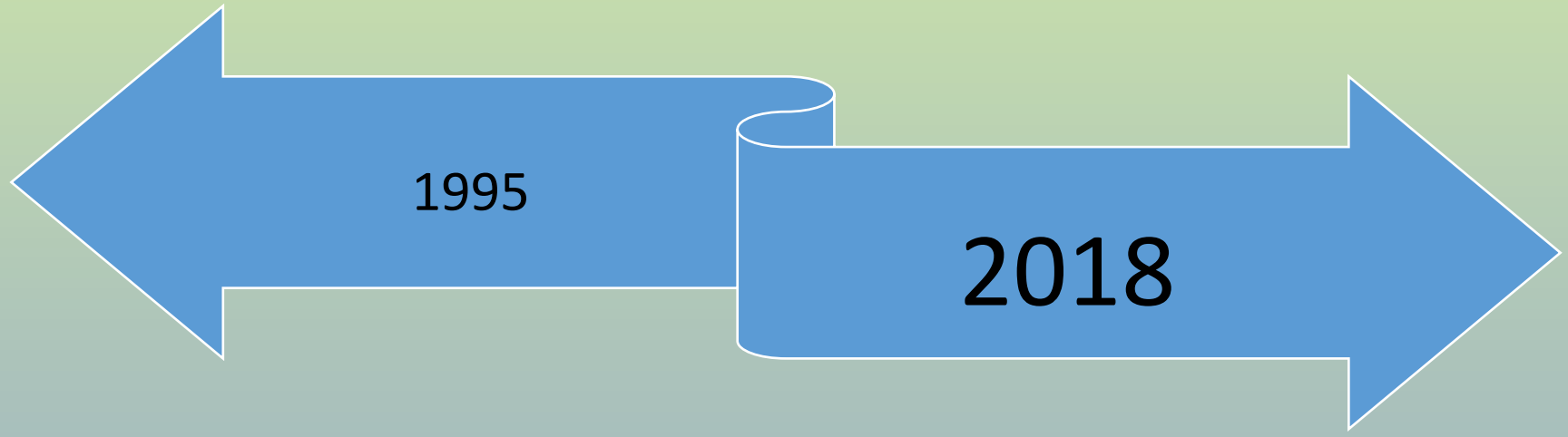
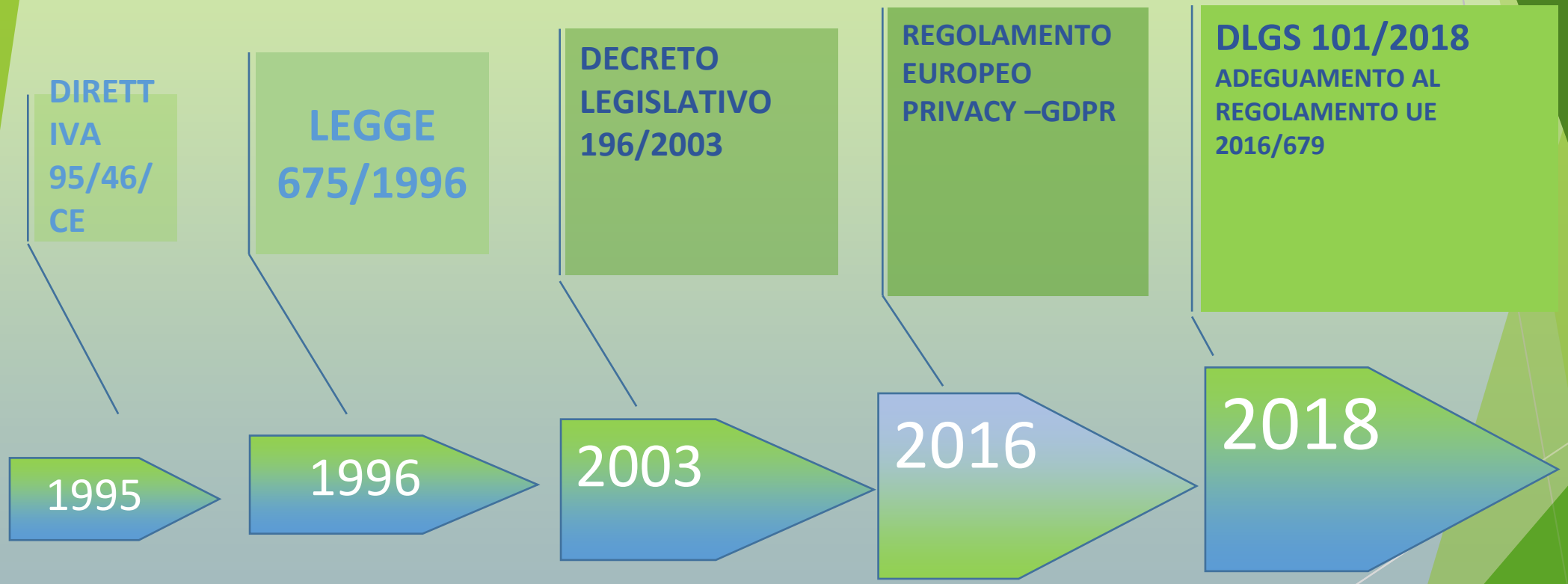
GDPR 679/2016
A un anno dall'entrata in vigore del Nuovo Regolamento Privacy

