Formazione IFEL
per i Comuni

Il GDPR

Le nuove regole privacy per i COMUNI

Dott.ssa Maria Pia Giovannini
ex dirigente Agid
17 Maggio 2018

General Data Protection Regulation

Dal 25 maggio 2018 enti pubblici ed aziende dovranno adempiere agli obblighi previsti dal nuovo Regolamento Europeo sulla Privacy UE 2016/679 del 27 aprile 2016

È in corso di approvazione alle Camere lo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento Europeo UE 2016/679 del Parlamento Europeo

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

Il valore dei dati per il GDPR

Il Regolamento Europeo riconosce:

i «**DATI**» quale «**Asset fondamentale**»

un bene non riproducibile, parzialmente riacquistabile, difficilmente ricostruibile che riguarda l'individuo ma che sono integrati con i dati che le organizzazione che li trattano per erogare un servizio (piattaforme tecnologiche di intermediazione, es. piattaforme di e-commerce) detengono attraverso un «rapporto fiduciario» con l'individuo.

I dati personali sono le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

GDPR: Regolamento per la protezione dei dati personali

I diritti dell'individuo:

LICEITA' ti dico solo queste cose e a questo scopo

ACCESSO posso accedere alle mie informazioni in tempi e costi certi

RETTIFICA quando necessario e voluto posso modificare i miei dati

OBLIO se te lo chiedo posso cancellare i miei dati in qualunque momento in via retroattiva

PORTABILITA' se te lo chiedo posso avere indietro i miei dati per affidarli a terzi

Gli obblighi del titolare al trattamento

NOMINA del RESPONSABILE per il trattamento dei dati , del Responsabile della protezione dei dati

REGISTRI la tenuta dei registri che in ogni momento posso fornire informazioni sui dati

RESPONSABILITA' del titolare del trattamento per bilanciare esigenze procedurali e rispetto dei diritti di libertà

TEMPESTIVITA' e TRASPARENZA nel fornire l'informativa richiesta

Come adeguarsi al GDPR?

Per un'organizzazione **un Progetto di adeguamento al GDPR** non è mai una banalità, perché bisogna rivedere l'organizzazione, l'informatica, la sicurezza, la modulistica, la formazione interna, l'informazione interna ed esterna, gli aspetti legali per il rapporto con i clienti/utenti/cittadini, ecc.

L'entità stessa del progetto può variare molto a secondo della tipologia di organizzazione in termini di dimensione e di attività svolta.

1 **ASSESSMENT**

2 **SCRITTURA DELLE PROCEDURE**

3 **IMPLEMENTAZIONE DELLE PROCEDURE**

4 **GOVERNANCE**

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

Che cosa serve fare?

NOMINARE IL RESPONSABILE DEL TRATTAMENTO

DOTARSI DI UNA FIGURA CHE VERIFICHI E GARANTISCA IL RISPETTO DELLE PROCEDURE : IL DATA PROTECTION OFFICER (DPO) O L'AMMINISTRATORE DELEGATO

VERIFICARE QUALI DATI PERSONALI VENGONO TRATTATI, CHI LI TRATTA, COME LI TRATTA E CON QUALI STRUMENTI («AS IS»)

ESEGUIRE DEGLI AUDIT PER VERIFICARE IL RISPETTO DELLE PROCEDURE

FORMARE IL PERSONALE PER RISPETTARE LE PROCEDURE

ADEGUARE GLI STRUMENTI SOFTWARE E NON (SISTEMI APPLICATIVI, INFRASTRUTTURE,HW/SW, SISTEMI DI SICUREZZA, ARCHIVI,..), AFFINCHÉ CONSENTANO DI RISPETTARE LE PROCEDURE

DEFINIRE LE PROCEDURE CHE STABILISCONO COME TRATTARE I DATI PERSONALI («TO BE»)

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

GDPR – le linee guida ANCI

- Schema di Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
- Schema di delibera di Consiglio comunale per l'adozione del Regolamento comunale di attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
- Schema di atto di designazione del Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679

