PROTEZIONE DEI DATI PERSONALI

LINEE GUIDA

Regolamento europeo (UE) 679/2016

INDICE DEGLI ARGOMENTI

(ctrl+click per dirigersi alla sezione desiderata)

1. FINALITA'

2. AMBITO DI APPLICAZIONE

3. DECORRENZA

4. AUTHORITY

5. SANZIONI

6. PRINCIPI

7. RESPONSABILIZZAZIONE

8. CONTITOLARITA'

9. RUOLI

10. ADEMPIMENTI

11. MISURE DI SICUREZZA

12. IMPATTO SUL SISTEMA CNA E SULLE IMPRESE

NOVITA'

Il **Regolamento europeo (UE) 679/2016** (detto anche RGPD) introduce regole chiare, che pongono le basi per l'esercizio di nuovi diritti stabilendo criteri rigorosi per il trattamento dei dati personali, inclusi i casi di violazione dei dati ed il trasferimento dei dati al di fuori dell'Ue.

1. FINALITA'

- Proteggere il trattamento dei dati personali delle **persone fisiche**
- Proteggere la **libera circolazione** dei dati personali nell'Unione.
- **Adeguare, rafforzare ed unificare le norme privacy** entro i confini dell'UE;
- Individuare regole adeguate all'**evoluzione tecnologica** ed alla **globalizzazione**;
- Creare un clima di **fiducia** per i cittadini europei per lo **sviluppo dell'economia digitale**.

Per merito delle battaglie, condotte anche dalla CNA in termini di semplificazione, è stata confermata la tutela dei dati personali riferiti esclusivamente alle sole persone fisiche.

2. AMBITO DI APPLICAZIONE

E' applicabile e vincolante in tutti gli Stati membri dell'Unione europea ed alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea.

Il nuovo regolamento apporta novità rilevanti in tema di protezione dei dati personali per:

- **Cittadini**
- **Aziende**
- **Enti Pubblici**
- **Associazioni**
- **Liberi Professionisti**

3. DECORRENZA

Il Regolamento generale sulla protezione dei dati "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali» (Gazzetta Ufficiale UE 4 maggio 2016), è entrato in vigore ufficialmente il 24 maggio 2016, ma sarà applicato solo a decorrere dal **25 maggio 2018**.

Proteggere il **trattamento dei dati** personali delle persone fisiche
Proteggere la **libera circolazione dei dati** personali nell'Unione.
Adeguare, rafforzare ed unificare le **norme privacy entro i confini dell'UE**
Individuare **regole adeguate all'evoluzione tecnologica** ed alla globalizzazione
Creare un clima di fiducia per i cittadini europei per lo sviluppo dell'economia digitale

4. AUTHORITY

Autorità di controllo

Ogni Stato membro dispone che, una o più autorità pubbliche indipendenti, sorveglino l'applicazione del RGPD. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione.

Comitato europeo per la protezione dei dati

Il Comitato UE, formato dalle Authority privacy nazionali, garantisce l'applicazione coerente del RGPD.

5. SANZIONI

E' previsto inoltre un elevato regime sanzionatorio, con **pene amministrative pecuniarie** che possono arrivare fino a **20 milioni di euro** o al **4% del fatturato globale**.

6. PRINCIPI

Si applicano al trattamento dei dati i seguenti principi:

- **Liceità, correttezza e trasparenza**
- **Limitazione della finalità (determinate, esplicite, legittime)**
- **Minimizzazione dei dati (adeguati, pertinenti, limitati)**
- **Esattezza**
- **Limitazione della conservazione**
- **Integrità e riservatezza**
- **Responsabilizzazione**

7. RESPONSABILIZZAZIONE E APPROCCIO BASATO SULRISCHIO

Sono definiti nuovi ambiti di responsabilità, competenza e facoltà:
Il "**principio di accountability**" dei Titolari e dei Responsabili prevede l'adozione, da parte loro, di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.
L'**analisi dei rischi**, invece, deve essere effettuata dal titolare tenendo conto dei pericoli noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che ritiene di dover adottare al fine di mitigare gli impatti negativi del trattamento sulle libertà e sui diritti degli interessati

8. CONTITOLARITA'

Qualora due o più titolari del trattamento **determinino congiuntamente le finalità ed i mezzi** del trattamento, essi saranno contitolari del trattamento.

