NEOSTUDIO
BUSINESS DATA PROTECTION

GDRP 2016/679: Conformi entro il 2018

-

Il Nuovo Regolamento Europeo in materia di Protezione dei Dati Personali

Linux Day 2017

Università degli Studi di Palermo

NEOSTUDIO
BUSINESS DATA PROTECTION

CHI SONO?

Adriano Bertolino

Data Protection Officer (DPO)| Consulente della Privacy

Consulente e formatore in materia di protezione dei dati personali

Dal 2001 mi occupo di consulenza tecnico-giuridica e formazione in materia di protezione dei dati personali per Pubbliche Amministrazioni ed imprese in tutti i settori di mercato. Sono chiamato relatore in numerosi convegni e seminari di approfondimento in tema di privacy e sicurezza dei dati personali in manifestazioni nazionali ed internazionali.

La pluriennale esperienza ha permesso di definire un profilo professionale altamente specializzato quale Data Protection Officer (DPO).

Certificato TÜV Italia n° CDP_272
conforme ISO/IEC 17024:2012

a.bertolino@neostudio.it

about.me/adrianobertolino

it.linkedin.com/in/adrianobertolino

EVOLUZIONE NORMATIVA

NEOSTUDIO
BUSINESS DATA PROTECTION

Direttiva Europea n. 95/46/CE

Legge n. 675/96 Legge sulla Privacy

D.Lgs. n. 196/2003 Codice della Privacy

REGOLAMENTO (UE) n. 2016/679

REGOLAMENTO (UE) 2016/679

Disciplina unica in tutti gli Stati a protezione dei cittadini europei anche in Extra-UE

NEOSTUDIO
BUSINESS DATA PROTECTION

Temi disciplinati dal Regolamento UE 2016/679

NEOSTUDIO
BUSINESS DATA PROTECTION

PRINCIPALI DEFINIZIONI

L’ Articolo 4 del **G**eneral **D**ata **P**rotection **R**egulation descrive le definizioni fondamentali per comprendere l’applicazione del Regolamento UE

- Dato Personale
- Trattamento
- Pseudoanonimizzazione
- Profilazione on line
- Consenso esplicito dell'interessato
- Titolare e Responsabile del trattamento
- Responsabile della protezione dati (Data Protection Officer)
- Valutazione d’Impatto Privacy (DPIA)
- Violazione dei dati personali (Data Breach)
- Trattamento transfrontaliero
- Norme vincolanti d'impresa

NEOSTUDIO
BUSINESS DATA PROTECTION

DATI PERSONALI

Cosa sono?

NEOSTUDIO
BUSINESS DATA PROTECTION

DATO PERSONALE

«Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); […], <u>direttamente o indirettamente</u>»

- Nome;
- Numero identificazione; (C.F./Matricola)
- Dati relativi all'ubicazione; (GPS, tag RFID)
- Identificativo online; (Login, IP, Cookies)

- Elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

(Immagine, Impronta, Iride, Comportamento, Etnia, Status sociale e Economico)

NEOSTUDIO
BUSINESS DATA PROTECTION

DATI PERSONALI

Quanto valgono?

[Calcolatore del valore dei dati personali](http://ig.ft.com/how-much-is-your-personal-data-worth/)

http://ig.ft.com/how-much-is-your-personal-data-worth/

NEOSTUDIO
BUSINESS DATA PROTECTION

NEOSTUDIO
BUSINESS DATA PROTECTION

DATI SENSIBILI (art.9)

- L'origine razziale ed etnica;
- Le convinzioni religiose o filosofiche;
- Le opinioni politiche;
- L'adesione a partiti, sindacati, associazioni a carattere religioso, politico o sindacale;
- Dati biometrici
- Dati genetici
- Lo stato di salute e la vita e l'orientamento sessuale

DATI GIUDIZIARI (art. 10)

- Provvedimenti di cui al casellario giudiziario e all'anagrafe delle sanzioni amministrative dipendenti da reato (D.lgs.231/2001)
- Condanne penali e ai reati o a connesse misure di sicurezza
- La semplice qualità di imputato o indagato ai sensi del codice di procedura penale

DATO COMUNE/IDENTIFICATIVO

I dati personali identificativi esclusi dalle categorie dei dati Sensibili (art. 9, GDPR) e dati Giudiziari (art. 10, GDPR).