Formazione IFEL per i Comuni

IFEL Fondazione ANCI

GDPR – ASPETTI GIURIDICI

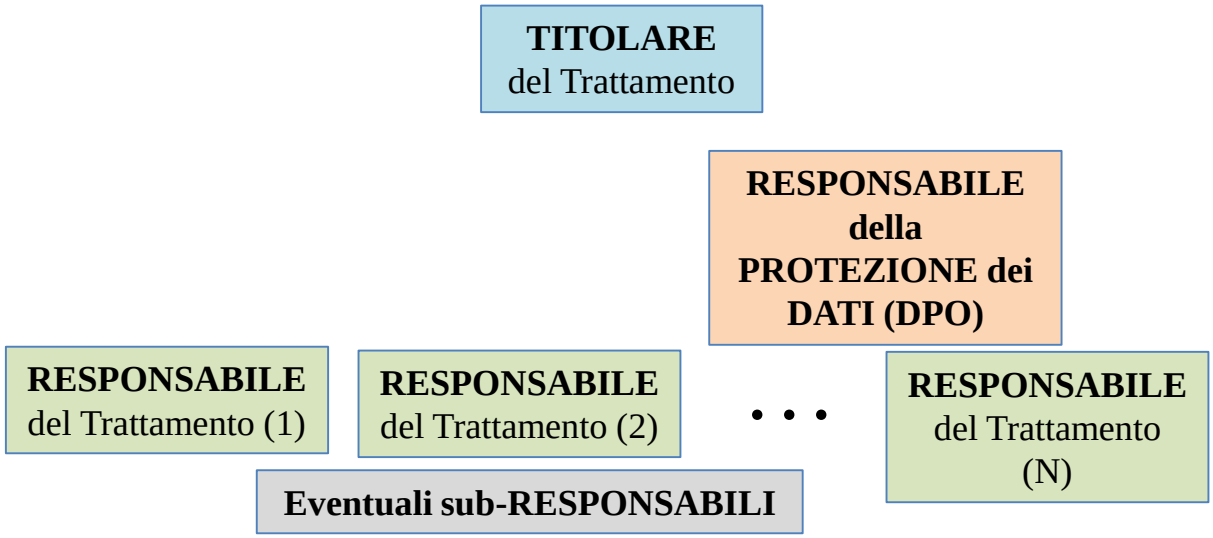
Revisione delle attuali figure
Istituzione del Titolare del trattamento, del/dei Responsabile/i del/dei trattamento/i e sub responsabile/i e del DPO data protection officer con stesura contratti ad hoc per disciplinare la distribuzione delle responsabilità

Revisione delle procedure e della modulistica per i rapporti con il cliente/utente
richiesta del consenso al trattamento dei dati, gestione procedure reclami, accesso ai dati etc

Procedure di notifica di violazione dei dati personali (Data breach) e gestione del registro data breach

GDPR – LE FIGURE RESPONSABILI

Tipicamente:



Ma ci possono essere scelte diverse, in funzione delle dimensioni del Comune, della presenza di Partecipate, ecc.

GDPR – IL DPO (art. 37)

La nomina del Data Protection Officer DPO è obbligatoria per un ente pubblico

Il DPO dovra essere designato per un determinato periodo ed in funzione delle qualità professionali , della conoscenza specialistica della materia e in condizioni di assicurare l'esercizio del proprio ruolo senza conflitti di interesse.

Il DPO puo essere un dipendente dell'Ente o un incaricato esterno che assolve al servizio sulla base di uno specifico contratto

Il DPO, per gli enti pubblici, può essere designato per più autorità pubbliche o organismi pubblici tenuto conto della loro struttura organizzativa

Il titolare del trattamento pubblica i dati di contatto del DPO e li comunica all'autorità di controllo

GDPR – I compiti del DPO (art. 39)

- Informare e fornire consulenza al titolare del trattamento e al responsabile del trattamento nonche' ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonchè da altre norme relative alla protezione dei dati

