NEOSTUDIO
BUSINESS DATA PROTECTION

Nuovo Regolamento EU 2016/679 su Data Protection, adempimenti e misure per lo studio

Ordine dei Commercialisti e Esperti Contabili di Palermo

2 marzo 2018

Camera di Commercio, Industria e Artigianato di Palermo

CHI SIAMO?

NEOSTUDIO
BUSINESS DATA PROTECTION

Neostudio Business Data Protection è partner nelle strategie di data protection in compliance al D.lgs. 196/2003 ed al Regolamento UE 2016/679 (GDPR), di Aziende, Professionisti e Pubbliche Amministrazioni da venti anni. E' stata la prima realtà in Sicilia organizzata con la specifica finalità di fornire competenze ed esperienze sugli specifici temi della data protection.

Neostudio è una azienda di professionisti che lavorano come partner di Aziende, Professionisti e Pubbliche Amministrazioni e si avvale di un gruppo di lavoro in possesso delle indispensabili competenze di tipo giuridico-organizzativo, tecnico-informatico, di risk management, commerciali e marketing. Tra i professionisti del nostro gruppo di lavoro vi sono Privacy Officer e Consulenti Privacy certificati da TUV Italia.

www.neostudioprivacy.it
info@neostudioprivacy.it

NEOSTUDIO
BUSINESS DATA PROTECTION

AGENDA

I. PRIMA PARTE

1) *Quadro Normativo;*
2) *Definizioni del GDPR;*
3) *Novità introdotte dal Regolamento UE 2016/679;*

II. SECONDA PARTE

1) *Nuovo sistema sanzionatorio;*
2) *Nuova responsabilità = accountability;*
3) *Il registro dei trattamenti;*
4) *Implementazione nell'attività di studio professionale*