NEOSTUDIO
BUSINESS DATA PROTECTION

RUOLI ORGANIZZATIVI PRIVACY

NEOSTUDIO
BUSINESS DATA PROTECTION

TITOLARE DEL TRATTAMENTO

La *persona fisica, persona giuridica,* ente o associazione cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e modalità del trattamento ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

NEOSTUDIO
BUSINESS DATA PROTECTION

AMMINISTRATORE DI SISTEMA

NEOSTUDIO
BUSINESS DATA PROTECTION

Deve possedere particolari caratteristiche:

- Requisiti tecnico-organizzativi;
- Qualità di affidabilità e onorabilità professionali;
- **Esperienza e competenza** di settore, anche sotto il profilo della sicurezza per garantire pieno rispetto delle normative vigenti in materia di protezione dei dati personali.

Provv. generale del 27/11/2008

PROVVEDIMENTO DEL GARANTE RELATIVI AL RUOLO DI AMMINISTRATORE DI SISTEMA

NEOSTUDIO
BUSINESS DATA PROTECTION

Registrazione degli accessi

- Devono essere adottati sistemi per la registrazione degli accessi logici (autenticazione informatica) ai sistemi informatici **soltanto** da parte degli amministratori di sistema;
- Gli access log devono garantire caratteristiche di completezza, inalterabilità e integrità oltre ai riferimenti temporali e descrizione dell'evento generato;
- I dati di log devono essere conservati per un periodo, non inferiore a sei mesi;

DPO: DATA PROTECTION OFFICER

Quali caratteristiche?

NEOSTUDIO
BUSINESS DATA PROTECTION

Art. 37 - GDPR

‘’designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati’’

DPO: DATA PROTECTION OFFICER

Quali compiti?

NEOSTUDIO
BUSINESS DATA PROTECTION

DPO: DATA PROTECTION OFFICER

Quali competenze e posizione?

NEOSTUDIO
BUSINESS DATA PROTECTION

1. Deve possedere competenze giuridiche, informatiche, di risk management e di analisi dei processi;
2. Si relaziona direttamente con i vertici gerarchici Titolare o Responsabile;
3. Deve svolgere i propri compiti in modo autonomo ed indipendente;
4. Non deve essere individuato tra soggetti che per funzioni o ruoli potrebbero determinare un conflitto d’interesse;

L'INTERESSATO

La persona *fisica* a cui si riferiscono i dati personali oggetto di trattamento

Il Regolamento UE ne tutela i diritti e le libertà fondamentali, a cui corrispondono i doveri di chi effettua il trattamento di dati personali

NEOSTUDIO
BUSINESS DATA PROTECTION

TRATTAMENTO DEL DATO PERSONALE

NEOSTUDIO
BUSINESS DATA PROTECTION

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:

- raccolta,
- registrazione,
- organizzazione,
- strutturazione,
- conservazione,
- adattamento o modifica,
- estrazione,
- consultazione,
- uso,
- comunicazione mediante trasmissione,
- diffusione o qualsiasi altra forma di messa a disposizione,
- raffronto o interconnessione,
- limitazione,
- cancellazione o distruzione;

I CONTROLLI

Ad oggi esistono due fonti di rischio principali in relazione ai controlli:

a) Su iniziativa dei soggetti precedentemente identificati (livello basso o medio-alto in caso si sia soggetti a notifica);
b) A seguito di segnalazione al Garante previa richiesta di esercizio dei diritti (livello alto in caso di non corretta gestione dei rapporti con l'interessato);

NEOSTUDIO
BUSINESS DATA PROTECTION

NEOSTUDIO
BUSINESS DATA PROTECTION

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'Autorità Garante ha il compito di:

- Verificare l'applicazione del Regolamento UE;
- Emanare pareri e provvedimenti generali interpretativi delle norme vigenti e Linee guida;
- Essere giudice nei procedimenti di tipo stragiudiziale su istanza dell'interessato;
- Emanare autorizzazioni generali;

IL POTERE DI INDAGINE DEL GARANTE

Il Garante può effettuare ispezioni volte a verificare l'applicazione delle norme con i propri ispettori.

oppure

Tramite la Guardia di Finanza in virtù di un Protocollo d'intesa stipulato nel 2005 (**Nucleo Speciale Privacy**) che verifica l'organizzazione e l'adeguamento alla norme vigenti sulla data protection.