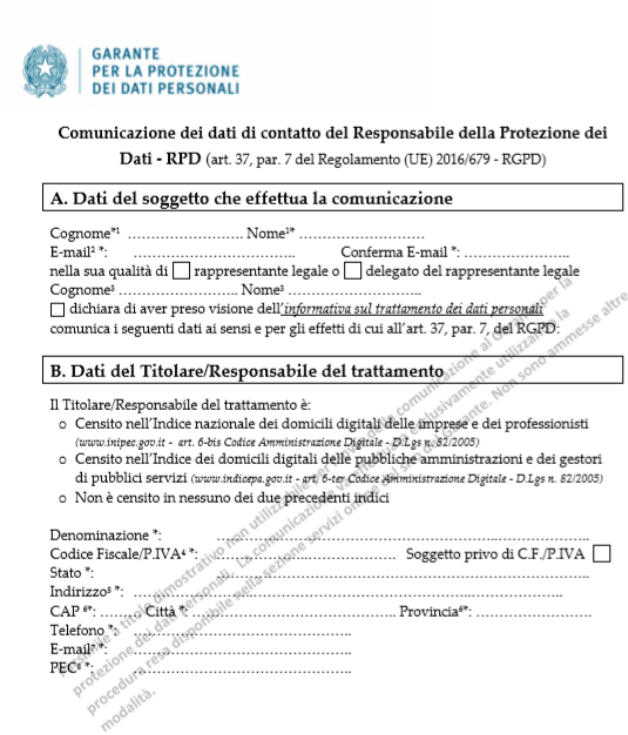
- Sorvegliare l'osservanza del GDPR nonchè delle politiche del titolare e del resposnsbaile del trattamento in materia di trattamento dei dati personali compresi l'attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento dei dati

- Fornire se richiesto un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35

- Cooperare con l'autorità di controllo

- Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento tra cui a consultazione preventiva di cui all'articolo 36 (casi complessi). L'indirizzo da utilizzare dovrà essere registrato sull'**IPA** (**Indice Pubbliche Amministrazioni**)

Come comunicare all'Autorità il DPO



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati - RPD (art. 37, par. 7 del Regolamento (UE) 2016/679 - RGPD)

A. Dati del soggetto che effettua la comunicazione

Cognome*[1] ..... Nome[1]* .....
E-mail[2] *: ..... Conferma E-mail *: .....
nella sua qualità di ☐ rappresentante legale o ☐ delegato del rappresentante legale
Cognome[3] ..... Nome[3] .....
☐ dichiara di aver preso visione dell'*informativa sul trattamento dei dati personali*
comunica i seguenti dati ai sensi e per gli effetti di cui all'art. 37, par. 7, del RGPD:

B. Dati del Titolare/Responsabile del trattamento

Il Titolare/Responsabile del trattamento è:
- o Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti *(www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)*
- o Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi *(www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)*
- o Non è censito in nessuno dei due precedenti indici

Denominazione *: .....
Codice Fiscale/P.IVA[4] *: ..... Soggetto privo di C.F./P.IVA ☐
Stato *: .....
Indirizzo[5] *: .....
CAP [6]*: ..... Città *: ..... Provincia[6]*: .....
Telefono *: .....
E-mail[7] *: .....
PEC[8] *: .....

Fac simile della comunicazione dei dati di contatto del Responsabile della Protezione dei dati

Scaricabile dal sito dell'Autorità
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8867026

GDPR – ASPETTI ORGANIZZATIVI E FORMATIVI

guide e moduli formativi per titolari e responsabili: va predisposto un apposito “corpus” formativo che accompagni i titolari e i responsabili all’uso dei documenti, dei dati e delle procedure nel rispetto della normativa privacy

processi ispettivi: definire e documentare i processi ispettivi (auditing interno) sull’utilizzo del prodotto in conformità alla normativa privacy

reingegnerizzazione dei processi per trattamento privacy “data protection by default and by design”

analisi dei rischi inerente il trattamento dei dati: impostare un sistema di valutazione dei processi e delle tecnologie utilizzate

documentazione e manutenzione: tutti i processi realizzati col software devono essere ben documentati, in particolare per gli aspetti relativi alla privacy. La manutenzione dei processi deve prevedere una costante parallela manutenzione della relativa documentazione

supporto agli interessati dei documenti gestiti (help desk, reclami, richieste di portabilità, ecc.)

supporto alla migrazione della raccolta dei consensi precedente alla data di avvio del nuovo codice o richiesta nuova per completamento dei dati

Registro delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Comune quale Titolare del trattamento, reca almeno le seguenti informazioni:

- il nome ed i dati di contatto del Comune, eventualmente del Contitolare del trattamento, del RPD
- le finalità del trattamento
- la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute)
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario
- l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate

Schema del registro attività di trattamento (fonte quaderno ANCI)

A) Registro attività di trattamento

REGISTRO ATTIVITA' DI TRATTAMENTO (art. 30, c.1, GPRD)

ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Registro tenuto da**	
Indirizzo		**Data di creazione**	
N. telefono		**Ultimo aggiornamento**	
Mail		**N. schede compilate**	
PEC		**Prossima revisione**	

