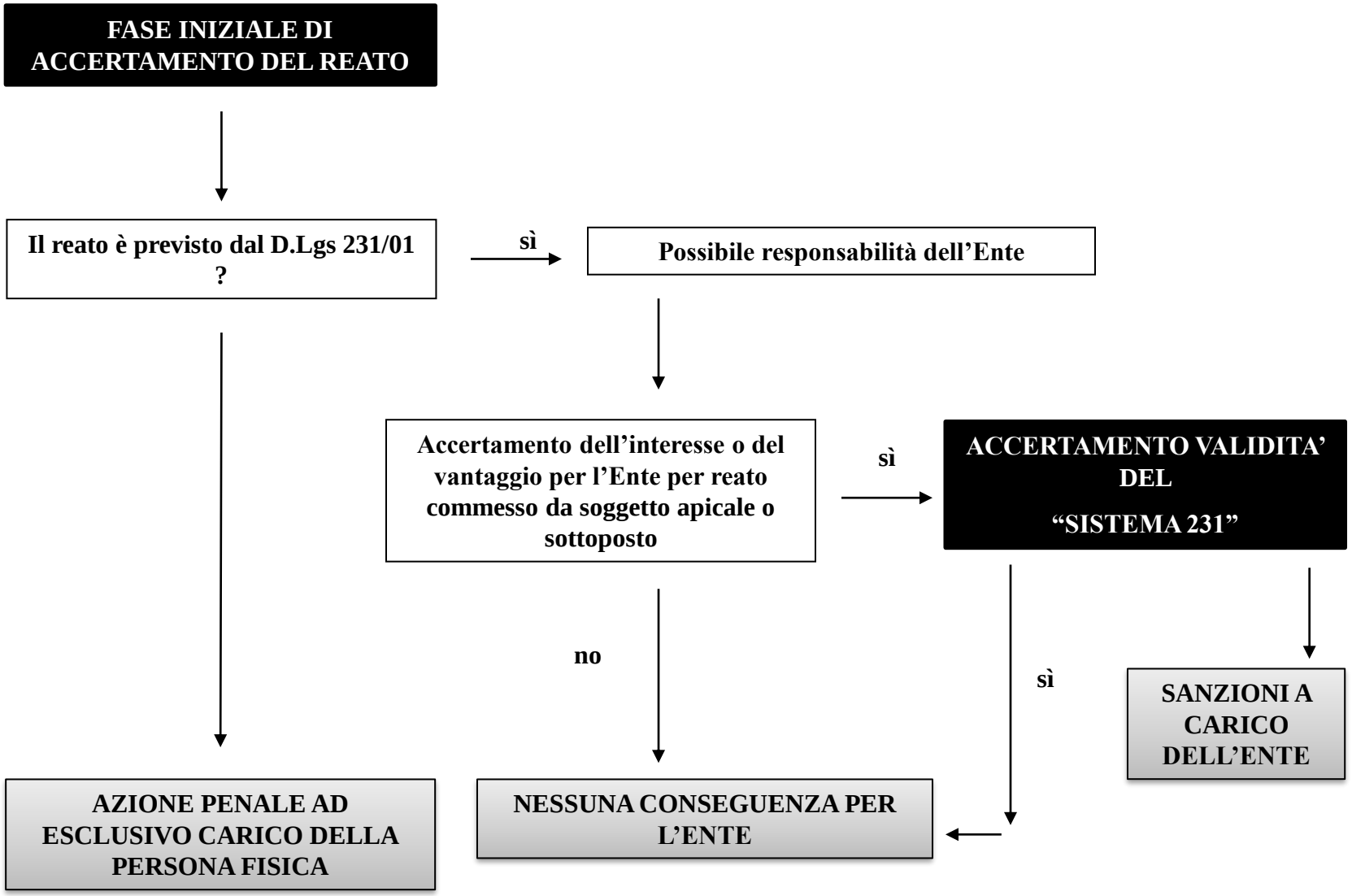
- **da persone sottoposte al controllo o alla vigilanza dei predetti**
- **soggetti, nel caso di inosservanza degli obblighi di direzione e vigilanza dei soggetti apicali**

c.d. "sottoposti"

NEL SUO INTERESSE O A SUO VANTAGGIO

L'Ente non risponde se le persone indicate hanno agito nell'interesse esclusivo proprio o di terzi