Evoluzione normativa



Quadro normativo



Quadro normativo

GDPR 679/2016 → news → Dlgs 101/2018

Il Regolamento UE introduce regole chiare stabilendo criteri rigorosi per il trattamento dati personali, trasferimento di questi fuori dall'Ue e violazione degli stessi

Maggior sviluppo Economia Digitale → Maggior circolazione dei dati

Adeguamento alle norme fuori UE → Maggior protezione dei dati

il GDPR <u>non parla</u> di dati sensibili ma di dati particolari:

Dati personali particolari :

<u>Dati identificativi</u> : *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*;

<u>Dati Sensibili</u> *: razza/etnia, sesso, orientamento religioso/politico, appartenenza sindacale, dati relativi alla salute, dati biometrici*

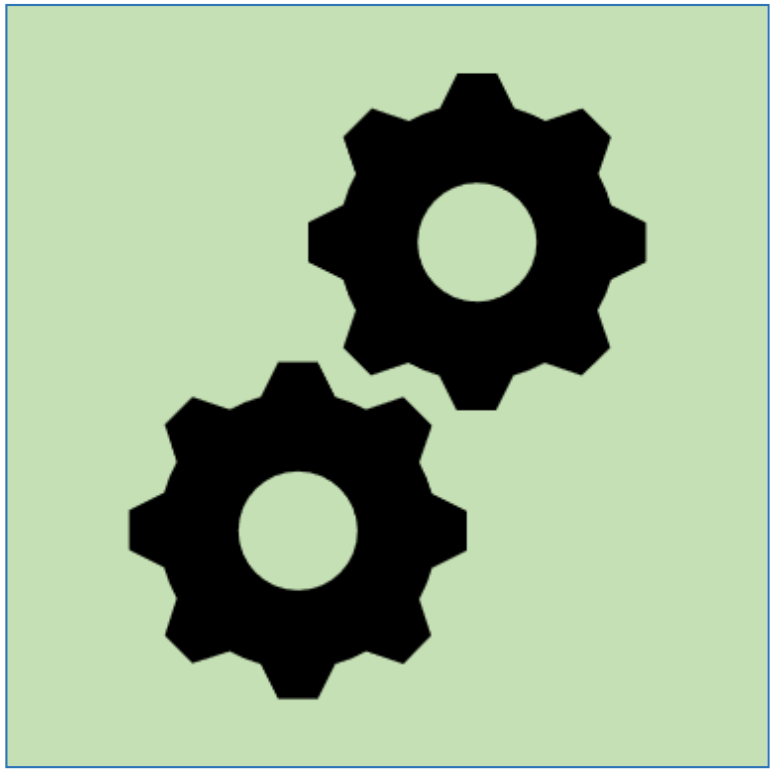
Attori del sistema Privacy

- Titolare del Trattamento dei Dati
- Responsabile del Trattamento dei Dati
- Addetto «Incaricato» del trattamento dei Dati

TITOLARE DEL TRATTAMENTO DATI:

persona fisica o giuridica cui competono tutte le responsabilità in merito ad un corretto trattamento dei dati di :

- -clienti
- -fornitori
- -dipendenti



Il **responsabile del trattamento**

Persona fisica o giuridica che tratta ed elabora i dati personali per conto del titolare del trattamento su **istruzione documentata da parte del titolare** stesso.