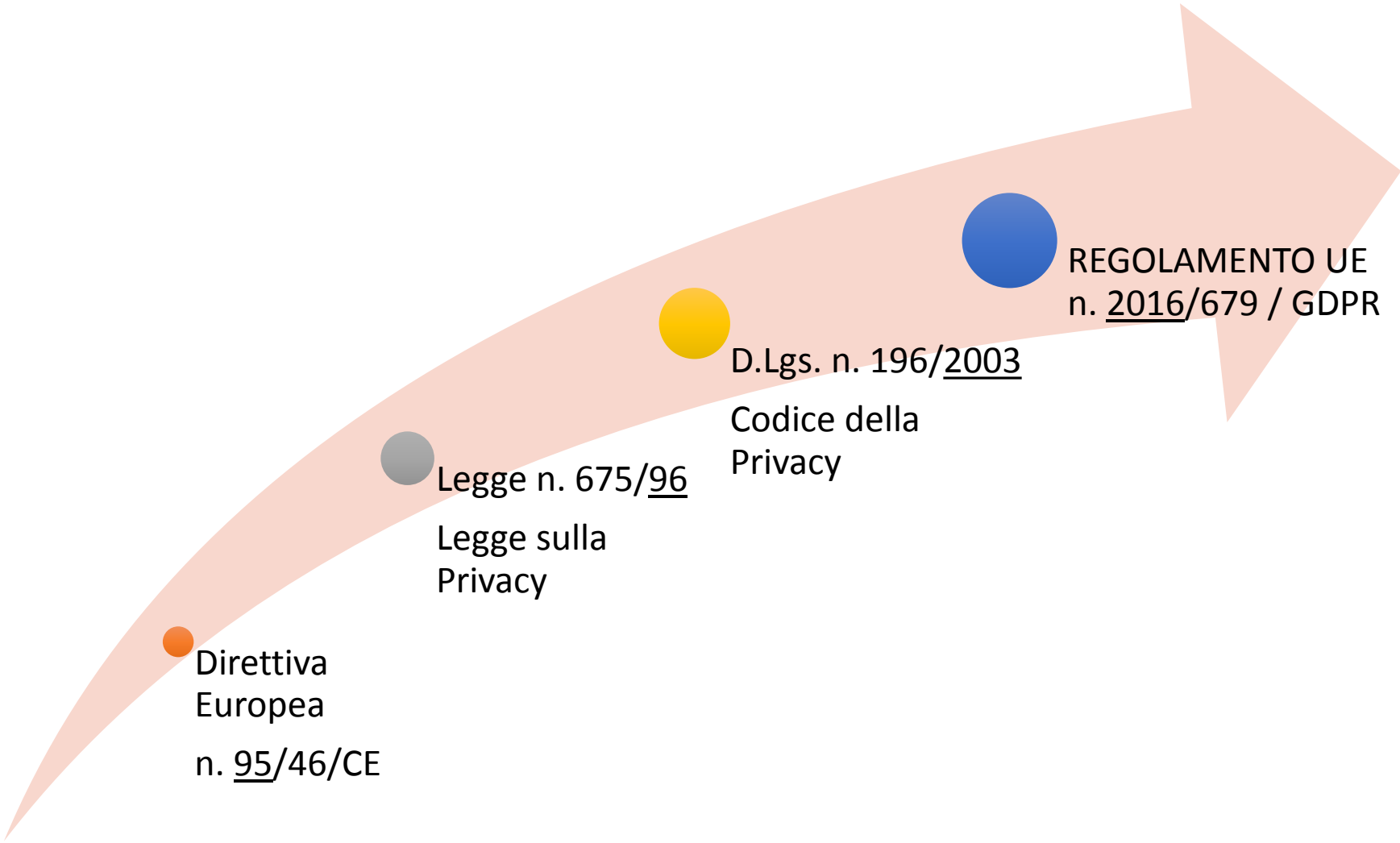
III. TERZA PARTE

1) *Nuova gestione dei rischi e valutazione d'impatto Privacy;*
2) *Sito dello studio e digitalizzazione;*
3) *Provvedimenti Generali del Garante Privacy;*
4) *Linee guida in materia di specifici trattamenti di dati personali;*

DOMANDE E RISPOSTE

EVOLUZIONE NORMATIVA

NEOSTUDIO
BUSINESS DATA PROTECTION



NEOSTUDIO
BUSINESS DATA PROTECTION

REGOLAMENTO (UE) 2016/679

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

NEOSTUDIO
BUSINESS DATA PROTECTION

Alcuni dei temi trattati dal Regolamento UE 2016/679

Data Protection Officer (DPO)	Trasferimenti Extra-UE	Social e minori	Diritto all'oblio	Data Protection Assessement (DPIA)
Privacy by Default	Privacy by Design	Profilazione online	Data Breach	Registro dei Trattamenti
Data Portability	Consenso Esplicito	Accountability	One Stop Shop	Elevazione Sanzioni Amministrative

PRINCIPALI DEFINIZIONI

Il **G**eneral **D**ata **P**rotection **R**egulation riprende alcune definizioni presenti già nel nostro Codice Privacy e ne introduce di nuove fondamentali per comprendere l'applicazione del Regolamento UE

- Dato Personale
- Trattamento
- Pseudoanonimizzazione
- Profilazione
- Consenso dell'interessato
- Titolare e Responsabile del trattamento
- Violazione dei dati personali (Data Breach)
- Trattamento transfrontaliero
- Rappresentante
- Norme vincolanti d'impresa
- Data Protection Officer
- Portabilità dei dati

DATO PERSONALE

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

- 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 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