ACCERTAMENTO DELLA RESPONSABILITÀ



CONDIZIONI PER L'ESENZIONE – ACCERTAMENTO DELLA VALIDITA' DEL SISTEMA 231

ESIMENTE

L'ENTE È ESENTE DA RESPONSABILITÀ SE PROVA:

di avere adottato ed efficacemente attuato, prima della commissione del reato
MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
idonei a prevenire la commissione dei reati della specie di quello verificatosi

che i soggetti che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello

di avere affidato ad un PROPRIO ORGANISMO INTERNO, con autonomi poteri di iniziativa e di controllo, il compito di vigilare sull'efficacia, l'osservanza e l'aggiornamento costante dei modelli

che non via sia stata omessa o insufficiente vigilanza da parte dell'Organismo

Il D.Lgs. 231/01 ha pertanto attribuito *rilevanza giuridica ai modelli organizzativi, di gestione e di controllo*, sollecitando le società ad un attento esame dei meccanismi formali e sostanziali che regolamentano la loro attività

TIPOLOGIA DI SANZIONI

SANZIONI APPLICABILI

➡ **SANZIONI INTERDITTIVE**

Applicabili solo nei casi espressamente previsti

➡ **SANZIONI PECUNIARIE**

Sempre applicabili

➡ **CONFISCA del prezzo o del profitto del reato**

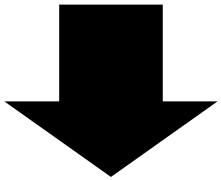
È sempre disposta con la sentenza di condanna

➡ **PUBBLICAZIONE DELLA SENTENZA**

Può essere disposta quando viene applicata una sanzione interdittiva

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Legge n. 48/2008 di ratifica della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23 Novembre 2001



INTRODUZIONE ART. 24 BIS NEL D.LGS. N. 231/2001

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

DUE TIPOLOGIE DI REATI RILEVANTI AI FINI DEL D.LGS. 231/2001

A) I REATI PROPRIAMENTE INFORMATICI

B) I REATI DI FALSO COMMESSI MEDIANTE L'UTILIZZO DI (O SU) DOCUMENTI/DATI INFORMATICI

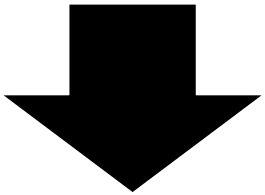
DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

A) I REATI PROPRIAMENTE INFORMATICI

- Art. 615 ter c.p. (Accesso abusivo ad un sistema informatico o telematico)
- Art. 617 quater c.p. (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)
- Art. 617 quinquies c.p. (Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)
- Art. 635-bis c.p. (Danneggiamento di informazioni, dati e programmi informatici)
- 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)
- Art. 635-quater c.p. (Danneggiamento di sistemi informatici o telematici)
- Art. 635-quinquies c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità)
- Art. 615 quater c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)
- Art. 615-quinquies c.p. (Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

B) I REATI DI FALSO COMMESSI MEDIANTE L'UTILIZZO DI (O SU) DOCUMENTI/DATI INFORMATICI

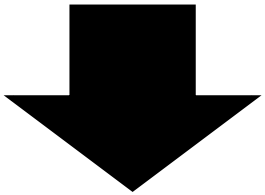


- Art. 491 bis c.p. (Documenti informatici)
- 640 quinquies c.p. (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

in cui viene punita la violazione dell'integrità dei documenti informatici e della loro gestione attraverso la falsificazione di firma digitale (elettronica)

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA



Il 20 novembre 2019 è stata pubblicata in Gazzetta Ufficiale la Legge n. 133/2019 di conversione del Decreto Legge n. 105/2019, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica«, a sua volta entrato in vigore il 21 settembre 2019. Il citato provvedimento normativo ha introdotto una serie di misure atte ad assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di interesse collettivo necessari allo svolgimento di funzioni o alla prestazione di servizi essenziali per lo Stato.

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

Le categorie menzionate dei reati informatici sono in realtà spesso interconnesse tra loro. La prevenzione dei reati stessi è particolarmente difficile e complessa, soprattutto perché non necessitano di elaborati processi di gestione/organizzazione aziendale, né del coinvolgimento di un elevato numero di soggetti, atteso che, solitamente, l'attività fraudolenta è perpetrata da un singolo soggetto che sfrutta le proprie conoscenze informatiche e la larghezza delle maglie della rete di protezione cibernetica aziendale. Con il proliferare di episodi di violazione dei sistemi informativi aziendali perpetrati da parte di *hacker* anonimi sempre più esperti, i vertici aziendali hanno dovuto prendere coscienza della necessità di provvedere non solo alla difesa della rete aziendale interna, ma anche ad un'azione di tutela rivolta verso l'esterno.

