APTB
ASSOCIAZIONE PROFESSIONISTI TECNICI BRESCIANI

in collaborazione con

AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro

SEMINARIO TECNICO

Il Regolamento (UE) 2016/679 – GDPR

Relatore: Giuseppe Galgano

BRESCIA, 28 maggio 2018 - dalle ore 14.30 alle ore 17.30

A Partner of VISION ZERO
Safety.Health.Wellbeing.

CONFCOMMERCIO
IMPRESE PER L'ITALIA

CIIP
Consulta Interassociativa Italiana per la Prevenzione

Media Partner

PuntoSicuro

AMBIENTE&SICUREZZA
Aggiornamento giuridico, normativa tecnica e applicazioni

AiFOS APTB

DI COSA PARLEREMO
Prima parte

- PROTEZIONE DEI DATI PERSONALI
  - Dove nasce, l'evoluzione in Europa e quella in Italia
  - Perché se ne sta parlando tanto
  - Siamo consapevoli? Gli utenti e le organizzazioni
  - La normativa di riferimento e chi controlla

AiFOS APTB

DI COSA PARLEREMO
Seconda parte

- Il GDPR
  - Aspetti generali
  - La novità
  - Le regole base del trattamento
  - Le sanzioni
  - Le figure coinvolte nella tutela dei Dati Personali
  - Ulteriori novità
  - I diritti dell'interessato

- LE ORGANIZZAZIONI - Come tutelarsi e le principali azioni da compiere

- DOMANDE

AiFOS APTB

Giuseppe GALGANO

Esperienze in ambito Data Protection

- Consulenza alle organizzazioni in ambito del Trattamento dei Dati Personali.
- Formatore sulla tematica Data Protection, relatore presso convegni e commissario in sessioni di esame per certificazione DPO.
- Coordinatore del Gruppo DPO-Data Protection di Federmanager Roma.
- Autore di articoli di divulgazione sull'argomento e coautore del testo "La certificazione della Data Protection" - Freni Angelo Editore.

Certificazioni/Qualificazioni

- Data Protection Officer
- Data Protection Auditor/Lead Auditor
- AXELOS M_o_R® (2010) Foundation
- Privacy Implementer PECB-CLPI ISO29100™
- Privacy Consultant

Il problema non è fare la cosa giusta …

… ma sapere quale sia la cosa giusta.

Lyndon B. Johnson

PROTEZIONE DEI DATI PERSONALI

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI

Esistono persone che NON posseggono

Dati Personali?

Esistono organizzazioni che NON utilizzano

Dati Personali?

L'argomento ci coinvolge tutti!

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Dove nasce

De «**Il diritto di essere lasciato in pace»**
(to be let alone)

e de «**Il diritto alla riservatezza»**

se ne inizia a parlare negli Stati Uniti, anche a seguito dell'utilizzo di una nuova tecnologia, la fotografia, e della facile diffusione di immagini private.

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Dove nasce

In Italia forte impulso al dibattito fu fornito da alcune sentenze della Corte di Cassazione riguardanti, ancora una volta, la diffusione di informazioni e immagini attraverso la stampa.

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Perché se ne sta parlando tanto

Oggi, in tutto il mondo, nuove tecnologie stanno *provvedendo* a diffondere una grande mole di dati …

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Perché se ne sta parlando tanto

In Europa il percorso è stato disomogeneo fino a che, nel 1950, il diritto al rispetto della vita privata fu consacrato dall'art. 8 della **Convenzione Europea**.

Nel 2000 la *Protezione dei dati di carattere personale* è sancito come diritto fondamentale dall'art. 8 della **Carta dei diritti fondamentali dell'Unione europea**.

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli?

Ognuno di noi è consapevole dell'importanza dei propri Dati Personali? … e di come li sta usando?

Le organizzazioni sono consapevoli dell'importanza di un corretto uso dei Dati Personali?

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

Siamo consapevoli?

Gli utenti

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

Ingenuità della gente riguardo i propri dati personali

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

Ma i nostri Dati Personali interessano a qualcuno?

Quale è, nel mondo, l'azienda a maggior capitalizzazione?