NEOSTUDIO
BUSINESS DATA PROTECTION

PARTE SECONDA

COSA FARE PER ADEMPIERE AL REG. (UE) 2016/679:

- Informativa e Consenso
- Valutazione d'impatto privacy e piano di sicurezza
- Misure di sicurezza adeguate al rischio
- Privacy by design e Privacy by default

INFORMATIVA E CONSENSO

Chi effettua il trattamento **deve** fornire l'Informativa (sempre obbligatoria) e acquisire il Consenso.

…l'Interessato ha diritto ad ottenere una serie di informazioni ed *ha diritto a prestare o meno* il consenso al trattamento!

COSA DEVE CONTENERE L'INFORMATIVA

NEOSTUDIO
BUSINESS DATA PROTECTION

L'informativa deve contenere (art. 13):

- Estremi identificativi e di contatto del Titolare e del DPO/RPD
- Legittimi interessi perseguiti dal Titolare del trattamento o da terzi;
- Base giuridica, finalità e modalità del trattamento;
- Tempi di conservazione;
- Destinatari ai quali i dati personali possono essere comunicati;
- Eventuali trasferimento di dati personali a Paesi UE o Extra-UE;
- Modalità di esercizio dei diritti

CONSENSO

Il Consenso deve essere in tutti i casi:

- libero, specifico, informato e inequivocabile e **NON** è ammesso il consenso tacito o presunto;
- Esplicito per il trattamento di dati sensibili;
- Nel caso di servizi online diretti a minori di 16 anni il trattamento è lecito se autorizzato da chi esercita la responsabilità genitoriale;

DIMOSTRABILE!!!

DIRITTO ALLA PORTABILITÀ DEI DATI (ART. 20)

NEOSTUDIO
BUSINESS DATA PROTECTION

L'interessato ha il diritto di **RICEVERE** in un formato **strutturato**, di **uso comune** e **leggibile da dispositivo automatico** i dati personali che lo riguardano forniti a un titolare del trattamento [...] **senza impedimenti** [...].

DIRITTO ALLA PORTABILITÀ DEI DATI (ART. 20)

Per quale motivazione?

1. Maggiore esercizio di controllo dell’interessato sui propri dati personali

2. Promuovere la concorrenza tra Titolari nella società dell’informazione

DIRITTO ALLA PORTABILITÀ DEI DATI (ART. 20)

Quando è applicabile?

NEOSTUDIO
BUSINESS DATA PROTECTION

Diritto alla portabilità dei dati (art. 20)

Come essere conforme?

NEOSTUDIO
BUSINESS DATA PROTECTION

Sviluppare ed applicare formati standard ed interoperabili

Misure di Sicurezza dei dati personali nel Regolamento UE 2016/679

art. 32 – General Data Protection Regulation

‘‘Tenendo conto dello stato dell’arte e dei costi di attuazione, […], come anche del rischio di varia **probabilità** e **gravità** per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative ***adeguate***…’’

NEOSTUDIO
BUSINESS DATA PROTECTION

DPIA: Data Protection Impact Assessment (art. 35)

NEOSTUDIO
BUSINESS DATA PROTECTION

Cos'è la DPIA?

E' una analisi da effettuare PRIMA di procedere al trattamento dati al fine di ***VALUTARE I RISCHI*** per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, così da identificare le misure necessarie per la mitigazione di tali rischi.

DPIA: Data Protection Impact Assessment (art. 35)

NEOSTUDIO
BUSINESS DATA PROTECTION

Quando è obbligatoria la DPIA?

Quando un trattamento "*possa presentare* ***un rischio elevato*** *per i diritti e le libertà delle persone fisiche*"

- In particolare in caso di:
  a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, compresa la profilazione;
  b) trattamento su larga scala di dati sensibili o giudiziari;
  c) sorveglianza sistematica su larga scala di zone di accesso pubblico;

e per tipologie di trattamenti *specificatamente indentificati* dal Garante

DPIA: Data Protection Impact Assessment (art. 35)

Quando è obbligatoria la DPIA?