I titolari del trattamento devono definire specificamente (**con un atto giuridicamente valido** ai sensi del diritto nazionale) il rispettivo ambito di responsabilità ed i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente ad uno qualsiasi dei titolari operanti congiuntamente.

I principi

- Liceità, correttezza e trasparenza
- Limitazione della finalità (determinate, esplicite, legittime)
- Minimizzazione dei dati (adeguati, pertinenti, limitati)
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza
- Responsabilizzazione

9. RUOLI

TITOLARE DEL TRATTAMENTO

Deve mettere in atto misure tecniche ed organizzative e può designare uno o più Responsabili del trattamento per le proprie attività di trattamento svolte in outsourcing.

Misure tecniche ed organizzative

Il trattamento deve essere effettuato in conformità al regolamento, tramite l'adozione di misure di sicurezza da adottare nel pieno rispetto dei seguenti principi:

- **Privacy by Design**

Il titolare deve compiere una corretta analisi dei rischi legati al trattamento dei dati, mettendo in atto tutte le misure tecniche ed organizzative necessarie per poterla effettuare correttamente. Tra queste misure rientrano:

- **Pseudonimizzazione**
- **(attuare in modo efficace i principi di protezione dei dati)**
- **Minimizzazione**
- **(integrare le garanzie al fine di tutelare i diritti degli interessati)**

Il regolamento prevede che il titolare tenga conto di alcuni parametri a garanzia della tutela dei diritti degli interessati:

- **Stato dell'arte**
- **Costi di attuazione**
- **Natura**
- **Ambito di applicazione**
- **Contesto**
- **Finalità del trattamento**
- **Rischi aventi probabilità e gravità diverse**

- **Privacy by Default**

Per **"Impostazione predefinita"** devono essere trattati solo i dati personali **necessari** per ogni **specifica finalità** del trattamento e tale obbligo vale per:

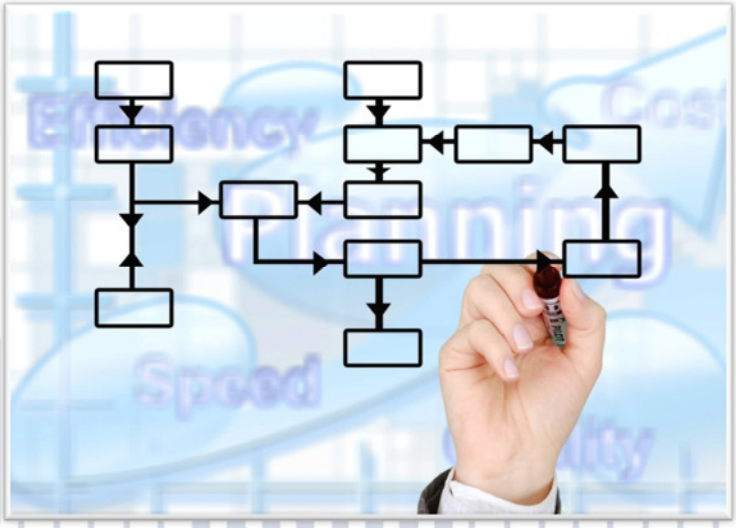
- La **quantità** dei dati personali raccolti
- La **portata** del trattamento
- Il **periodo** di **conservazione**
- L'**accessibilità**

Non devono essere resi **accessibili** dati personali ad **un numero indefinito** di persone fisiche senza l'intervento della persona fisica.