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale Rappres.nte)	Categoria	Dati sensibili (SI/NO)	Termine ultimo cancell.ne	Categoria	Consenso (SI/NO)	Categoria	Paesi terzi, org.ni int.li (eventuale) (SI/NO)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

Registro delle categorie di attività

Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento reca le seguenti informazioni:

- il nome ed i dati di contatto del Responsabile del trattamento e del RPD
- le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione
- l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Schema Registro delle categorie di attività (fonte quaderno ANCI)

B) Registro categorie di attività di trattamento

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art. 30, c.2, GPRD)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile del trattamento**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
Delegato dal Titolare (eventuale)		**Responsabile protezione dati**	
Indirizzo		Indirizzo	
N. telefono		N. telefono	
Mail		Mail	
PEC		PEC	
		Registro tenuto da	
		Data di creazione	
		Ultimo aggiornamento	
		N. schede compilate	
		Prossima revisione	

	TRATTAMENTO				TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Categorie	eventuale diverso Titolare e/o Contitolare (eventuale Rappres.nte)	Paesi terzi, org.ni int.li (eventuale)	Misure tecniche ed organizzative adottate

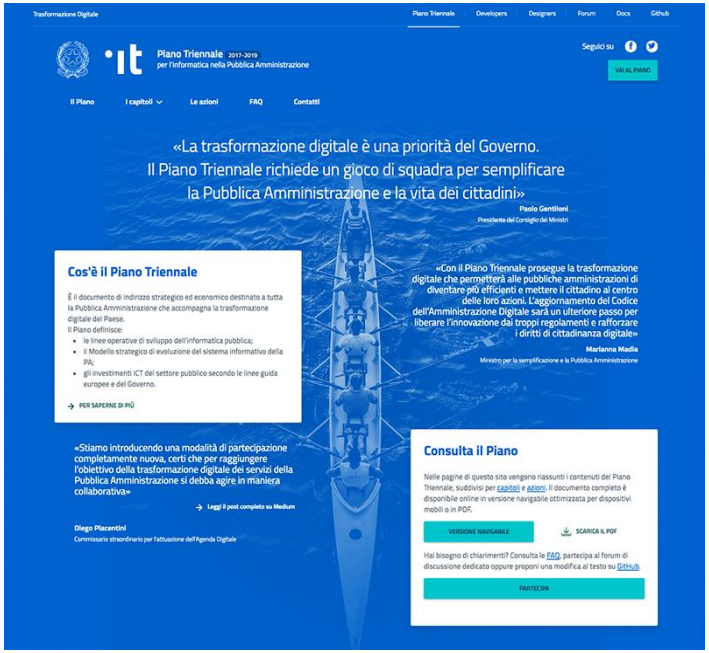
GDPR – Gli Impatti informatici

- **Analisi dei rischi e revisione dei piani di sicurezza (Dpia)**
  - adeguamento ai regolamenti sulla sicurezza
  - disposizioni del CAD (codice dell'Amministrazione digitale dlgs 82 del 2005)
  - piano triennale per l'ICT della PA (Circolare Agid 24/6/2016, n. 216 razionalizzazione dei CED)
- **Analisi delle basi dati aziendali**

