Analisi pratica del Quadro generale di insieme e dei nuovi adempimenti privacy. In relazione alle dinamiche *dei Periti dei Trasporti*

Relatore : Francesco Tola - Cybersecurity Manager, Data Protection Specialist e Responsabile per la protezione dei Dati (DPO)

Francesco.tola@piramisgroup.com.

GDPR

General Data Protection Regulation
(Regolamento Generale sulla protezione dei Dati)

Il GDPR, conosciuto anche come “normativa sulla privacy”, è entrato in vigore il 25 maggio 2016, ed il termine ultimo per adeguarsi è stato il 25 maggio 2018.

E’ una normativa rivoluzionaria che per la prima volta uniforma ed espande l’ambito di applicazione ben oltre i confini Italiani ed Europei, e che sta portando radicali cambiamenti nel modo di concepire la protezione dei dati nel mondo del lavoro e nella vita di tutti i giorni.

Art. 1 GDPR

Oggetto e Finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Art. 2 GDPR

Ambito di Applicazione MATERIALE

Il Regolamento si applica al trattamento interamente o parzialmente automatizzato dei dati personali di persone fisiche e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Sono esclusi dall'ambito materiale i trattamenti di dati personali:

a) Effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) Effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) Effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

d) Effettuati da autorità competenti al fine di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di Sanzioni penali

<u>Quindi, qualsiasi ente od azienda che tratta dati personali, deve applicare il GDPR</u>

Art. 3 GDPR

Ambito di Applicazione TERRITORIALE

Il Regolamento si applica:

- al trattamento dei dati personali, da parte di un Titolare o un Responsabile del trattamento stabilito nell'Unione, indipendentemente dal fatto che il trattamento sia (materialmente) effettuato o meno nell'Unione;

- al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un Titolare del trattamento o da un Responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi,

b) il monitoraggio dei loro comportamenti nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Quindi, ogni ente od azienda che ha sede in UE, o che pur avendo la sede Extra UE tratti i dati di persone fisiche che si trovano in Europa,
è tenuta all'applicazione del GDPR

DEFINIZIONI

Dato personale: qualsiasi informazione che riguardi una persona fisica identificata o identificabile.

- ***Dato identificativo:*** permette l'identificazione diretta della persona (nome + cognome, codice fiscale, le immagini);
- ***Dato anonimo:*** non può essere associato ad un Interessato identificato o identificabile, come può essere, ad esempio, un dato statistico.

DEFINIZIONI

Art. 9 e art. 10 del GDPR - Dati Particolari e giudiziari

E’ stata eliminata la definizione di **dati sensibili**, ora si parla di «categorie particolari di dati personali».

- **Dati particolari:** dati personali che rivelino l’origine etnica o razziale, le opinioni politiche, le convinzioni religiose, l’appartenenza sindacale, dati biometrici, genetici, relativi alla salute o alla vita sessuale di una persona fisica.
- **Dato giudiziario:** dati personali relativi a condanne penali e a reati.

Definizioni

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

la raccolta, la registrazione, l'organizzazione, la strutturazione, *la 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 o la distruzione.

In Pratica, dal momento che l'azienda "acquisisce" un dato personale, fino a quando non lo "elimina" definitivamente dai propri archivi, lo stà di fatto trattando 24 ore al giorno, 365 giorni l'anno,

E ne è totalmente e completamente responsabile!

Definizioni

Titolare del trattamento:

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina, singolarmente o insieme ad altri, le finalità e i mezzi del trattamento dei dati personali.

E' quindi "colui che decide" le regole di come verranno effettuati i trattamenti di sua competenza.

Definizioni

Interessato:

la persona fisica a cui si riferiscono i dati personali soggetti al trattamento.

Gli interessati <u>siamo tutti noi!</u>

Definizioni

Responsabile del trattamento:

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Il Responsabile (Art. 28)

Qualora un trattamento dei dati debba essere effettuato per conto del Titolare del trattamento, quest'ultimo deve ricorrere unicamente a responsabili del trattamento che **presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'Interessato.