■ Designazione di rappresentante, responsabile del trattamento, responsabile per la protezione dei dati personali e formazione per soggetti che agiscono sotto l'autorità del titolare.

Il Titolare del trattamento *che opera fuori dall'Unione Europea* ma che offre servizi o prodotti a persone che si trovano nel territorio della UE deve nominare un proprio **rappresentante** in materia di privacy che ha la funzione di relazionarsi con le Autorità di controllo o con gli interessati.
Per le attività esternalizzate che comportano il trattamento di dati, invece, il titolare può provvedere, con contratto o altro atto giuridico, a regolare questi rapporti, dettagliandone i contenuti, nel rispetto di tutti gli elementi previsti dal RGPD, attraverso la **designazione di responsabile del trattamento**.
Il Titolare, inoltre, in talune ipotesi previste dal RGPD, può doversi dotare delle competenze di un **responsabile per la protezione dei dati personali**, figura di garanzia del corretto rispetto della normativa RGPD.
Infine, il Titolare del trattamento deve fare in modo che chiunque agisca sotto la sua autorità sia **incaricato** ed istruito (magari con istruzioni scritte o percorsi formativi).
.

I RUOLI NEL TRATTAMENTO DEI DATI PERSONALI



Titolare del trattamento

R.P.D. / D.P.O.

Responsabile del trattamento

Incaricato del trattamento

Interessato del trattamento

RESPONSABILE DEL TRATTAMENTO

Opera per conto del titolare

- quando in grado di dimostrare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate volte a soddisfare i requisiti richiesti dal RGPD o a garantire la tutela dei diritti dell'interessato;
- in base ad un contratto od altro atto giuridico all'interno del quale si precisano informazioni quali: natura, durata e finalità dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e delle disposizioni contenute nel RGPD.

Può nominare dei sub-responsabili

- Per specifiche attività di trattamento e nel rispetto degli stessi obblighi contrattuali che lo legano al titolare è stata introdotta questa possibilità, in precedenza esclusa.

Potrebbe essere tenuto ad obblighi specifici distinti da quelli dei titolari

- tenuta del registro dei trattamenti svolti
- adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti
- designazione di un RPD
- designare un rappresentante in Italia se il responsabile non è stabilito nell'Ue.

INCARICATO DEL TRATTAMENTO

Questa figura, presente nel Codice Privacy, pur non essendo prevista espressamente dal RGPD, non viene esclusa dal Garante in quanto si fa comunque riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile".
Gli incaricati devono essere istruiti dal Titolare sui contenuti del RGPD.

INTERESSATO DEL TRATTAMENTO

Diritti

- Informativa concisa, trasparente, intelligibile
- Accesso a tutte le informazioni che lo riguardano
- Rettifica dei dati inesatti
- All'oblio/cancellazione (anche dopo l'avvenuta revoca del consenso al trattamento)
- Portabilità (trattamenti automatizzati: social network, servizi Internet ecc.).
- Opposizione
- Limitazione di trattamento
- Al non essere sottoposto a decisione basata unicamente sul trattamento automatizzato

I DIRITTI DELL'INTERESSATO DEL TRATTAMENTO

RESPONSABILE della PROTEZIONE dei DATI - RPD/DPO

Questa neonata figura, delineata nel Regolamento Europeo, ha il compito fondamentale di facilitare la conformità dei trattamenti delle imprese alle disposizioni del RGPD.

Requisiti

- Possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati
- Adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse
- Operare alle dipendenze del titolare o del responsabile o sulla base di un contratto di servizio

Compiti

- Sorvegliare l'osservanza del RGPD
- Informare e sensibilizzare Titolare/Responsabile del trattamento nonché i loro dipendenti sugli obblighi derivanti dal RGPD e da altre disposizioni in materia di protezione dei dati
- Supportare Titolare/Responsabile del trattamento in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività
- Collaborare con il titolare/responsabile, nel condurre una valutazione di impatto (quando necessaria)
- Fungere da punto di contatto con il Garante

E' obbligatorio

- Quando il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**.
- In caso di trattamenti che richiedono il **monitoraggio regolare e sistematico** degli interessati su **larga scala**;
- Qualora vengano trattati, su **larga scala**, dati relativi a **condanne penali o a reati** oppure **particolari categorie di dati** (stato di salute, appartenenza ad organizzazioni sindacali, ecc.).