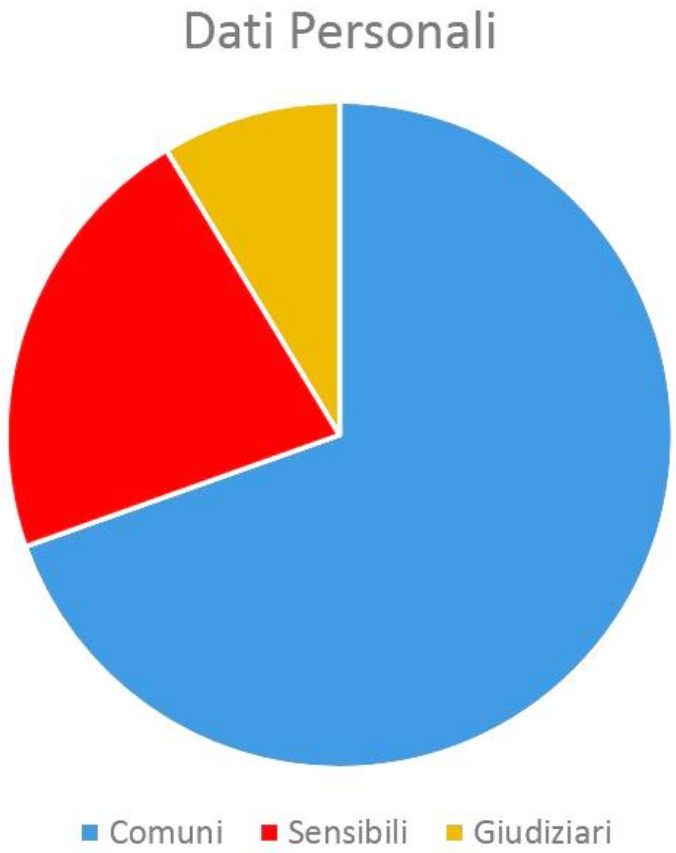
DATI GIUDIZIARI (art. 10)

- 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

NEOSTUDIO
BUSINESS DATA PROTECTION

DATO COMUNE/IDENTIFICATIVO

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



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;

RUOLI ORGANIZZATIVI PRIVACY

NEOSTUDIO
BUSINESS DATA PROTECTION

NEOSTUDIO
BUSINESS DATA PROTECTION

RESPONSABILE DEL TRATTAMENTO

La *persona fisica, giuridica, ente* che tratta dati personali per conto del titolare del trattamento

Una responsabilità derivante dal conferimento di incarichi professionali, consulenziali o di assistenza esterna, estendendo allo stesso, nei limiti dell'oggetto dell'incarico, tutti **gli obblighi e le responsabilità** di un responsabile interno

NEOSTUDIO
BUSINESS DATA PROTECTION

SUB-RESPONSABILE DEL TRATTAMENTO IN OUTSOURCING – art. 28 c. 2

NOVITÀ

Il ricorso ad un sub-responbabile del trattamento da parte di un responsabile in outsourcing nominato per lo svolgimento di un determinato trattamento può essere effettuato **soltanto** in presenza di **AUTORIZZAZIONE SCRITTA** o su nomina diretta del Titolare.

FORNITORE TECNOLOGICO IN OUTSOURCING

Stessa situazione nei casi di eventuali rapporti con il fornitore o manutentore del software o del sistema informativo specie ove lo stesso fornisca un servizio di aggiornamento o assistenza mediante un collegamento telematico.

Naturalmente è necessario tenere conto delle nuove norme sulla figura dell'Amministratore di sistema

NEOSTUDIO
BUSINESS DATA PROTECTION

AMMINISTRATORE DI SISTEMA

È quella figura tecnica professionale dedicata alla gestione e alla manutenzione dei sistemi informatici e tecnologici con cui vengono effettuati trattamenti di dati personali.

Provv. generale del 27/11/2008

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

…LE PERSONE AUTORIZZATE…
(L'INCARICATO DEL TRATTAMENTO)

"…le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile…"

Le persone *fisiche* autorizzate dal titolare o dal responsabile a compiere **soltanto** operazioni di trattamento per le quali sono state designate.

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

DPO: DATA PROTECTION OFFICER

Quali caratteristiche?