Il Responsabile

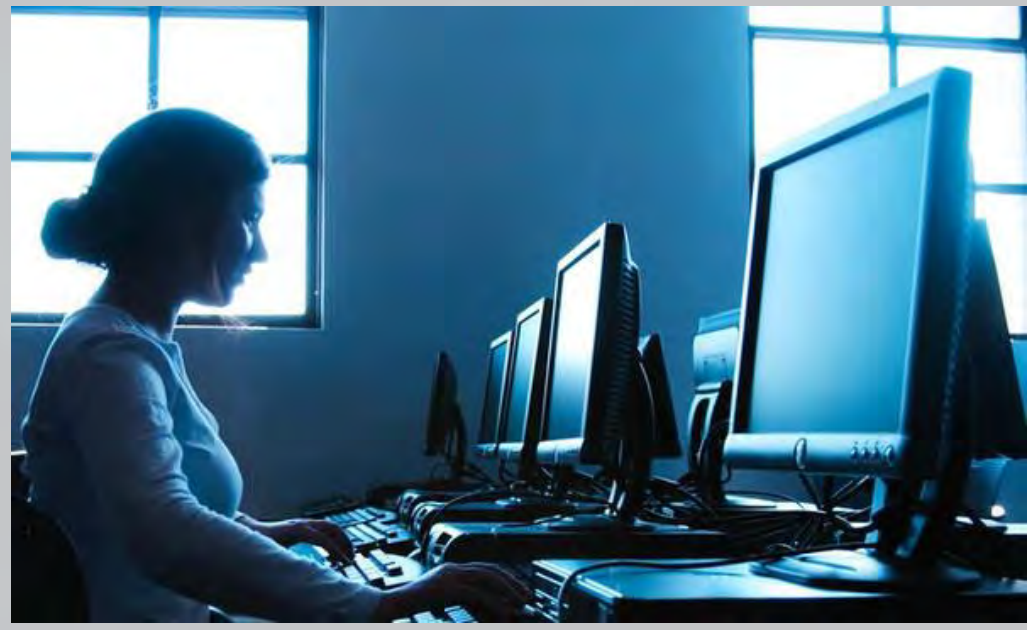
L'esecuzione di trattamenti su incarico, è regolata da **contratto o altro atto giuridico che vincoli** il Responsabile (par. 3): devono essere indicati l'oggetto, la durata del trattamento, la natura e finalità del trattamento, il tipo di dati, la categoria di interessati, obblighi e diritti del Responsabile.

Per lo svolgimento dei compiti affidati, e previa autorizzazione del Titolare del Trattamento, il Responsabile può avvalersi a sua volta di altri soggetti esterni alla propria struttura che diventano quindi ***Sub-Responsabili*** del trattamento (e di cui risponde direttamente nei confronti del Titolare del Trattamento stesso).

Il Responsabile del trattamento è quindi quel soggetto "esterno" all'azienda (sia esso un'altra azienda, che un libero professionista) che "segue le regole" dettate dal titolare del trattamento.

Incaricato del trattamento

- ✓L'Incaricato, o soggetto autorizzato, è il **soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali richieste**.
- ✓IL Titolare od il Responsabile del trattamento, garantiscono che **le persone autorizzate al trattamento dei dati personali** si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.



Incaricato del trattamento

L’incaricato riceve precise istruzioni (con apposita lettera di incarico) dal Titolare o dal Responsabile del trattamento da cui lo stesso dipende, in maniera tale da poter svolgere le operazioni di trattamento richieste.

Semplificando, l’incaricato è di conseguenza in qualche maniera alle “dirette dipendenze” dell’azienda per cui tratta i dati, sia essa stessa il Titolare o Responsabile del trattamento. Es: Gli operatori dell’azienda sono incaricati del trattamento.