Va ricordato che anche quando il Regolamento non richiede specificatamente la nomina di tale figura, le imprese e le organizzazioni private **possono reputare utile designarla ugualmente** su base volontaria per facilitare la "**compliance**".

Quando non è obbligatorio

Il Titolare deve comunque

- **Documentare l'analisi interna effettuata** per determinare se un RPD deve essere nominato (tranne quando sia evidente che un soggetto non è tenuto a designarlo)
- Essere in **grado di dimostrare** che gli aspetti relativi alla determinazione sono stati presi in considerazione correttamente.

RESPONSABILE DELLA PROTEZIONE DEI DATI - RPD/DPO

I compiti

- Sensibilizzare e formare il personale
- Prestare consulenza al Titolare/Responsabile del trattamento
- Fornire un suo parere in merito alla valutazione di impatto
- Monitorare l'osservanza del Regolamento
- Fungere da punto di contatto con il Garante

10. ADEMPIMENTI

INFORMATIVA

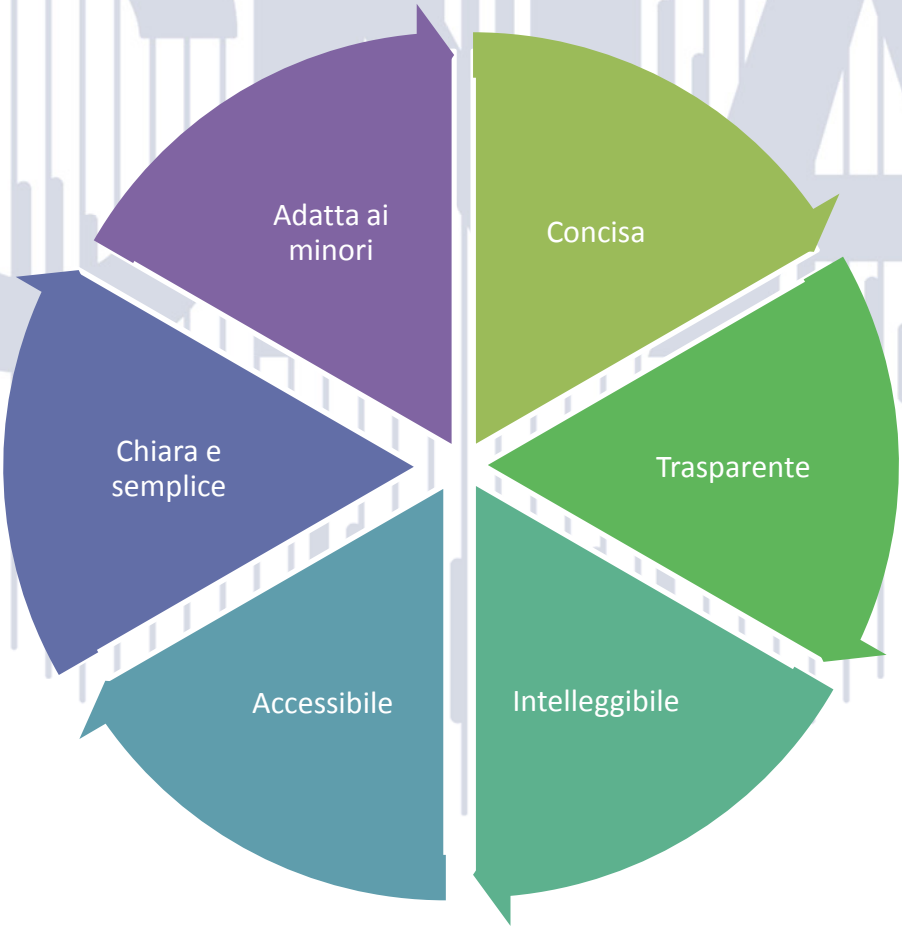
- **Deve sempre specificare**
  - L'identità del titolare e i dati di contatto
  - I dati di contatto del RPD (ove esistente)
  - La base giuridica del trattamento
  - L'interesse legittimo se presente
  - Se vengono trasferiti dati personali in Paesi terzi almeno in presenza di decisione di adeguatezza
  - Il periodo di conservazione dei dati od i criteri seguiti per stabilire tale periodo di conservazione
  - I diversi diritti degli interessati (accesso, rettifica, cancellazione, portabilità, ecc.)
  - Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), la logica di tali processi decisionali e le conseguenze previste per l'interessato
- **Per i dati non raccolti direttamente dall'interessato**
  - Deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta oppure al momento della comunicazione dei dati a terzi od all'interessato.
- **Deve avere forma**
  - Concisa
  - Trasparente
  - Intelligibile per l'interessato
  - Facilmente accessibile
  - Chiara e semplice
  - Idonea per i minori
- **Può essere data**
  - Per iscritto
  - Oralmente (anche se sconsigliata per l'onere della prova in capo al titolare)
  - In formato elettronico anche se sono ammessi "altri mezzi"
  - Tramite icone (definite dalla Commissione europea) che presentino i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa

CONSENSO

Deve essere

- **Esplicito**
  - Per i dati "sensibili;
  - Per decisioni basate su trattamenti automatizzati (compresa la profilazione)
- **Prestato il consenso a uno specifico trattamento**
  - Il titolare deve essere in grado di dimostrare
- **Valido per i minori**
  - A partire dai 16 anni
  - Prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

L'INFORMATIVA



REGISTRO DEL TRATTAMENTO DEI DATI

Deve essere tenuto in forma scritta (anche elettronica)

- da parte di imprese, aziende od organizzazioni con più di 250 dipendenti
- da parte di imprese, aziende od organizzazioni che effettuino un trattamento che presenta rischi per diritti e libertà dell'interessato, che non sia occasionale e includa categorie particolari di dati sensibili (es. dati sindacali o inerenti allo stato di salute) o relativi a condanne penali.

Per le tipologie sopra elencate, i **soggetti tenuti a redigere un registro** sono:

- Aziende con più di 250 dipendenti
- Associazioni sindacali
- Patronati
- Centri assistenza fiscale (caf)
- Cliniche private, ambulatori, studi odontoiatrici, case di riposo, residenze sanitarie assistite che si avvalgono di cartelle sanitarie
- Imprese di sicurezza privata incaricate della sorveglianza di più centri commerciali ed aree pubbliche
- Società di elaborazione cedolini o di software che svolgono queste attività per conto dei loro clienti
- Studi legali composti da più professionisti
- Soggetti che curano il funzionamento di una rete di telecomunicazioni, etc …

Informazioni contenute

- nome e dati di contatto del Titolare;
- finalità del trattamento;
- descrizione delle categorie di interessati e di dati personali;
- categorie di destinatari cui i dati sono stati o saranno comunicati;
- termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- descrizione generale delle misure di sicurezza tecniche e organizzative.