Alphabet A + Alphabet C

=

1.056.679 milioni di €

(fonte: tabella pubblicata su Plus del Sole24ore il 27/01/2018)

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

Questo è quello che ci appare quando apriamo Google

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

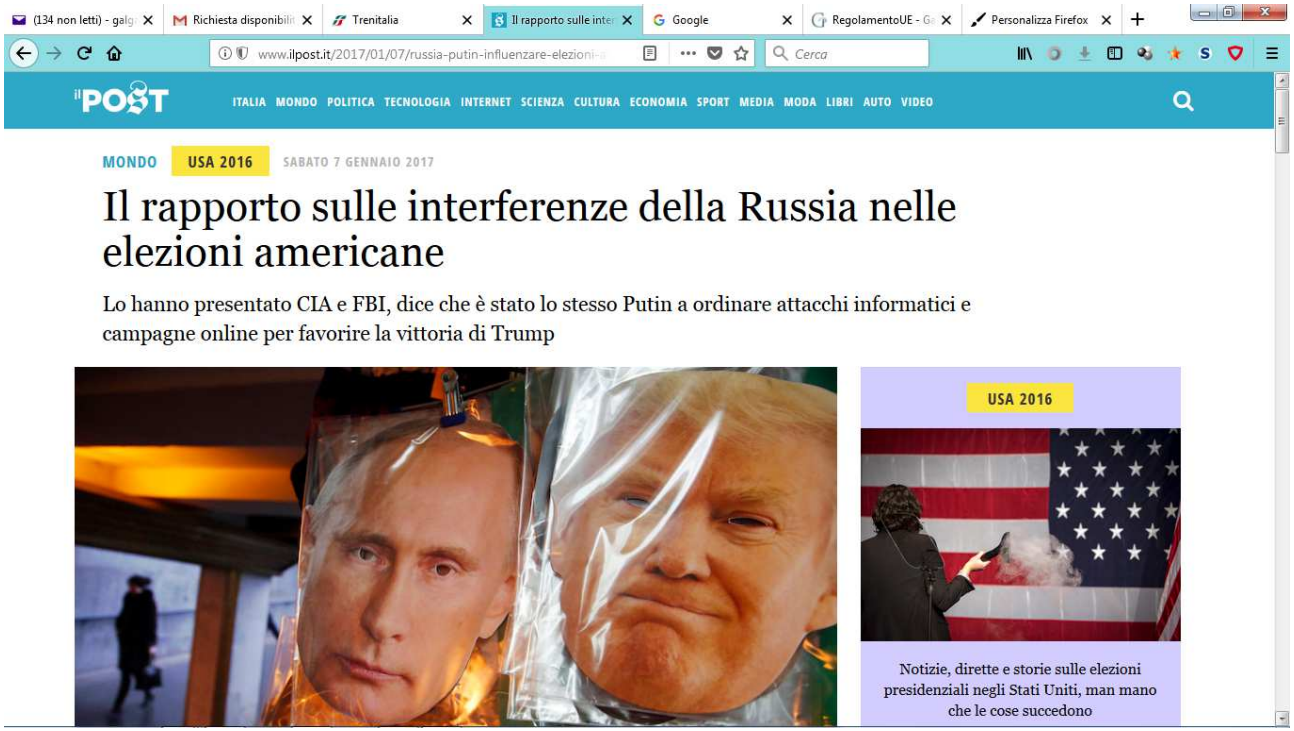
Perché è importante proteggere i nostri Dati Personali?

- Pubblicità *non gradite*
- Concorrenza sleale
- Discriminazioni
- Manipolazioni
- … …

Il Regolamento (UE) 2016/679 – GDPR

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti



Utilizzando in modo *raffinato* i Dati Personali si possono manipolare le persone o le masse

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Gli utenti

Ognuno di noi è consapevole dell'importanza dei propri Dati Personali? … e di come li sta usando?

- sono nostri
- interessano alle aziende
- potrebbero essere utilizzati diversamente da come vorremmo

È importante che ognuno di noi sappia utilizzarli e proteggerli

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Siamo consapevoli?

Le organizzazioni

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Conformità, o compliance aziendale

La conformità normativa a leggi, regole o standard indica il rispetto di specifiche disposizioni impartite dal legislatore, da autorità di settore, da organismi di certificazione nonché da regolamentazioni interne alle società stesse.

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Tutte le organizzazioni (grandi, piccole, ditte individuali, professionisti, ecc.) verificano costantemente che le attività siano coerenti con l'obiettivo di **prevenire la violazione di norme** di etero-regolamentazione (leggi e regolamenti) e auto-regolamentazione (codici di condotta, codici etici).