Ma anche…

quando viene introdotta una nuova tecnologia che può comportare un rischio elevato nel trattamento dei dati personali

oppure

Siano intervenute variazioni dei rischi rilevati tenuto conto della natura, dell'ambito, del contesto e della finalità dei trattamenti

NEOSTUDIO
BUSINESS DATA PROTECTION

DPIA: Data Protection Impact Assessment (art. 35)

Cosa contiene la DPIA?

Data Protection Impact Assessment

- descrizione dei trattamenti previsti e delle finalità di tali trattamenti;
- valutazione della necessità e proporzionalità dei trattamenti;
- valutazione dei rischi per i diritti e le libertà degli interessati;
- misure previste per mitigare i rischi e dimostrare la conformità al GDPR;

NEOSTUDIO
BUSINESS DATA PROTECTION

DPIA: Data Protection Impact Assessment (art. 35)

La DPIA è un processo ciclico che prevede l'analisi continua dei possibili rischi elevati gravanti sul trattamento dei dati personali e l'adozione delle misure necessarie alle riduzione di tali rischi per i diritti e le libertà fondamentali delle persone fisiche

NEOSTUDIO
BUSINESS DATA PROTECTION

DPIA: Data Protection Impact Assessment (art. 35)

Qual è lo scopo delle DPIA?

E' un importante strumento per il Titolare,

per **raggiungere** e **dimostrare** la compliance al GDPR, in quanto rileva i rischi nel trattamento effettuato e descrive le misure di sicurezza adottate per ridurli.

Sostiene il principio di *accountability* (responsabilizzazione) del Regolamento UE 2016/679 *(art. 5 comma 2)*

NEOSTUDIO
BUSINESS DATA PROTECTION

Come devono essere Trattati? – art. 5 del GDPR

NEOSTUDIO
BUSINESS DATA PROTECTION

''Trattati in maniera da garantire **un'adeguata sicurezza dei dati** personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali''

Il Titolare del trattamento è responsabile della compliance di ogni trattamento effettuato e deve essere in grado di comprovarlo («**accountability**»)

Sources: Press reports; company statements; BCG analysis.
Note: Of the more than 1.8 billion records lost in these 50 data breaches, 490 million were excluded from our analysis because there was insufficient information to determine a root cause.

NEOSTUDIO
BUSINESS DATA PROTECTION

LE MAGGIORI CAUSE
DI DATA BREACH
DI DATI PERSONALI?

MANCANZA DI

CONSAPEVOLEZZA

DATA BREACH (art. 33)

NEOSTUDIO
BUSINESS DATA PROTECTION

- Comunicazione dell'evento al Garante **entro 72 ore.**

- Se la violazione comporti **elevati rischi** per i diritti e le libertà degli interessati andrà comunicato **tempestivamente** anche agli stessi.

Privacy by Design

NEOSTUDIO
BUSINESS DATA PROTECTION

Protezione dei dati personali già dalla fase di ideazione e progettazione di un trattamento, in modo da *prevenire* possibili rischi di violazione

[art. 25 - GDPR]

Privacy by Design

art. 25.1 – General Data Protection Regulation

‘‘Tenuto conto dello stato dell’arte e dei costi di attuazione,[…]delle finalità del trattamento, come anche dei rischi di probabilità e gravità, al momento di determinare i mezzi del trattamento e all’atto del trattamento stesso, il Titolare mette in atto misure tecniche ed organizzative adeguate quali la **pseudoanonimizzazione** e la **minimizzazione**.’’

NEOSTUDIO
BUSINESS DATA PROTECTION

NEOSTUDIO
BUSINESS DATA PROTECTION

Privacy by Design

art. 4 -5)

Pseudoanonimizzazione:

Una misura di protezione dei dati personali in modo che tali dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive.