Requisiti – Obblighi del GDPR

Il GDPR introduce tutta una serie di nuovi obblighi e requisiti di conformità per la tutela dei dati personali, tenendo sempre a mente e come punto cardine **“la protezione dei diritti e delle libertà fondamentali delle persone fisiche”**. E visto che viviamo in un mondo che tecnologicamente corre molto velocemente, e che il trattamento viene sempre più spesso effettuato con strumenti elettronici, il GDPR non determina precise misure di sicurezza che diventerebbero obsolete nell’arco di poco tempo, ma introduce una grande novità, che è il vero e proprio “cuore” del GDPR Stesso: Il principio di **“Accountability”** (Responsabilità).

Accountability (Responsabilità)

Il Titolare del trattamento deve attuare misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati venga effettuato in modo conforme al Regolamento.

Art. 24
Responsabilità del Titolare /2

Questo significa che il Titolare ha completa autonomia su come meglio organizzare il trattamento (e relative misure di sicurezza dello stesso), all'interno della propria struttura.

Non ha nessun "obbligo" predefinito, se non quello di:

-Proteggere i diritti, le libertà, ed i dati personali delle persone fisiche

-Dimostrare in pratica (e non solo sulla carta!!) di essere ***davvero*** in grado di farlo.

Questo punto è ciò che fa la differenza tra

***la reale protezione dei dati*,**

ed il totale ed *irreparabile disastro*!

Documenti del Titolare

Il registro dei trattamenti e il registro delle violazioni

Il documento dell'analisi dei rischi

Le informative ben strutturate, complete e facilmente comprensibili

Con il GDPR il Titolare deve produrre e conservare la documentazione con cui possa, in caso di necessità, dimostrare la propria accountability, come:

Elenco degli incaricati e dei responsabili e relative lettere di designazione

Se il rischio è alto, il documento sulla valutazione d'impatto dei trattamenti

I diritti dell'Interessato

Ogni persona fisica, in qualsiasi momento della propria vita, può chiedere di esercitare i propri diritti presso il Titolare del Trattamento, il quale ha 30 giorni per rispondere a tale richiesta.

I diritti che una persona può esercitare, descritti dall'articolo 15 al 22, sono :

-**Diritto di Accesso**
-**Diritto di Rettifica**
-**Diritto alla Cancellazione (Diritto all'Oblio)**
-**Diritto di Limitazione al trattamento**
-**Diritto alla Portabilità dei Dati**
-**Diritto di Opposizione al Trattamento**

Art 32. Sicurezza del Trattamento

Abbiamo visto quanto la sicurezza informatica giochi un ruolo fondamentale e cardine nel GDPR per la protezione dei dati e dei diritti e le libertà fondamentali delle persone fisiche.

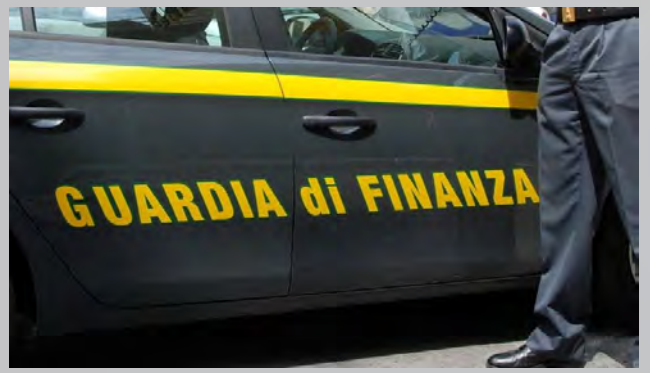
Mancare di proteggere in maniera adeguata i propri sistemi informatici e tecnologici, non solo può portare letteralmente a **"disastri"** operativi (e purtroppo talvolta irrecuperabili), ma anche a **sanzioni molto significative nei confronti dell'azienda stessa.**

Ma la sicurezza passa anche da altri fattori, come ad esempio la formazione delle persone che trattano i dati, la creazione di processi che promuovano la sicurezza (senza mai però "affossare" l'operatività aziendale) e dalla continua sorveglianza.

Ma cosa succede se l'azienda non può dimostrare di essere in grado di ***proteggere per davvero ed in pratica*** i dati personali ed i diritti e le libertà delle persone fisiche…?