Il fine è quello di evitare:

- **sanzioni**
- **perdite finanziarie**
- **danni di reputazione**

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Money transfer: Garante privacy, 11 mln di multa a cinque società per uso illecito di dati

Sanzioni per oltre 11 milioni di euro sono state comminate dal Garante privacy a cinque società che operano nel settore del money transfer per aver usato in modo illecito i dati personali di più di mille persone inconsapevoli

(estratto da: www.garanteprivacy.it)

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

… TUTTO CIO' PREMESSO

IL GARANTE

nei confronti di Conerobus S.p.A.:
a) dichiara illecito, nei termini indicati in motivazione, il trattamento dei dati personali degli interessati effettuato mediante la comunicazione a soggetti non legittimati delle ragioni di assenza dal servizio del personale, in violazione degli artt. 11. comma 1, lett. a) e d), 24, 26 del Codice; …

Roma, 3 luglio 2014

(estratto da: www.garanteprivacy.it)

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Tutte le organizzazioni (grandi, piccole, ditte individuali, professionisti, ecc.) verificano costantemente che le attività siano coerenti con l'obiettivo di **prevenire la violazione di norme** di etero-regolamentazione (leggi e regolamenti) e auto-regolamentazione (codici di condotta, codici etici).

Il fine è quello di evitare:

- **sanzioni**
- **perdite finanziarie**
- **danni di reputazione**

ma anche quello di:

guadagnarsi e mantenere la fiducia degli interessati

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

I Dati Personali vengono AFFIDATI dalle persone fisiche (interessati) alle organizzazioni (titolari del trattamento)

Affidare:

- dare in custodia, consegnare all'altrui capacità, cura o discrezione
- assicurare, ispirare fiducia

(estratto da: www.treccani.it)

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Gli interessati sono i **proprietari** dei propri Dati Personali

Gli interessati **affidano** ai titolari i propri Dati Personali

I titolari del trattamento, nel gestire i Dati Personali, devono **guadagnarsi e mantenere** la fiducia degli interessati

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Gran Bretagna: attacco hacker a gestore telefonico TalkTalk.
A rischio i dati di 4 milioni di utenti

Alcuni utenti hanno già denunciato che sono state sottratte centinaia di sterline dai loro conti dopo che i pirati informatici hanno colpito. A TalkTalk inoltre è arrivata un'insolita "richiesta di riscatto", tramite un'email, di cui non è stata rivelata l'entità. E' probabile che il riscatto riguardi proprio i dati che sono stati sottratti nel corso dell'attacco

23 ottobre 2015

Fonte: http://www.rainews.it/

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI

Siamo consapevoli? Le organizzazioni

FINECO BANK

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli? Le organizzazioni

Le organizzazioni sono consapevoli dell'importanza di un corretto uso dei Dati Personali?

- sanzioni
- perdite finanziarie
- danni di reputazione
- guadagnarsi e mantenere la fiducia degli interessati

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Siamo consapevoli?

Interessati e **titolari** come possono cautelarsi?

Acquisendo maggiore consapevolezza

Conoscendo e applicando le regole

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

Fonti di diritto derivato: due strumenti della UE

Le DIRETTIVE

Sono indirizzate solo agli Stati membri e non sono obbligatorie in tutti i loro elementi, in quanto vincolano i destinatari solo riguardo al risultato da raggiungere, lasciando alla loro discrezione la scelta dei mezzi e della forma

I REGOLAMENTI

Hanno una portata generale, sono obbligatori in tutti i loro elementi e direttamente applicabili

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

Le istituzioni UE hanno colto l'importanza della Protezione dei Dati Personali e hanno affrontato la tematica tramite:

- **Direttiva 95/46 CE (Tutela e libera circolazione dei dati personali)**
- Direttiva 2002/58 CE (Telecomunicazioni)
- Direttiva 2006/24 CE (Conservazione di dati)
- Decisione quadro 977/2008 (dati scambiati dalle autorità di polizia)
- Direttiva 2009/136 CE (E-Privacy)
- …

I testi dei documenti sono disponibili nel sito http://eur-lex.europa.eu

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

In Italia la direttiva 95/46 CE è stata recepita tramite il

D.Lgs. 196 del 30 giugno 2003

Codice in materia di protezione dei dati personali

Il testo del Codice Privacy è disponibile nel sito http://www.garanteprivacy.it

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

Il *Codice della Privacy*

ha, tra le altre, disciplinato

l'***Autorità Garante per la protezione dei dati personali***

(G.P.D.P.)