L'occasione privilegiata per attuare questa protezione a doppio raggio d'azione dell'azienda si è rivelata proprio la redazione o l'implementazione di un efficace **Modello di Organizzazione Gestione e Controllo (Modello 231)**

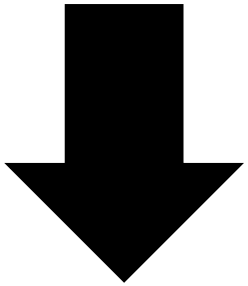
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Nell'ambito dell'attività di predisposizione del Modello 231, la gestione dei rischi legati al mondo dell'informatica si fonda principalmente su tre pilastri:

- la **Prevenzione**, che viene normalmente attuata attraverso la previsione di specifiche misure di sicurezza volte a ridurre la possibilità che vengano commessi reati all'interno della rete aziendale;
- **Controlli**: vengono effettuati attraverso l'introduzione di presidi di controllo ad hoc, finalizzati a supervisionare la gestione ed il funzionamento dei diversi ambiti aziendali condizionati dall'uso di internet e di *device* tecnologici;
- la **Formazione**, consistente nella diffusione di una cultura aziendale in materia informatica attraverso la formazione del personale e la responsabilizzazione di alcune figure

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

A livello di prevenzione, è importante che ogni azienda si doti di apposite **regole comportamentali e di sicurezza** per gli **utenti**



sia INTERNI che ESTERNI

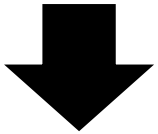
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Quanto agli <u>UTENTI INTERNI</u> risulta fondamentale innanzitutto definire i livelli di accesso in base alla confidenzialità delle informazioni ed alla responsabilità di ogni soggetto. Si tratta, in particolare, di adottare una **policy di sicurezza del sistema informatico**, che regolamenti in maniera strutturata l'accesso ai documenti ed alle informazioni aziendali ed il loro utilizzo, **che dovrebbe contenerne quanto meno le seguenti previsioni:**

- **la protezione da software pericoloso ricorrendo all'uso di antivirus ed al loro monitoraggio/aggiornamento costante**;
- **i back-up periodici delle informazioni** in possesso all'azienda e dei software dalla stessa utilizzati;
- **la protezione dello scambio di informazioni** attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi (ad esempio regolamentando l'uso di dispositivi removibili quali USB);
- **la tracciatura delle attività eseguite sulle applicazioni**, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
- **la verifica periodica dei log che registrano le attività degli utilizzatori**, le eccezioni e gli eventi concernenti la sicurezza;
- **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;

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Per quanto riguarda i controlli, l'impresa deve provvedere a nominare un amministratore di sistema, un esperto di IT che si occupi del monitoraggio dei sistemi informativi aziendali e che risponda a tutte le segnalazioni provenienti dalle varie funzioni.



Inoltre, risultano fondamentali la programmazione di **audit interni** da eseguire periodicamente (anche mediante attività di penetrazione ed ingegneria sociale) ed il **controllo costante sui cambiamenti apportati agli elaboratori e ai sistemi**. Tutti gli strumenti e le misure sopra indicate sono estremamente utili anche nella tutela dagli attacchi esterni.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

L'implementazione del Modello 231 ad oggi può infatti rivelarsi uno strumento prezioso ed efficace anche per tutelare l'azienda da eventuali minacce cyber provenienti dall'**ESTERNO**.

L'incremento delle misure di prevenzione e controllo contenute nel Modello anche con strumenti di contrasto a tali fenomeni provenienti dall'esterno, si rivela sempre più vantaggioso per le aziende che vogliono una tutela a 360 gradi e, quindi, una continuità della loro attività.

È importante, dunque, che le aziende non solo prevengano, ma anche **costituiscano un sistema di *disaster recovery* per il trattamento degli incidenti e delle anomalie di qualsiasi tipo relativi alla sicurezza informatica**.