LE SANZIONI

Sanzioni amministrative pecuniarie fino a
€ 20.000.000
oppure fino al 4% del fatturato Annuo



Le Sanzioni – d.lgs. 101/2018

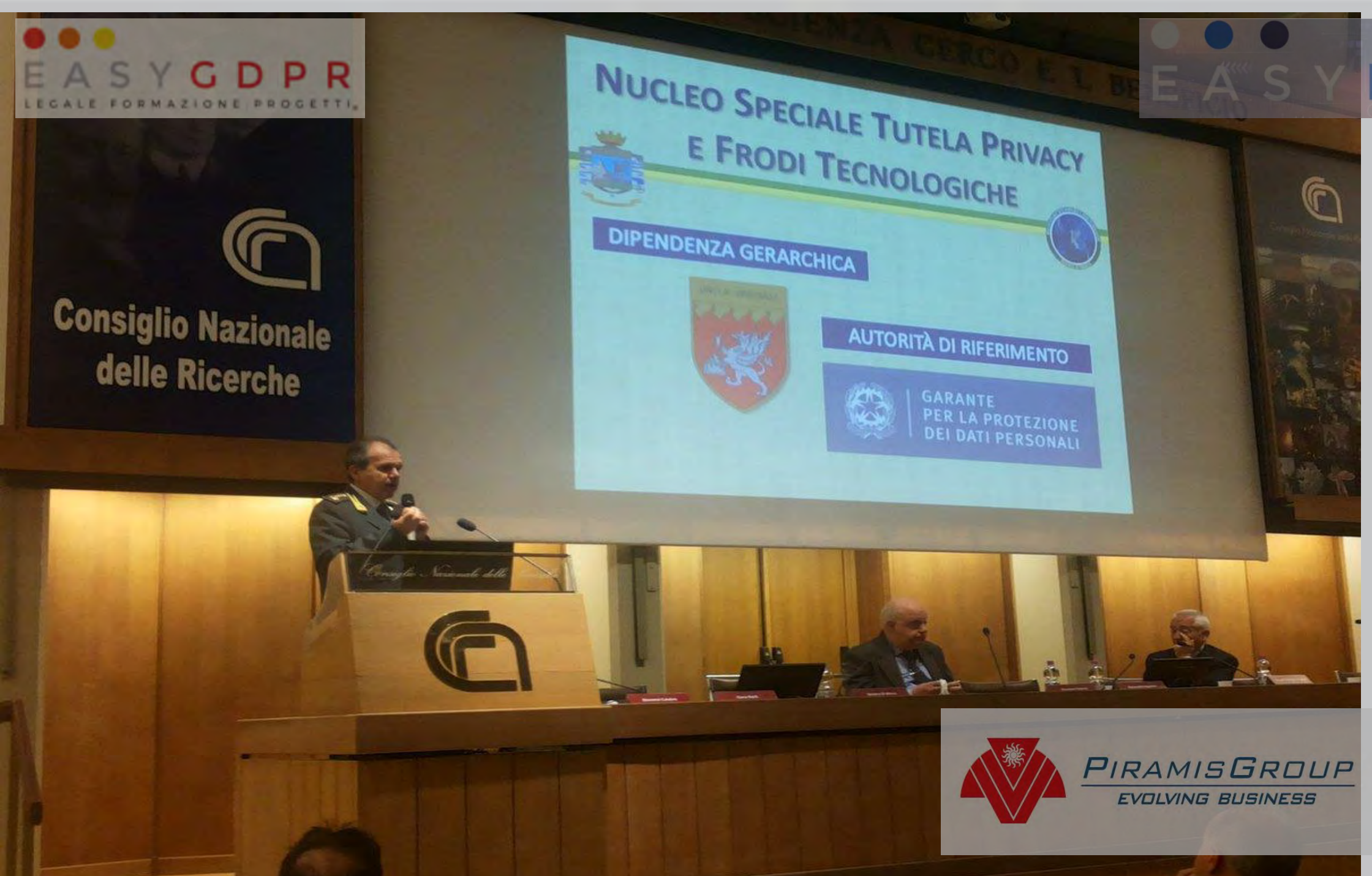
Sanzioni penali: reclusione da sei mesi fino a sei anni

- **Trattamento illecito di dati**. "Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'Interessato, operando in violazione del Regolamento arreca un danno all'Interessato, è punito con la reclusione da sei mesi fino a un anno e sei mesi. E nei casi più gravi fino a tre anni.