autorità amministrativa indipendente che si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Chi controlla

1997 2017

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Il logo dell'Autorità garante

Il Presidente dell'Autorità garante Antonello Soro

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI

Chi controlla

Guardia di Finanza - Nucleo Speciale Privacy

Sede: ROMA
Prov.: RM
C.a.p.: 00155
Indirizzo: Via Fortunato Depero, 76
Telefono: 06225941

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

Rispetto alla normativa di base adottata oltre 20 anni fa sono intervenuti:

1. **Cambiamenti nel contesto**
    - Fenomeno della globalizzazione
    - Nuove tecnologie
    - Nuovi servizi collegati alle nuove tecnologie
2. **Frammentazione e disomogeneità del quadro normativo**
    - Tempi e modi diversi, da parte dei 28 paesi membri, di recepire la direttiva 95/46 CE e le successive norme
    - Provvedimenti in materia Privacy adottati dai singoli stati

Per dare una risposta ai due punti nasce la nuova normativa europea …

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

25 MAGGIO 2018

totalmente applicabile il

REGOLAMENTO (UE) 2016/679

DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

«Il Regolamento raggiunge l'ambizioso obiettivo di assicurare una disciplina uniforme ed armonizzata tra tutti gli Stati membri, eliminando definitivamente le numerose asimmetrie che si erano create nel tempo.»

Antonello Soro
Presidente dell'Autorità Garante

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

… e il Codice della Privacy che fine fa?

… ma ci sarà una proroga?

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
La normativa

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Gdpr, Garante privacy: nessuna pronuncia su differimento applicazione sanzioni

Con riferimento a notizie circolanti in Internet è necessario precisare che non è vero che il Garante per la protezione dei dati si sia pronunciato sul differimento dello svolgimento delle funzioni ispettive e sanzionatorie né il provvedimento richiamato nei siti attiene a tale materia.

Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo fissata al 25 maggio 2018.

Roma, 19 aprile 2018

AiFOS APTB

Il GDPR

AiFOS APTB

Il GDPR
Aspetti generali

Il Regolamento

- definisce i principi
- governa i rapporti tra i vari attori coinvolti

al fine di tutelare i dati personali delle persone fisiche

Il GDPR
Aspetti generali

Articolo 1
Il regolamento stabilisce norme relative alla protezione delle **persone fisiche**.

Articolo 2 (ambito materiale)
Il regolamento si applica al **trattamento** interamente o parzialmente automatizzato **di dati personali** e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

AiFOS APTB

Il GDPR
Aspetti generali

Articolo 4

Il dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Il GDPR
Aspetti generali

Articolo 4

Il 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

AiFOS APTB

Il GDPR
Aspetti generali

Articolo 3 (ambito territoriale)
Le disposizioni del Regolamento si applicano ai Titolari:

- stabiliti con le proprie attività **in uno o più Paesi Membri UE**
- stabiliti **al di fuori della UE** ma con attività di trattamento dati, di individui che si trovano nella UE, in relazione a:
  - offerta di beni e/o servizi anche se non remunerati
  - attività di monitoraggio del comportamento

AiFOS APTB

Il GDPR
La novità

- **Accountability**
  Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate** per garantire, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Il GDPR
Le regole base del trattamento

I dati personali devono essere

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza**)
- raccolti per finalità determinate, esplicite e legittime (**limitazione della finalità**)
- esatti e, se necessario, aggiornati; ovvero cancellati o rettificati tempestivamente rispetto alle finalità per le quali sono trattati (**esattezza**)

AiFOS APTB

Il GDPR
Le regole base del trattamento

I dati personali devono essere

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**)
- conservati in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**limitazione della conservazione**)
- trattati in maniera da garantirne un'adeguata sicurezza (**integrità e riservatezza**)

Il GDPR
Le regole base del trattamento

Il titolare del trattamento è competente per l'osservanza di questi principi fondamentali e deve essere in grado di comprovarne il rispetto.

AiFOS APTB

Il GDPR
Le sanzioni

Il Regolamento ha inasprito le sanzioni amministrative pecuniarie applicabili in caso di trattamento dei dati personali effettuato in modo non conforme a quanto previsto dalla normativa.