A questo proposito risulta estremamente utile l'introduzione di meccanismi di comunicazione immediata tramite alert automatici che segnalino eventuali episodi di *hackeraggio* e di appropriati canali gestionali per la comunicazione immediata degli incidenti e dei problemi oltre che l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della rispettiva rootcause in modo da poter creare una rete di prevenzione-protezione sempre più ampia e sofisticata.

CERTIFICAZIONE ISO/IEC 27001:2017

Un ulteriore strumento di tutela a livello informatico per il mondo aziendale è poi aderire a standard internazionali, in particolare allo standard ISO 27001 (norma internazionale per i Sistemi di Gestione della Sicurezza delle Informazioni denominata anche SGSI) e, quindi, ottenere la **certificazione ISO/IEC 27001:2017**

La norma internazionale è stata elaborata allo **scopo di fornire i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni.**

CERTIFICAZIONE ISO/IEC 27001:2017

L'obiettivo del nuovo **standard ISO 27001:2017** è proprio la **protezione dei dati e delle informazioni aziendali da minacce di qualsiasi tipo**, allo scopo di assicurarne l'integrità, la riservatezza e la disponibilità e fornire alle società i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una gestione efficace e corretta dei dati sensibili dell'azienda.

L'adesione a tale standard **non è obbligatoria**, ma certamente aiuta le aziende a **contrastare i rischi per la sicurezza**, a proteggere i dati sensibili ed a identificare l'ambito e i limiti dei propri programmi sulla sicurezza.

L'adesione allo standard ISO 27001, unitamente all'implementazione di un Modello 231, adeguato efficace ed idoneo a prevenire la realizzazione dei reati considerati ed alla attività di informazione e **formazione del personale** sia elementi che certamente verranno valutati dalla magistratura ai fini dell'esonero di responsabilità di cui all'art. 6 del D.Lgs. 231/2001.

CERTIFICAZIONE ISO/IEC 27001:2017

L'adesione a tali modelli **non rende** automaticamente l'ente "*compliant*" anche al GDPR e alla normativa Privacy nazionale (D.lgs. 196/2003 novellato dal D.lgs. 101/2018) e neppure esula l'organizzazione da altri adempimenti, se previsti

Tuttavia questi modelli, norme e standard che agiscono in armonia rafforzando ancor di più la tutela dell'Ente sono quindi da considerarsi come efficaci sostegni per la protezione di organizzazioni di qualsivoglia dimensione.

GDPR E ISO 27001

GDPR e ISO 27001 sono due standard di conformità importanti che hanno molti elementi in comune. Entrambi mirano ad **irrobustire la sicurezza dei dati** ed a **diminuire il rischio di violazione dei dati**, ed entrambi necessitano e spingono fortemente verso la creazione di un **sistema organizzato** per assicurare la riservatezza, l'integrità e la disponibilità dei dati sensibili.

Ci sono molte aree in cui ISO 27001 e il GDPR presentano **elementi comuni.**

La maggior parte di esse sono correlate alla sicurezza delle informazioni: la ISO 27001, ad esempio, specifica regole per la protezione dei dati simili a quelle delineate dalla GDPR negli articoli 5, 24, 25, 28, 30 e 32.

GDPR E ISO 27001

I principali **punti cardine in comune** ad entrambi gli standard (a titolo esemplificativo) sono i seguenti:

- **Riservatezza, confidenzialità e integrità dei dati.** Nel GDPR l'articolo 5 specifica i principi generali per l'elaborazione dei dati, come la protezione contro l'elaborazione non autorizzata o non conforme alla legge, la perdita, la distruzione o danni accidentali. Nell'articolo 32 vengono date linee guida più dettagliate, che specificano che le organizzazioni sono tenute ad attuare, operare e mantenere misure tecniche e organizzative per assicurare la sicurezza dei dati, come la crittografia, la resilienza dei sistemi e dei servizi di elaborazione, la capacità di ripristinare la disponibilità dei dati personali tempestivamente e molto altro. Allo stesso modo, molti controlli nella ISO 27001 mirano ad aiutare le organizzazioni a garantire la riservatezza, la disponibilità e l'integrità dei dati. Partendo dalla **clausola 4,** la ISO 27001 richiede alle organizzazioni di identificare i problemi interni ed esterni che potrebbero avere impatto sui programmi di sicurezza. La **clausola 6** richiede loro di determinare i propri obiettivi di sicurezza IT e di creare un programma di sicurezza che li aiuti a raggiungere tali obiettivi. La **clausola 8** stabilisce gli standard per la manutenzione continua del programma di sicurezza e richiede **all'organizzazioni di documentare lo stesso programma per dimostrarne la conformità normativa.**