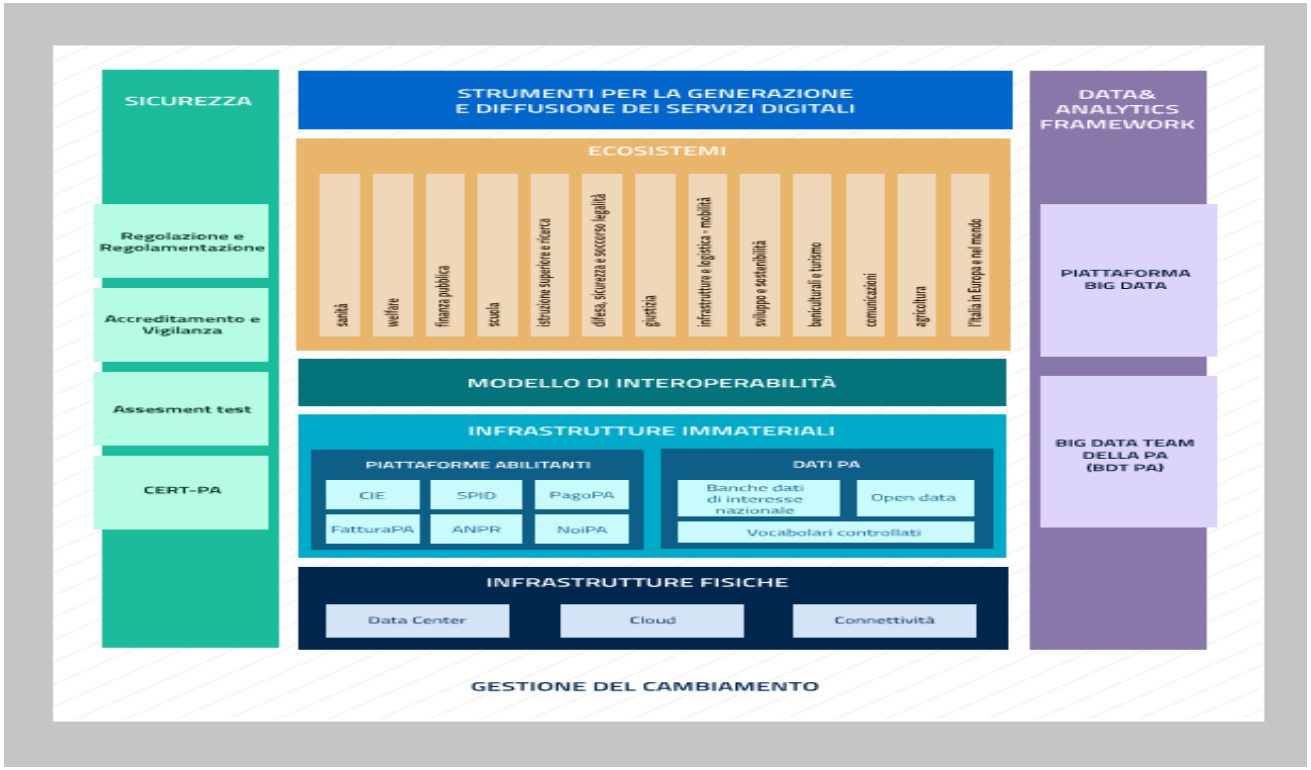
  accelerazione adozione di banche dati nazionali (ANPR, CIE) e strumenti e servizi di livello nazionale (es. SUAP, NOIPA, centrali di committenza COMPROPA, PAGOPA)
- **Adeguamenti del software di gestione documentale quale orchestratore dei processi informativi dell'ente**
  - Profilazione degli utenti per assegnazione dei diritti di accesso ai dati
  - Automazione del registro dei trattamenti attraverso la gestione dei metadati
  - gestione dei diritti: di accesso, di oblio, di limitazioni del trattamento, di portabilità
- **Adozione di sistemi di conservazione a norma dei dati e dei documenti**
  - Adesione ai poli archivistici regionali

Il Piano Triennale: cos'è

È il documento di indirizzo strategico ed economico destinato a tutta la Pubblica Amministrazione che accompagna la trasformazione digitale del Paese.
Il Piano definisce:
le linee operative di sviluppo dell'informatica pubblica;
il Modello strategico di evoluzione del sistema informativo della PA;
gli investimenti ICT del settore pubblico secondo le linee guida europee e del Governo.



Il Modello Strategico



IL GDPR – Le Sanzioni

L'articolo 83 del GDPR stabilistisce «**le condizioni generali per infliggere sanzini amministrative pecuniarie**» all'ente o impresa che disattende le disposizioni del regolamento.

L'autorità di controllo provvede affinchè le sanzioni amministrative pecuniarie inflitte ai sensi dell'articolo 83 del GDPR siano in ogni singolo caso **effettive, proporzionate e dissuasive**

Le sanzioni amministrative amministrative sono inflitte in ragione delle circostanze di ogni singolo caso tenendo conto degli elementi indicati nel comma 2 del citato articolo 83 (natura , gravità, carattere doloso, il grado di responsabilità, ...)

Le violazioni delle disposiizoni è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 di euro e per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente

Formazione IFEL
per i Comuni

IFEL
Fondazione ANCI

Grazie per l'attenzione

Maria Pia Giovannini
ICT Senior Advisor
mp.giov@gmail.com

I materiali didattici saranno disponibili su
www.fondazioneifel.it/formazione

Twitter Facebook YouTube