Stabilisce un importo massimo applicabile dal Garante e, ove si tratti di impresa, un metodo di quantificazione alternativo che consiste nel calcolo di una percentuale del fatturato mondiale annuo dell'esercizio precedente.

AiFOS APTB

Il GDPR
Le sanzioni

In presenza di violazioni gravi si potrà arrivare a sanzioni fino

a **20.000.000 di euro**

o (in caso di imprese)

al **4% del fatturato** mondiale annuo della società

(fra le due varrà la sanzione più gravosa)

Il GDPR
Le sanzioni

In aggiunta, il Regolamento riconosce all'interessato il diritto al risarcimento del danno dal titolare o dal responsabile del trattamento.

Inoltre, riconosce a ogni Stato membro la possibilità di stabilire ulteriori sanzioni, comprese eventuali sanzioni penali.

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

Il Regolamento prevede:

- Interessato
- Titolare del trattamento
- Contitolare del trattamento
- Responsabile del trattamento
- Persone autorizzate al trattamento
- Data Protection Officer (DPO) o Responsabile Protezione Dati (RPD)

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

Abbiamo già conosciuto

INTERESSATO

il proprietario del Dato Personale

TITOLARE DEL TRATTAMENTO

colui a cui vengono affidati i Dati Personali

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

L'INTERESSATO

Affida i suoi Dati Personali ai titolari e può esercitare diversi diritti, tra cui:

- ricevere, velocemente, tutte le informazioni sui suoi Dati Personali
- opporsi, in tutto o in parte, al trattamento
- "ottenere giustizia"

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il TITOLARE DEL TRATTAMENTO

È la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che singolarmente o insieme ad altri **determina le finalità, le condizioni e i mezzi del trattamento** di dati personali.

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il TITOLARE DEL TRATTAMENTO

Il Regolamento gli assegna alcuni obblighi; tra questi:

- garantire il rispetto dei diritti dell'interessato;
- notificare la violazione o il tentativo di violazione dei Dati Personali sia all'autorità di controllo sia, in alcuni casi, agli interessati;
- la conservazione della documentazione;
- fornire le istruzioni al personale;

continua …

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il TITOLARE DEL TRATTAMENTO

… segue *alcuni obblighi assegnati al titolare*:

- l'esecuzione della valutazione d'impatto sulla protezione dei Dati Personali;
- l'attuazione dei requisiti di sicurezza;
- il rispetto dei requisiti di autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo;
- la designazione del Data Protection Officer, quando necessaria;
- … …

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il TITOLARE DEL TRATTAMENTO

È il "**garante supremo**" della fiducia dell'interessato.

Risponde all'interessato e all'Autorità Garante del trattamento dei Dati Personali.

Con riguardo ai Dati Personali

meno delega …

… più ne deve sapere

Può avvalersi di figure di supporto.

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il RESPONSABILE DEL TRATTAMENTO

È la persona fisica o giuridica, a cui il titolare delega delle responsabilità con riferimento al trattamento di Dati Personali.

Quando il titolare affida all'esterno della propria organizzazione dei trattamenti, deve essere sempre individuato e formalmente nominato.

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il RESPONSABILE DEL TRATTAMENTO

esempi di affidamenti esterni

Gestione buste paga
Servizi di marketing
RSPP
Call center
Servizi di cloud
Servizi di assistenza informatica
Dismissione PC
…

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

Il RESPONSABILE DEL TRATTAMENTO

È individuato dal titolare tra coloro che, per **esperienza, capacità e affidabilità**, fornisce idonea garanzia circa il rispetto delle disposizioni vigenti in materia dei Dati Personali.

Nel Sistema Protezione Dati Personali la risorsa, l'organizzazione o il professionista nominati responsabile del trattamento devono avere **competenze elevate**.

Può rispondere di eventuali **danni** cagionati all'interessato.

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

Spetta al Titolare e al Responsabile:

- la definizione dei compiti, dei ruoli e delle responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, con particolare riferimento alla necessità di garantire la loro sicurezza;
- l'adozione di specifiche procedure atte a completare e rafforzare le contromisure tecnologiche presenti.

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Le PERSONE AUTORIZZATE al TRATTAMENTO

Il Regolamento non contiene definizioni formali per questa figura. Tuttavia specifica che il titolare deve fornire istruzioni alle persone autorizzate al trattamento dei dati personali.