Il responsabile del Trattamento può essere:

- Interno (es. dirigente)
- Esterno (es.commecialista/consulente del lavoro…..)

L’ Addetto «incaricato»
al trattamento dei dati

Personale operativo di supporto all’attività del Titolare e/o del Responsabile del Trattamento

Devono avere ricevuto una nomina scritta dal titolare ed una adeguata istruzione

Il DPO - RPD Responsabile Protezione Dati Personali

Il Garante Privacy

Il DPO - RPD Responsabile Protezione Dati Personali

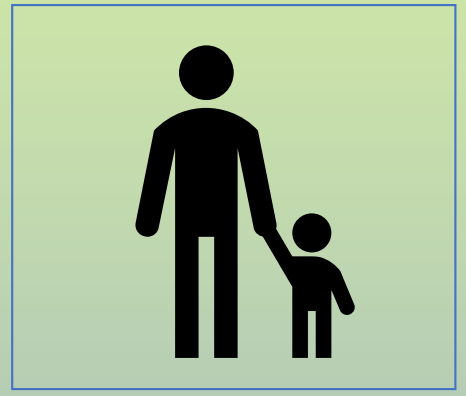
Figura obbligatoria in specifici contesti, con compiti di consiglio, informazione e controllo i n merito agli obblighi legali relativi alla Privacy

Il Garante Privacy

E’ l’autorità amministrativa indipendente istituita dalla legge n. 675 del 31 dicembre 1996, per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

Informative

- Clienti/ fornitori/ dipendenti
  - Sempre per scritto
  - Se i dati trattati sono solo anagrafici non occorre il consenso



PECULIARITA’

Particolare attenzione deve essere posta nei casi di trattamento dati di soggetti minori di 16 anni.
Nei confronti di tali soggetti dovrà essere espresso il consenso genitoriale per scritto a seguito di una informativa semplice, chiara ma dettagliata.
L’età è stata ridotta a 14 anni per i servizi della società dell’informazione.

Nomine

Si tratta di un contratto che dovrà essere espresso per scritto (cartaceo/elettronico) e contenere i seguenti elementi

- OGGETTO – DURATA – NATURA - FINALITA’ del trattamento
- CATEGORIE soggetti interessati e TIPO dei dati oggetto del trattamento
- OBBLIGHI e DIRITTI del Titolare del trattamento