Strumento fondamentale

- In caso di eventuale supervisione da parte del Garante
- Per la puntuale ed aggiornata risultanza dei trattamenti in essere
- Per adempiere ad ogni corretta valutazione
- Effettuare adeguate analisi dei rischi
- In un sistema di corretta gestione dei dati personali

REGISTRO DEL TRATTAMENTO DEI DATI

In caso di eventuale supervisione da parte del Garante

Per la puntuale ed aggiornata risultanza dei trattamenti in essere

Per adempiere ad ogni corretta valutazione

Effettuare adeguate analisi dei rischi

In un sistema di corretta gestione dei dati personali

VALUTAZIONE D'IMPATTO (DPIA)

Il Titolare deve effettuare la valutazione d'impatto, avvalendosi della collaborazione del RPD, quando il trattamento che intende effettuare:

- Prevede (in particolare) l'uso di nuove tecnologie
- Presenta un rischio elevato (per natura, oggetto, contesto e finalità) per i diritti e le libertà delle persone fisiche.
- Effettua una valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato (compresa la profilazione), e sulla quale si fondano decisioni che hanno effetti giuridici o incidono significativamente su dette persone fisiche;
- Viene effettuato su larga scala di dati sensibili o relativi a condanne penali/reati;
- Comporta una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CONSULTAZIONE PREVENTIVA

- Qualora il Titolare, in presenza di una **valutazione d'impatto** sulla protezione dei dati che abbia indicato un trattamento comportante un **rischio elevato** ed in **assenza di misure volte ad attenuarlo**, prima di procedere al trattamento, deve consultare il Garante.
- Nel caso in cui il **Garante** ritenga che il trattamento violi il Regolamento, entro otto settimane dal ricevimento della richiesta di consultazione (alle quali se ne possono aggiungere altre sei se il parere richiesto è complesso), è tenuto a fornire un **parere scritto** al titolare ed ad avvalersi dei poteri conferitigli dal Regolamento stesso per vietarlo.

CERTIFICAZIONE E CODICI DI CONDOTTA

L'adesione ai codici di condotta o ad un meccanismo di certificazione può essere utilizzata come elemento **per dimostrare il rispetto degli obblighi** del titolare del trattamento.

Il Regolamento UE, per la certificazione prevede che vengano prese in considerazione le **esigenze** specifiche delle **micro, piccole e medie imprese**.

La certificazione potrà essere **rilasciata** da un **soggetto abilitato** oppure dallo stesso **Garante**.

IL REGOLAMENTO UE, PER LA CERTIFICAZIONE PREVEDE CHE VENGANO PRESE IN CONSIDERAZIONE LE **ESIGENZE** SPECIFICHE DELLE **MICRO, PICCOLE E MEDIE IMPRESE**.

11. MISURE DI SICUREZZA

I titolari/responsabili dovranno adottare **misure di sicurezza (tecniche ed organizzative) adeguate al rischio del trattamento**. Tale valutazione dovrà essere effettuata in relazione alla natura dei dati e all'effettiva pericolosità dei trattamenti effettuati in grado di arrecare pregiudizio alle libertà ed ai diritti degli interessati.

In questo senso la lista di misure di sicurezza del § 1 dell'art. 32 del RGPD deve considerarsi aperta e non esaustiva ma nel dettaglio possono essere riconducibili a:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il nuovo sistema si basa su alcuni principi cardine, ineludibili. I primi tre sono: la necessità di un'analisi del rischio, l'attenzione ai costi da supportare e l'applicazione della nozione di "accountability".

In attesa che codici di condotta e schemi di certificazioni possano agevolare titolari/responsabili nel loro compito di accountability riferito alle misure di sicurezza, già ora è ipotizzabile l'utilizzo di **check list** redatte tenendo conto delle peculiarità delle micro, piccole e medie imprese ed in grado di infondere elementi di consapevolezza presso le stesse in relazione ai contenuti del RGPD.