Le istruzioni devono essere impartite tramite:

- formazione
- lettere
- mansionario
- disciplinare interno

AiFOS APTB

Il GDPR
Le figure coinvolte nella tutela dei Dati Personali

Il DPO o RDP

È una **figura di garanzia**, già contemplata da alcune legislazioni europee, introdotta in Italia dal Regolamento.

È designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali e della capacità di assolvere i compiti previsti dal Regolamento.

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il DPO o RDP

Quando è previsto (1)

Dovranno designare **obbligatoriamente** un Responsabile della protezione dei dati personali:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

continua …

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il DPO o RDP

Quando è previsto (2)

Dovranno designare **obbligatoriamente** un Responsabile della protezione dei dati personali:

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **controllo regolare e sistematico degli interessati su larga scala**;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di **categorie particolari di dati personali* o di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza**.

* Dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il DPO o RDP

I compiti

Il Regolamento specifica che il DPO deve almeno svolgere i seguenti compiti:

- **informare** e fornire consulenza al Titolare …;
- **sorvegliare** l'attuazione e l'applicazione …;
- **fornire**, se richiesto, un parere …;
- **cooperare** con l'Autorità di controllo …;
- **fungere** da punto di contatto per ….

Non è una figura operativa ma consultiva e di garanzia.

AiFOS APTB

Il GDPR

Le figure coinvolte nella tutela dei Dati Personali

Il DPO o RDP

Ma serve avere un DPO?

Va valutato caso per caso. Spetta al titolare del trattamento deciderlo considerando:

- il numero degli interessati coinvolti
- la quantità e il tipo di dati trattati
- la durata e la continuità delle operazioni di trattamento
- l'estensione geografica delle attività di trattamento

La sola presenza di un "vero" DPO **aumenta la conformità aziendale** alla normativa agli occhi dell'Autorità Garante, degli interessati e di tutti gli stakeholder.

AiFOS APTB

Il GDPR
Ulteriori novità

I Dati

"dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

"dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

"dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

AiFOS APTB

Il GDPR
Ulteriori novità

Categorie particolari di dati personali

Dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il Regolamento vieta il trattamento di categorie particolari di dati personali, ad eccezione dei seguenti casi:

- previo **consenso esplicito** al trattamento;
- nell'ambito delle **legittime attività** da parte di una fondazione, associazione o altro organismo senza scopo di lucro;
- per salvaguardare un **interesse vitale**;
- per accertare, esercitare o difendere un **diritto in sede giudiziaria**;

… segue

AiFOS APTB

Il GDPR
Ulteriori novità

Categorie particolari di dati personali

Il Regolamento vieta il trattamento di categorie particolari di dati personali, ad eccezione dei seguenti casi:

… continua

- per motivi di **interesse pubblico**;
- per finalità di archiviazione, storiche, statistiche o scientifiche nel pubblico interesse per **dati personali resi manifestamente pubblici dall'interessato** (laddove il trattamento sia effettuato nell'interesse dell'interessato);
- in materia di **diritto del lavoro, sicurezza e protezione sociale**;
- per finalità di **prevenzione diagnosi, assistenza o terapia medico-sanitaria o di medicina del lavoro** (se da parte o sotto la responsabilità di un professionista soggetto al segreto professionale).

AiFOS APTB

Il GDPR
Ulteriori novità

Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment)

Saranno richieste valutazioni d'impatto sulla protezione dei dati personali quando il trattamento, per la sua natura, il suo soggetto o le sue finalità, presenta rischi specifici per i diritti e la libertà degli interessati. Ad esempio i trattamenti riguardanti l'ubicazione, la salute, i dati biometrici, la videosorveglianza, i minori ecc.

Sicurezza del Trattamento

Tenuto conto dei risultati della valutazione di impatto, il Responsabile è l'incaricato del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta.

AiFOS APTB

Il GDPR
Ulteriori novità

Obbligo di notificazione in caso di violazione (Data Breaches)
Viene introdotto l'obbligo di notifica in caso di violazione dei dati personali all'autorità di controllo e in alcuni casi l'obbligo di comunicare l'accaduto anche all'interessato.

Corresponsabilità del Trattamento
Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi diventano contitolari del trattamento. Devono determinare tramite un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti Regolamento.