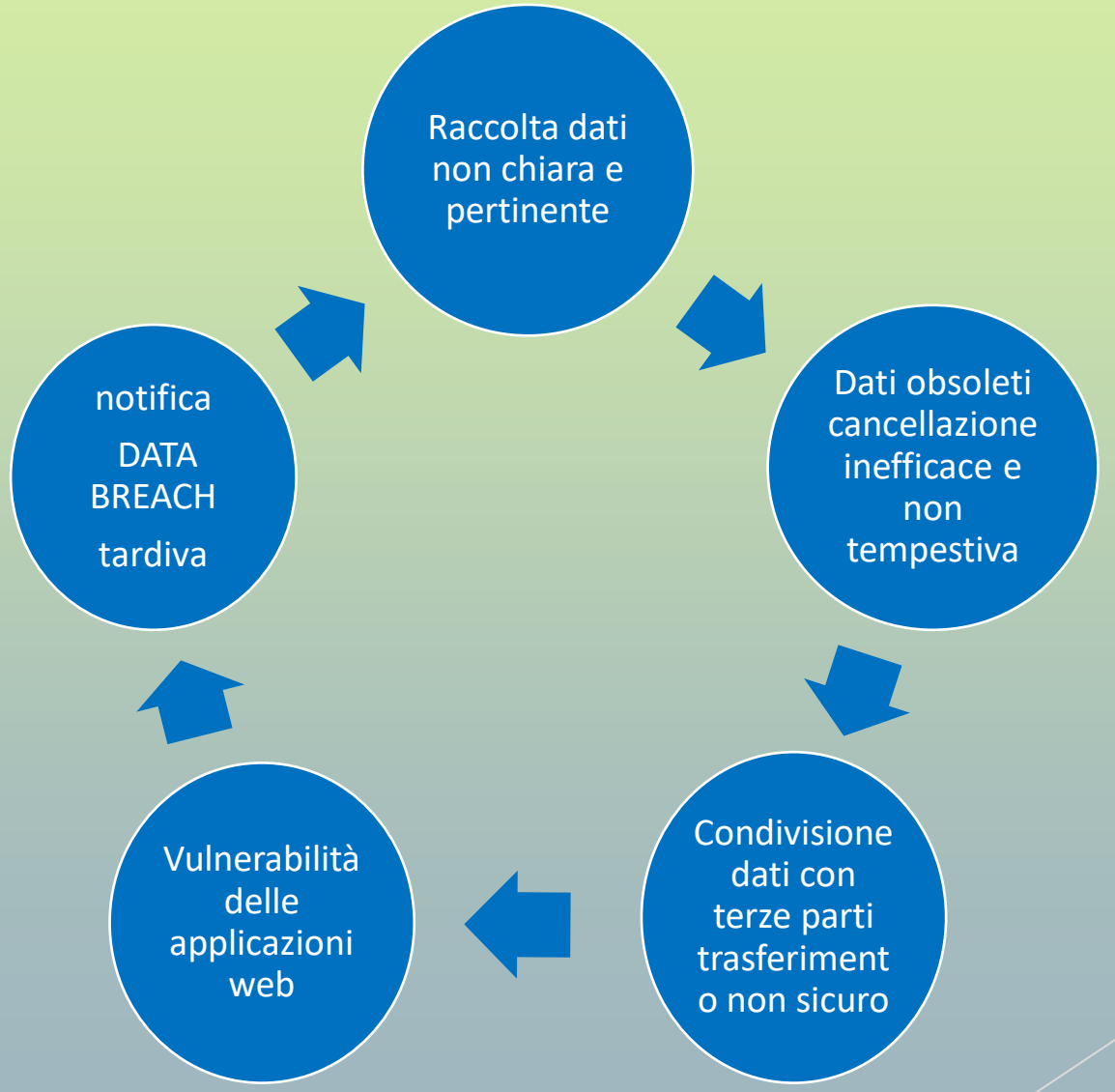
VALUTAZIONE DEI RISCHI E MISURE DI SICUREZZA

Il Regolamento prevede che **il Titolare del trattamento e il Responsabile del trattamento mettano in atto misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio:**

-**REGISTRO DEI TRATTAMENTI**
-DPIA

- principali elementi di *accountability* del titolare,
- strumento idoneo a fornire un quadro aggiornato dei trattamenti
- indispensabile ai fini della valutazione o analisi del rischio e preliminare rispetto a tale attività.

Generalità della valutazione dei rischi



Il registro dei trattamenti

SI tratta di un registro da redigere in forma cartacea o elettronica in cui elencare le attività per le quali è necessario il trattamento dei dati particolari

E' obbligatorio sia per il Titolare che per il Responsabile nei seguenti casi:

- ***esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente*** *(bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);*

- ***liberi professionisti*** *con almeno un dipendente (es. commercialisti, notai, avvocati, fisioterapisti, farmacisti, medici…);*