Privacy by Design

Minimizzazione dei dati

Limitazione nel trattamento dei dati:

- Adeguati;
- Pertinenti;
- Limitati;
- Conservazione

Solo

i dati necessari rispetto alle finalità perseguite

Privacy by Default

Art. 25.2 – General Data Protection Regulation

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, **solo i dati personali necessari** per ogni **specifica finalità** del trattamento. Tale obbligo vale per la **quantità** dei dati personali raccolti,[…] il **periodo di conservazione** e l'**accessibilità**.[…]

NEOSTUDIO
BUSINESS DATA PROTECTION

I 7 principi fondanti della Privacy by Design

1. Sicurezza Proattiva e non reattiva / Preventiva e non correttiva;
2. Impostazioni di protezione dei dati di **default**;
3. Tutela dei dati personali **inclusa** nel progetto;
4. Massima funzionalità di protezione dei dati ($\Sigma>0$ e non $\Sigma=0$);
5. Sicurezza durante **tutto il ciclo** del trattamento, dalla raccolta alla distruzione;
6. Trasparenza nelle informazioni all'interessato;
7. Centralità dell'utente nel trattamento (**User Centric**);

NEOSTUDIO
BUSINESS DATA PROTECTION

I Vantaggi del "*Privacy by Design*"

- Individuazione in anticipo di potenziali difetti o anomalie, quando la correzione è spesso più semplice e meno costosa;
- Riduzione dei rischi di Data Breach o di eventuali eventi dannosi sui dati personali;
- Crescita di affidabilità e di fiducia negli stakeolders, con conseguente creazione di valore economico;
- Maggiore consapevolezza del concetto di privacy e protezione dei dati sia nell'organizzazione che negli utenti;

NEOSTUDIO
BUSINESS DATA PROTECTION

Applicabilità del Diritto nazionale

NEOSTUDIO
BUSINESS DATA PROTECTION

GDPR - Consid. (10) [...Il presente regolamento prevede anche un margine di manovra degli Stati membri [...] con riguardo al trattamento di categorie particolari di dati personali. In tal senso,[...] il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.]

PARTE TERZA

PROVVEDIMENTI A CARATTERE GENERALE E LINEE GUIDA DEL GARANTE

- Linee guida sul dossier sanitario elettronico
- Linee guida in materia di posta elettronica e internet
- Dismissione o trasferimento di apparecchiature elettroniche
- Videosorveglianza
- Informativa e Consenso per l’uso dei cookie nei sito/blog
- Sistemi di localizzazione dei veicoli nell'ambito lavorativo
- Linee guida in materia di trasparenza on line della PA

NEOSTUDIO
BUSINESS DATA PROTECTION

Linee guida sul dossier sanitario elettronico

Provv. n. 331 del 4 giugno 2015

NEOSTUDIO
BUSINESS DATA PROTECTION

TUTELA DEI PAZIENTI

- Possibilità di scegliere, in piena libertà, se far costituire o meno il dossier sanitario
- Stessa possibilità di accedere alle cure mediche richieste anche in mancanza del DSE
- E' necessario un consenso specifico per inserire nel DSE informazioni particolarmente delicate (Hiv, Interruzione volontaria della gravidanza, Atti di violenza sessuale o pedofilia)
- Il paziente dovrà essere informato in modo chiaro e semplice sulle modalità di costituzione del DSE, indicando in particolare, chi avrà accesso ai suoi dati e che tipo di operazioni potrà compiere.

PRESCRIZIONI PER LE STRUTTURE SANITARIE

- L'accesso al dossier sarà consentito solo al personale sanitario coinvolto nella cura.
- Garantire la possibilità al paziente di conoscere il reparto, la data e l'orario in cui è avvenuta la consultazione del suo dossier. Anche la semplice consultazione, dovrà essere tracciata e registrata in appositi log, conservati per almeno 24 mesi.
- Garantire la possibilità al paziente di "oscurare" alcuni dati o documenti sanitari.
- Adottare **elevate** misure di sicurezza. I dati sulla salute dovranno essere **separati** dagli altri dati personali, e crittografati.
- Obbligo di comunicare al Garante eventuali violazioni di dati o incidenti informatici (DATA BREACH) entro 48 ore dalla conoscenza del fatto.