Viene istituito il comitato europeo per la protezione dei dati personali
Il Gruppo di lavoro dei Garanti Europei sarà sostituito dal Consiglio Europeo per la Protezione dei dati Personali. Viene prevista una "lead authority" quando sono coinvolti più stati membri.

AiFOS APTB

Il GDPR
Ulteriori novità

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Si tratta di nuovi obblighi che il Titolare avrà ancor prima di procedere al trattamento dei dati. Dovrà cioè pensare in un'ottica di Privacy già dal momento in cui disegna il nuovo hardware o software o semplicemente il nuovo servizio (by design). Inoltre, dovrà pensarlo con tutte le impostazioni di Privacy chiuse e non aperte come si è fatto finora (by default).

Si dovrà, quindi, prevedere:

- Minimizzazione dei dati personali già in fase di raccolta;
- Pseudonimizzazione dei dati personali;
- Sistemi già predisposti alla cancellazione dei dati dopo il termine stabilito;
- Accesso ai dati consentito solo per soggetti autorizzati al trattamento;
- Trasparenza nei confronti dei soggetti interessati con informative chiare;
- Modalità facili e veloci per consentire all'utente di avere accesso ai dati personali e controllare o modificare le condizioni del trattamento.

AiFOS APTB

Il GDPR
Ulteriori novità

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono specificati dal Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Il GDPR
Ulteriori novità

Informativa

Le informative all'interessato dovranno risultare più dettagliate e soprattutto più efficaci delle precedenti, usando anche moduli, schemi e disegni. Di seguito gli elementi essenziali con evidenziate le **novità rispetto al Codice Privacy**:

- l'identità e i dati di contatto del Titolare del trattamento e, **se designato, del DPO**;
- le finalità del trattamento e se il trattamento si basa su legittimi interessi perseguiti dal Titolare;
- i destinatari dei dati o le categorie di destinatari;
- se è previsto un trasferimento di dati all'Estero e **le garanzie esistenti a tutela** dei dati trasferiti;
- **il periodo temporale** previsto per la conservazione dei dati o **il criterio per determinarlo**;
- i diritti riconosciuti ai soggetti interessati;

… segue

AiFOS APTB

Il GDPR
Ulteriori novità

Informativa

… continua

- la possibilità di revocare il consenso in qualsiasi momento;
- **il diritto di proporre reclamo** ad un'autorità di controllo;
- **l'indicazione se la comunicazione di dati personali è un obbligo legale o è necessario** per la conclusione di un contratto;
- se l'interessato ha l'obbligo di fornire i dati e le possibili conseguenze di un rifiuto;
- se l'interessato sarà oggetto di attività **per il perseguimento del legittimo interesse de Titolare**.

Se i dati personali non sono conferiti direttamente dall'interessato, il Titolare del trattamento deve fornire anche:

- le categorie di dati personali trattati;
- la fonte dalla quale derivano i dati personali e se tale fonte è accessibile al pubblico.

AiFOS APTB

Il GDPR
Ulteriori novità

Consenso

Il consenso dovrà essere richiesto in modo chiaro ed espresso in modo inequivocabile. Dovrà essere sempre documentabile.

Condizioni specifiche sono previste per il consenso dei minori.

Il consenso non potrà essere utilizzato per giustificare trattamenti illeciti.

Il consenso dell'interessato è "qualsiasi manifestazione di volontà"…

LIBERA SPECIFICA INFORMATA INEQUIVOCABILE

dell'interessato, con la quale lo stesso manifesta il proprio assenso al trattamento mediante una sua

DICHIARAZIONE o AZIONE POSITIVA INEQUIVOCABILE

AiFOS APTB

Il GDPR
Ulteriori novità

ULTERIORE POSSIBILITÀ PER LA CONFORMITÀ (1)

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di **codici di condotta** destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

AiFOS APTB

Il GDPR
Ulteriori novità

ULTERIORE POSSIBILITÀ PER LA CONFORMITÀ (2)

L'Unione Europea intende promuovere la possibilità di predisporre **meccanismi di certificazione** per il rilascio di sigilli e marchi per la rapida valutazione da parte degli interessati e delle autorità coinvolte, al fine di stabilire con estrema rapidità il livello di protezione, di qualità e affidabilità dei dati gestiti.

AiFOS APTB

Il GDPR
I diritti dell'interessato

Dopo aver affidato i propri dati personali a un titolare del trattamento, **l'interessato non ne perde la proprietà**; per la propria tutela può esercitare dei diritti nei confronti del titolare.