- ***associazioni, fondazioni e comitati***

- ***il condominio*** *ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).*

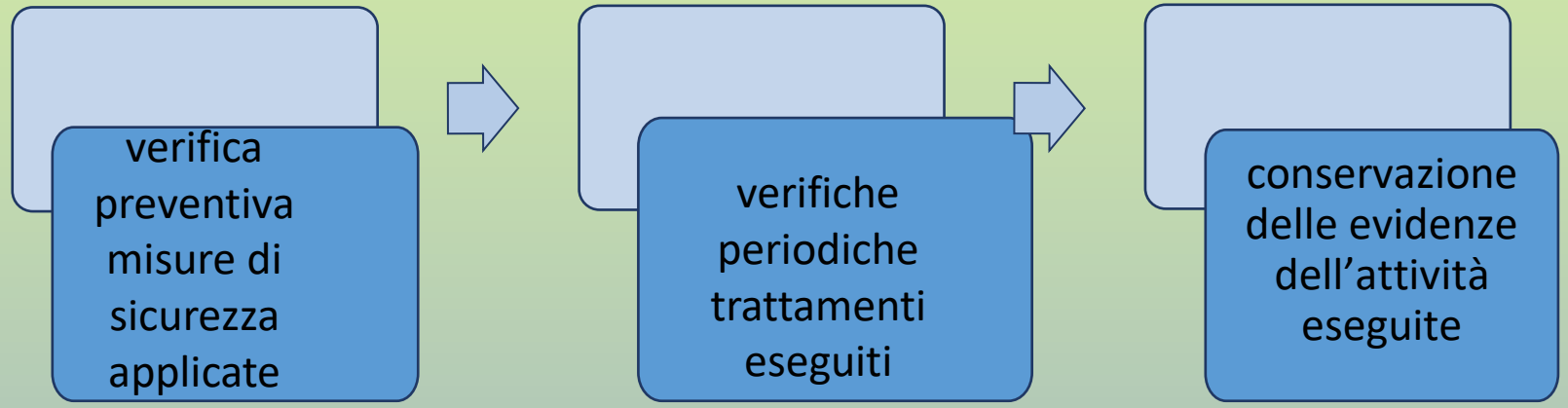
La DPIA - Data Protection Impact Assessment

Per ogni rischio occorre individuare PREVENTIVAMENTE la probabilità dell'evento, nonché la gravità dello stesso

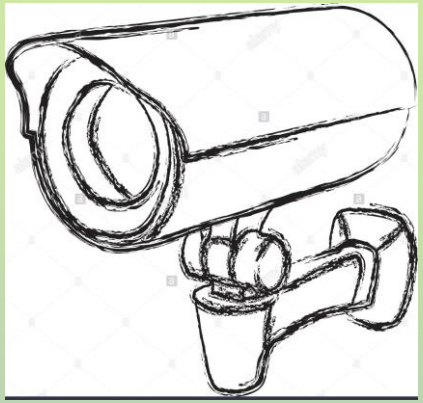
è obbligatoria nei seguenti casi:
-trattamento automatizzato dei dati personali compresa la profilazione
-trattamento su larga scala di metadati
-video sorveglianza
-dati relativi a soggetti vulnerabili (minori/anziani/soggetti con patologie psichiatriche)
-trattamento dati giudiziari o strettamente personali

Il responsabile del trattamento deve assistere il titolare fornendogli ogni informazione necessaria.

come dichiarare “adeguate” le misure di sicurezza adottate



LA VIDEOSORVEGLIANZA



Tutte le immagini riprese da un sistema di videosorveglianza all'interno dello spazio aziendale costituiscono sempre un trattamento di dati personali.

Pertanto il Titolare del Trattamento deve predisporre adeguate misure di tutela e conseguire il consenso d parte dei soggetti interessati l trattamento .

SANZIONI

La violazione di disposizioni in materia di controlli distanza è punibile con sanzioni punibili dall'art.38 dello Statuto di Lavoratori con sanzione amministrativa E arresto

ART. 4 STATUTO DEI LAVORATORI

Divieto di uso di impianti audiovisivi per finalità di controllo a distanza dell'attività del lavoratore.

NO telecamere sua postazione di lavoro

NO riprese aree ricreative, spogliatoi, servizi

Sono ammesse telecamere sono in accordo con le rappresentanze sindacali e DTL

Ammessa per le sole esigenze organizzative/produttive/ sicurezza e tutela del patrimonio aziendale

Le immagini registrate devono essere limitate alle 24 ore successive alla rilevazione

Utilizzo di sistemi GPS e di geolocalizzazione

Per l’utilizzo dei sistemi di geolocalizzazione valgono le stesse disposizioni previste in materia di videosorveglianza.

Anche i dati rilevati attraverso l’uso di tale strumentazione è considerato trattamento dei dati personali e pertanto è necessario che il Titolare del Trattamento raccolga il consenso scritto da parte dell’interessato.