LE LINEE GUIDA PER POSTA ELETTRONICA E INTERNET

NEOSTUDIO
BUSINESS DATA PROTECTION

Il provvedimento raccomanda ai Titolari:

- L'adozione di un disciplinare interno che descriva gli usi consentiti di internet e della posta elettronica, definito coinvolgendo anche le rappresentanze sindacali.
- Informare con chiarezza e con massima pubblicità, i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica.
- Informare sulla possibilità che vengano effettuati controlli ed analisi per fini di sicurezza dei sistemi informativi garantendo principi di pertinenza e non eccedenza.

PROVVEDIMENTO DEL GARANTE RELATIVO ALLA DISMISSIONE DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE

Il Garante richiama sulla necessità di adottare idonei accorgimenti e misure, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

a. *reimpiegate o riciclate;*
b. *smaltite;*

seguendo le procedure indicate nel provvedimento stesso

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE ON LINE

Il Provvedimento del Garante prevede che il Titolare del trattamento (l'azienda o ente "proprietario" del sito internet) debba rendere il proprio sito internet conforme a determinati requisiti in relazione all'utilizzo di cookies propri e di terzi.

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIES

NEOSTUDIO
BUSINESS DATA PROTECTION

DIFFERENZA TRA I COOKIES

TECNICI	PROFILAZIONE
Rilasciati solitamente dal sito stesso, necessari o propedeutici all'utilizzo del sito. (sessione, navigazione e analytics se anonimi). *No consenso, No notifica*	Rilasciati dal sito stesso o da altri siti collegati, per fini di profilazione e marketing in base alle preferenze dell'utente. *Si Consenso e Si Notifica*

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE

NEOSTUDIO
BUSINESS DATA PROTECTION

OBBLIGHI DI INFORMATIVA

SEMPRE!

Privacy Policy o *Cookie Policy*

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE

NEOSTUDIO
BUSINESS DATA PROTECTION

FAQ

Se il sito web si trova all'estero?

- *'Gli obblighi si applicano a tutti i siti che installano cookie sui terminali degli utenti, a prescindere dalla presenza di una sede in Italia.*

Se lo stesso Titolare gestisce più di un sito con profilazione?

- *È sufficiente una sola notificazione per tutti i diversi siti web che vengono gestiti dallo stesso Titolare.*

DOCUMENTAZIONE PRIVACY

NEOSTUDIO
BUSINESS DATA PROTECTION

Una fotografia *corrispondente* e *aggiornata*, del sistema di trattamento dei dati personali, che contiene la valutazione d'impatto privacy e le soluzioni applicate per un trattamento a norma di legge sia di tipo organizzativo che informatico e documentale.

Una corretta documentazione è essa stessa una prova dell'adozione delle misure di sicurezza.

PER NON RISCHIARE…

NEOSTUDIO
BUSINESS DATA PROTECTION

- Identificazione delle finalità del trattamento;
- Valutazione d'impatto privacy (DPIA);
- Selezione solo di partner conformi alle norme privacy (Outsourcing);

- Adeguate misure di sicurezza dei dati, nei sistemi tecnologici e nei processi aziendali;
- Nomina del Data Protection Officer qualificato (DPO);
- Compliance ai provvedimenti delle Autorità Garanti

TEMPI DI ADEGUAMENTO AL GDPR

PUBBLICA AMMINISTRAZIONE ED IMPRESE

DOVRANNO ESSERE CONFORMI ENTRO

Diritti e Responsabilità

Art. 82 – GDPR - **Diritto al risarcimento e responsabilità**

1.Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il **risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento.

ma…

3.Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, […] **SOLO** se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

NEOSTUDIO
BUSINESS DATA PROTECTION

Quattro spicci...

NEOSTUDIO
BUSINESS DATA PROTECTION

art. 83 - GDPR

4. Fino a 10.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, **se superiore**.

5. Fino a 20.000.000 euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, **se superiore**.

NEOSTUDIO
BUSINESS DATA PROTECTION

Questions & Answers

What?

Who?

Where?

When?

Why?

How?

NEOSTUDIO
BUSINESS DATA PROTECTION

Adriano Bertolino

Data Protection Officer | Consulente della Privacy

Certificato TÜV Italia n° CDP_272

conforme ISO/IEC 17024:2012

a.bertolino@neostudio.it – mobile +39 3477167484

NEO STUDIO 2000 S.R.L.

Largo Villaura, 27 – PALERMO

Tel. 091 364924 - neostudio@neostudio.it