NEOSTUDIO
BUSINESS DATA PROTECTION

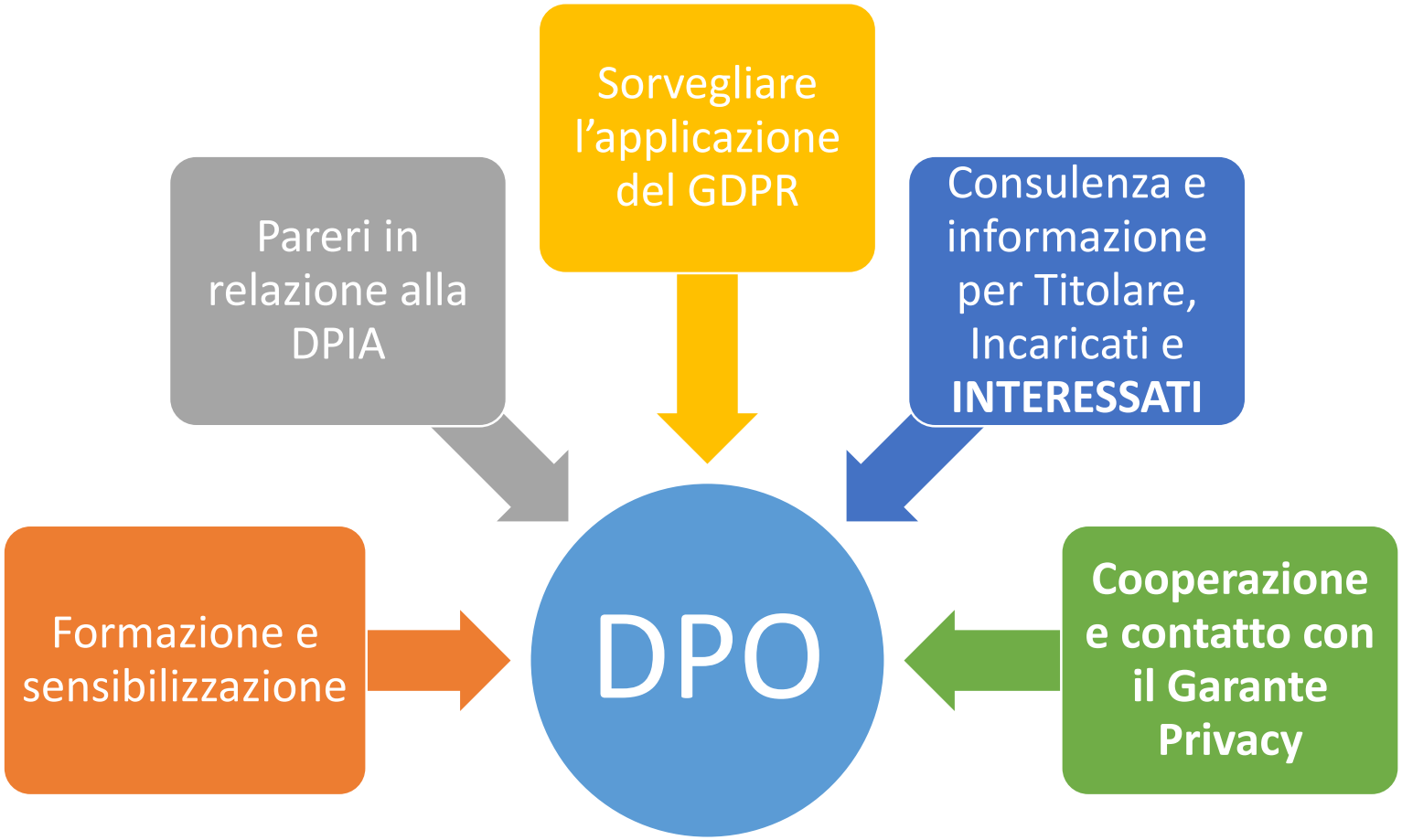
Art. 37 - GDPR

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

NEOSTUDIO
BUSINESS DATA PROTECTION

DPO: DATA PROTECTION OFFICER

Quali compiti?