NOTIFICAZIONE E COMUNICAZIONE DI EVENTUALI VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

- **Il Titolare in caso di violazione** nell'ipotesi in cui tale evento possa generare **danni fisici, materiali o immateriali** alle persone fisiche

  - Perdita del controllo dei dati personali che li riguardano
  - Limitazione dei loro diritti
  - Discriminazione
  - Furto
  - Usurpazione d'identità
  - Perdite finanziarie
  - Decifratura non autorizzata della pseudonimizzazione
  - Pregiudizio alla reputazione
  - Perdita di riservatezza dei dati personali protetti da segreto professionale
  - Qualsiasi altro danno economico o sociale significativo alla persona fisica interessata

- **Dovrà effettuare formale notifica della violazione al Garante**

  - senza ingiustificato ritardo
  - ove possibile, **entro 72 ore** dal **momento in cui ne è venuto a conoscenza**.

- **Dovrà comunicarlo agli interessati**

  - Eccetto quando sia esclusa (anche i base alle misure di sicurezza preventive adottate) dal RGPD la comunicazione si deve effettuare quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati

- **Mancata notificazione/comunicazione**

  - comporta una **sanzione amministrativa pecuniaria fino a 10.000 Euro**
  - per le imprese, la sanzione può arrivare **fino al 2% del fatturato mondiale totale** annuo dell'esercizio precedente.

NOTIFICAZIONE DI EVENTUALI VIOLAZIONI (DATA BREACH)

I Rischi

- Perdita del controllo dei dati personali che li riguardano
- Limitazione dei loro diritti
- Discriminazione
- Furto
- Usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della pseudonimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati personali protetti da segreto professionale
- Qualsiasi altro danno economico o sociale significativo alla persona fisica interessata

12. IMPATTO SUL SISTEMA CNA E SULLE IMPRESE

OBBLIGO / ADEGUAMENTO

Chi in particolare?

- CNA Nazionale
- CNA Territoriali
- CNA Pensionati
- CAF CNA srl
- EPASA –ITACO
- FONDAZIONE ECIPA
- Imprese che per la natura delle loro attività trattano dati appartenenti a categorie particolari
- Imprese che operano un monitoraggio sistematico dei dati ed in larga scala
- Imprese che effettuano trattamenti in grado di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Come?

- Documentazione adeguata (Registro del trattamento dei dati del titolare e del responsabile, nomina RPD/DPO, check list di conformità e di sicurezza, ecc.)
- Implementazione delle misure di sicurezza
- Nomina dell'RPD/DPO
- Formazione continua (specifica per funzioni)
- Eventuale adozione di codici di condotta e certificazioni

OPPORTUNITA' / SVILUPPO DI SERVIZI

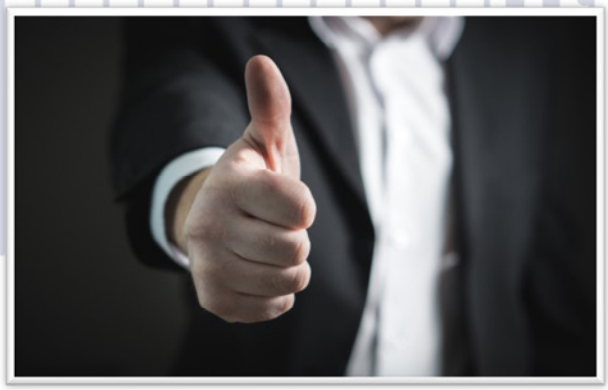
La nuova normativa in materia di protezione dei dati personali consente di dare servizi e risposte adeguate alle imprese attraverso le strutture CNA Territoriali a prezzi calmieratori del mercato.

CNA Territoriali

- Consulenti della CNA specializzati e costantemente aggiornati
- Supporto di CNA Nazionale
- Portale GDPR realizzato da Sixtema S.p.A. in accordo con CNA Nazionale

Potenziali destinatari dei erogati dalle CNA

- Imprese
- Enti privati e statali, ecc..

IMPATTO SUL SISTEMA CNA

LA CNA POTRA' ACCOMPAGNARE LE IMPRESE IN UN CORRETTO PERCORSO VOLTO ALL'ADEMPIMENTO DELLA NUOVA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E VERSO "LA DIGITAL TRANSFORMATION"