- **L'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala è** punita con la reclusione da uno a quattro anni.
- **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala è** punita con la reclusione da uno a sei anni.
- **L'inosservanza dei provvedimenti del Garante è** punita con la reclusione da tre mesi a due anni.

Sanzioni amministrative

- Sarà compito del Garante Privacy scrivere le regole per l'applicazione delle sanzioni amministrative, previste per esempio, si legge nel decreto legislativo, per chi non effettua la valutazione d'impatto sulla protezione dati - la **Dpia.**


NUCLEO SPECIALE TUTELA PRIVACY
E FRODI TECNOLOGICHE
DIPENDENZA GERARCHICA
AUTORITÀ DI RIFERIMENTO
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
Consiglio Nazionale
delle Ricerche

A proposito di sanzioni…

"Proteggere i dati vuol dire proteggere le persone"

ha dichiarato **Marco Menegazzo, Colonnello Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza:**

"La nostra attività ispettiva è focalizzata su tanti punti con al centro l'accountability art.24 del GDPR e la capacità del titolare di dimostrare il processo di adeguamento, ***per cui non crederemo a documentazione precompilata, fotocopiata o che non rispecchi i reali trattamenti effettuati. Ci metteremo insieme al DPO od al responsabile privacy interno a valutare l'effettività di quanto dichiarato, ricordando che le false attestazioni al Garante (art. 168 Codice Privacy) ricadono nell'ambito della disciplina penale***."

Dopo aver appreso queste informazioni , secondo voi la vostra attività azienda è conforme alla normativa ?
Come si applica il GDPR al lavoro di tutti i giorni della vostra attività? Ovvero, quando si trattano dati personali.?

Nella vostra attività probabilmente effettuate:

- *Raccolta dati dei clienti per emettere fattura*
- *Raccolta dati di prospect/clienti dal sito web*
- *Invio comunicazioni ai clienti (mail, ecc.)*
- *Conservazione dei dati e misure di sicurezza*
- *Gestione dei dati dei dipendenti /fornitori/Clienti*
- *ecc. ecc.*

Come si applica al Vostro lavoro di Periti dei Trasporti

Sono gli stessi punti ed esempi elencati prima:

- *Raccolta dati dei clienti per emettere fattura*
- *Raccolta dati di prospect/clienti dal sito web*
- *Invio comunicazioni ai clienti (mail, ecc.)*
- *Conservazione dei dati e misure di sicurezza*
- *Gestione dei dati dei dipendenti /fornitori/Clienti*
- *ecc. ecc.*

Ma con una importante aggiunta…

Dovendo lavorare per conto ci committenti, sia in perizia, sia in controllo ed eventuale supporto alla liquidazione dei danni, è molto probabile che riceviate dati personali da varie aziende, entità, organizzazioni o anche Pubbliche Amministrazioni. Questi dati personali per essere trattati «lecitamente» devono essere accompagnati da documentazione e procedure specifiche, la cui responsabilità ricade in egual misura tra Voi ed il committente dell'attività a voi richiesta. La mancanza di questi prerequisiti fondamentali, possono portare a sanzioni amministrative, o addirittura, in casi particolarmente gravi, anche penali.

Soluzione EasyGDPR / EasyDPO

Un approccio diverso - continuo – pratico , per ottenere realmente lo scopo di proteggere i dati personali trattati nel lavoro di tutti i giorni.

E non solo raggiungere quindi la conformità normativa, ma il fondamentale scopo di proteggere i dati lavorativi, il vero cuore della propria attività….!

Grazie per l'attenzione !

Relatore : Francesco Tola - Cybersecurity Manager, Data Protection Specialist e Responsabile per la protezione dei Dati (DPO)

Francesco.tola@piramisgroup.com

Customer Support:

Stefano.negri@piramisgroup.com