- **Valutazione del rischio.** Sia la ISO 27001 sia il GDPR richiedono un approccio alla sicurezza dei dati basato sul rischio. L'articolo 35 del GDPR richiede alle aziende di eseguire delle valutazioni dell'impatto sulla protezione dei dati per valutare ed identificare i rischi per i dati delle persone. Queste valutazioni sono obbligatorie prima di intraprendere dei processi ad alto rischio, come il monitoraggio sistematico dei dati estremamente sensibili. La ISO 27001 consiglia, al paragrafo 6.1.2, a tutte le organizzazioni di condurre delle valutazioni accurate del rischio per identificare minacce e vulnerabilità che potrebbero influire sulle attività, e per selezionare delle appropriate misure di sicurezza delle informazioni basate sui risultati della valutazione del rischio (al paragrafo 6.1.3).

- **Conservazione dei registri.** L'**articolo 30** del GDPR richiede alle organizzazioni di conservare dei registri delle loro attività di trattamento, comprese le categorie di dati, le finalità del trattamento e una descrizione generale delle misure tecniche e organizzative rilevanti per la sicurezza. La ISO 27001 afferma che le organizzazioni devono documentare i loro processi di sicurezza, nonché i risultati delle loro valutazioni del rischio di sicurezza e del trattamento del rischio (**clausola 8**). Secondo il **paragrafo A.8**, le attività di informazione devono essere inventariate e classificate, i proprietari di attività devono essere assegnati e le procedure per l'utilizzo di dati accettabili devono essere definite.

GDPR E ISO 27001

Ci sono **molte differenze** tra questi due standard:

il **GDPR** è uno standard completo che fornisce una visione strategica di come le organizzazioni devono garantire la riservatezza dei dati mentre la **ISO 27001** è un insieme di best practice con un'attenzione particolare alla sicurezza delle informazioni e fornisce consigli pratici su come proteggere le informazioni stesse e ridurre le minacce informatiche.

La **ISO 27001** non copre direttamente i seguenti aspetti associati alla privacy dei dati, che sono delineati nel Capitolo 3 del GDPR (**Diritti dell'Interessato**)

- **Consenso: i** responsabili del trattamento dei dati devono dimostrare che le persone interessate hanno acconsentito al trattamento dei loro dati personali (**articoli 7 e 8**). La richiesta di consenso deve essere fornita in un modulo facilmente accessibile, con lo scopo del trattamento dei dati allegato. Gli interessati hanno anche il diritto di revocare il loro consenso in qualsiasi momento;
- **Portabilità dei dati**: le persone hanno il diritto di ottenere e riutilizzare i propri dati personali per i propri scopi tra diversi servizi, nonché di trasmettere tali dati ad un altro titolare senza ostacoli all'usabilità (**articolo 20**);
- **Diritto all'oblio**: le persone hanno il diritto di cancellare i loro dati personali o di interromperne ulteriormente la divulgazione (**articolo 17**);
- **Diritto di limitazione del trattamento**: gli individui hanno il diritto di limitare il modo in cui un'organizzazione utilizza i propri dati personali se i dati sono stati trattati in modo illecito o se l'individuo ne contesta l'accuratezza (**articolo 18**);
- **Diritto di opporsi:** le persone interessate hanno il diritto di opporsi al trattamento dei dati per il marketing diretto, l'esecuzione di compiti legali, o scopi di ricerca e statistiche (**articolo 21**);
- **Trasferimento soggetto a garanzie adeguate:** le organizzazioni devono garantire che i trasferimenti internazionali di dati siano effettuati in conformità con le regole approvate dalla Commissione europea (**articolo 46**).

GDPR E ISO 27001

La conformità alla ISO 27001 **non garantisca la conformità al GDPR**, ma, tuttavia, **ne costituisce una parte importante**.

Le organizzazioni dovrebbero prendere in considerazione la possibilità di perseguire la certificazione ISO 27001 anche per garantire che le loro **misure di sicurezza siano sufficientemente efficaci per proteggere i dati personali**

Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

CONCLUSIONI

-

GRAZIE PER L'ATTENZIONE

mario.valentini@studiopirola.com

LinkedIn