PRIVACY & WEB

Anche la gestione di siti web, sia ai soli fini pubblicitari che di E-Commerce, impone il rispetto di alcune regole ben definite dal Regolamento:

-deve essere esplicitata la Policy Privacy utilizzata dal sito web;

-devono essere indicati i cookies utilizzati;

-nel caso in cui nel sito vengano richiesti «volontariamente» dati che consentano il riconoscimento dell'utente utilizzatore del sito, (oltre all'indirizzo IP già raccolto) è indispensabile che si predisponga una adeguata informativa e relativo consenso, che deve essere accettato nel momento in cui si procede a lasciare i propri dati nel form.

NOTIFICA DELLE VIOLAZIONI

-il Responsabile del trattamento informa il Titolare
- entro le 72 ore deve essere fatta denuncia al Garante
-Non si è tenuti alla notifica qualora sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

LA FORMAZIONE

Obbligo di formazione del personale coinvolto nel trattamento dei dati personali

Il GDPR impone in maniera esplicita di fornire un adeguata preparazione ai soggetti attivi nel trattamento in base al ruolo che questi ricoprono.

Il Garante in sede ispettiva analizza il profilo delle istruzioni degli incaricati al trattamento e del Titolare stesso e richiede i seguenti documenti:

-piano di formazione
-programma
-attestati di frequenza al corso di formazione

SANZIONI

AMMINISTRATIVE

FINO A 10 MILIONI DI EURO OPPURE IL 2% DEL FATTURATO MONDIALE ANNUO per

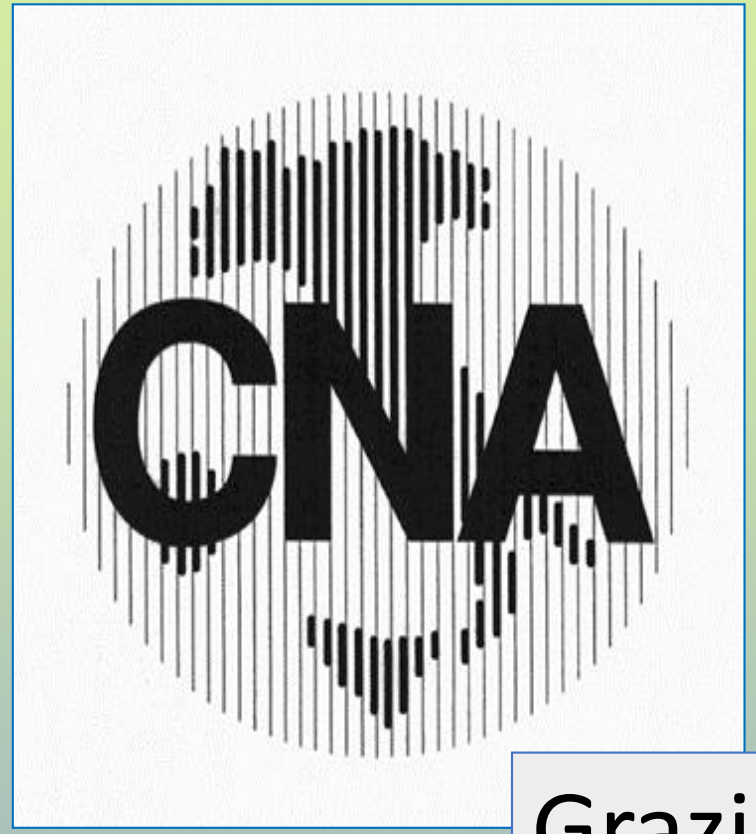
-inosservanza degli obblighi del Titolare e Responsabile del Trattamento ;
-inosservanza degli obblighi dell'organismo di certificazione
-inosservanza degli obblighi dell'organismo di controllo

FINO A 20 MILIONI DI EURO O 4% DEL FATTURATO MONDIALE ANNUO per

-inosservanza d un ordine, di una limitazione provvisoria o definitiva imposta da una autorità competente;
-trasferimento illecito dei dati personali ad un destinatario di un Paese Terzo

PENALI

Il Garante Italiano ha introdotto anche sanzioni penali punibili con la reclusione da 6 mesi fino ad un massimo di 6 anni



Grazie per l’attenzione