Il titolare deve **agevolare** l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile deve collaborare con il titolare per l'esercizio dei diritti degli interessati.

AiFOS APTB

Il GDPR
I diritti dell'interessato

Il termine per la risposta all'interessato è, per tutti i diritti, **1 mese**, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

L'esercizio dei diritti è, in linea di principio, **gratuito**.

AiFOS APTB

Il GDPR
I diritti dell'interessato

- Diritto di accesso
- Diritto di rettifica
- Diritto alla cancellazione («diritto all'oblio»)
- Diritto di limitazione di trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione
- Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Fiducia
Responsabilizzazione
Leggi
Sanzioni
e anche adempimenti e obblighi
… …

Come fare per essere conformi?

Come tutelare i Dati Personali?

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Da dove si inizia

Intanto, ogni organizzazione dovrebbe tutelare i propri dati aziendali (i Dati Personali sono un di cui dei dati aziendali) …

Audi assume hacker per arginare gli attacchi informatici

(fonte Il sole 24 ore; 21/08/2017)

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

… ma questo non basta:

ogni pezzo di un'organizzazione deve sapere **come trattare i Dati Personali** con cui viene in contatto …

… e questo vale per tutti!

FINECO BANK

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Tutto questo imporrà alle imprese **l'adozione di un vero e proprio modello organizzativo** per la tutela dei Dati Personali.

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Passi operativi (1)

- Redazione della politica per la protezione dei dati personali dell'istituto
- Individuazione dei trattamenti effettuati e delle relative basi legali
- Valutazione dei rischi per ogni trattamento
- Individuazione e implementazione delle eventuali e adeguate azioni di riduzione dei rischi
- Predisposizione di:
  - informativa interessati esterni (clienti, associati, iscritti, ecc.)
  - informativa interessati interni (dipendenti, collaboratori «stabili», stagisti, ecc.)
  - informative sito web e cookie
  - procedura Gestione del consenso degli interessati
  - regolamento utilizzo strumenti aziendali

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Passi operativi (2)

- Predisposizione di
  - procedura gestione violazioni e schede sintetiche di supporto: cosa fare e come agire
  - procedura gestione diritti degli interessati
  - predisposizione Linee guida valutazione fornitori
  - regolamento gestione videosorveglianza e informativa completa (se presente)
- Predisposizione e formalizzazione di:
  - nomine a Responsabile del Trattamento per fornitori a cui vengono affidati trattamenti
  - clausole protezione dati personali per fornitori che non hanno accesso ai dati
  - nomina dell'Amministratore di sistema

AiFOS APTB

LE ORGANIZZAZIONI
Come tutelarsi e le principali azioni da compiere

Passi operativi (3)

- Gestione documenti privacy - istruzioni per la conservazione dei documenti cartacei/elettronici fino al loro eventuale smaltimento/distruzione
- Guida operativa per IT
- Progettazione ed erogazione corsi per personale interno differenziati in base alle attività effettuate con i dati personali
- Redazione del registro del trattamento
- Revisione annuale privacy: aggiornamenti documentali, piano di audit, ecc.
- Individuazione e nomina del DPO e relativa comunicazione all'Autorità Garante

AiFOS APTB

PROTEZIONE DEI DATI PERSONALI
Come tutelare i Dati Personali

AiFOS

sta predisponendo numerose e diverse iniziative per supportare ogni esigenza di Data Protection.

Ognuno individui quella più appropriata e utile.

Per maggiori info: formarsi@aifos.it

Può darsi che non siate responsabili per la situazione in cui vi trovate, ma lo diventerete se non fate nulla per cambiarla.

Martin Luther King

AiFOS APTB

GRAZIE PER L'ATTENZIONE

Giuseppe GALGANO
giuseppe.galgano@privacyinchiaro.it

AiFOS APTB

DOMANDE

AiFOS APTB

DISCLAIMER
REGIME DI UTILIZZO DELLE SLIDES

Le presenti slide vanno considerate quale mera esemplificazione delle materie trattate.

Nessuna responsabilità legata ad una decisione assunta sulla base delle informazioni qui contenute potrà, quindi, essere attribuita al professionista o ad AiFOS.

È vietato l'utilizzo delle slide.

Grazie per l'attenzione!

AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro

APTB
ASSOCIAZIONE PROFESSIONISTI TECNICI BRESCIANI