I CONTROLLI

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

a) Su iniziativa dei soggetti precedentemente identificati (livello basso);

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

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

L'Autorità Garante ha il compito di:

- Verificare l'applicazione del Codice e 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;

NEOSTUDIO
BUSINESS DATA PROTECTION

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 che verifica

l'organizzazione e l'adeguamento

alla norme vigenti sulla data protection.

PARTE SECONDA

- Nuovo sistema sanzionatorio;
- Nuova responsabilità = accountability;
- Il registro dei trattamenti;
- Implementazione nell'attività di studio professionale

Quattro spicci...

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**.

I SOGGETTI RESPONSABILI

Il TITOLARE ed il RESPONSABILE sono sempre gli UNICI responsabili in solido a livello civile e penale.

In caso di dolo o colpa grave dell'INCARICATO *(persona autorizzata al trattamento)* può essere esercitato il diritto di rivalsa su quest'ultimo.

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

Principio di Accountability (art. 24)

''Tenuto conto della natura, […] e delle finalità del trattamento, nonché dei rischi […] 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 presente regolamento…''*

Principio di Accountability (art. 24)

Come dimostrare la conformità?

NEOSTUDIO
BUSINESS DATA PROTECTION

1. Adozione di misure di sicurezza e l'attuazione di politiche per garantire la tutela dei diritti e delle libertà delle persone fisiche;
2. Adesione ai codici di condotta elaborati in funzione di specifici settori o esigenze delle PMI (art. 40);
3. Meccanismo di certificazione della protezione dei dati personali (art. 42);

NB: L'adesione a codici di condotta o certificazione non riduce la responsabilità in caso di illeciti trattamenti o non conformità al GDPR

NEOSTUDIO
BUSINESS DATA PROTECTION

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***…’’

Registro dei Trattamenti (art. 30)

NEOSTUDIO
BUSINESS DATA PROTECTION

‘‘Ogni titolare del trattamento e il responsabile, ove nominato, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità…’’

Sostituisce la notificazione ex art. 37 e il c.d. prior checking (o verifica preliminare) ex art. 17 D.lgs. 196/03

Registro dei Trattamenti (art. 30)

Chi è obbligato?

NEOSTUDIO
BUSINESS DATA PROTECTION

Titolari del trattamento con più di 250 dipendenti;

Quei trattamenti con:

a) con un rischio per i diritti e le libertà dell'interessato;
b) Non siano occasionali;
c) Trattamenti che comprendono i dati di cui all'art. 9 *(dati sensibili)* o art. 10 *(dati giudiziari)*;

Registro dei Trattamenti (art. 30)

Cosa contiene?

NEOSTUDIO
BUSINESS DATA PROTECTION

a) Dati identificativi e di contatto del Titolare/i o Responsabile;

b) Tipologia dei dati personali trattati e categorie degli interessati;

c) Finalità dei trattamenti;

d) Tempi di conservazione, per tipologia di dati ;

e) Identificazione di eventuali Destinatari, anche transfrontalieri dei dati personali;

f) Descrizione delle misure di sicurezza tecniche e organizzative adottate ex art. 32;

INFORMATIVA E CONSENSO

Chi effettua il trattamento **deve** fornire l'Informativa (sempre obbligatoria) in modo chiaro e trasparente, anche in forma orale 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 <u>deve</u> contenere anche (art. 13):

- Eventuali intenzioni di trasferimento di dati personali a Paesi UE o Extra-UE;
- Modalità di esercizio dei diritti dell'interessato:
  - ✓ Accesso;
  - ✓ Rettifica;
  - ✓ Cancellazione *(diritto all'oblio)*;
  - ✓ Limitazione del trattamento;
  - ✓ Portabilità dei dati;
  - ✓ Opposizione;
  - ✓ Divieto di profilazione automatizzata;

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;

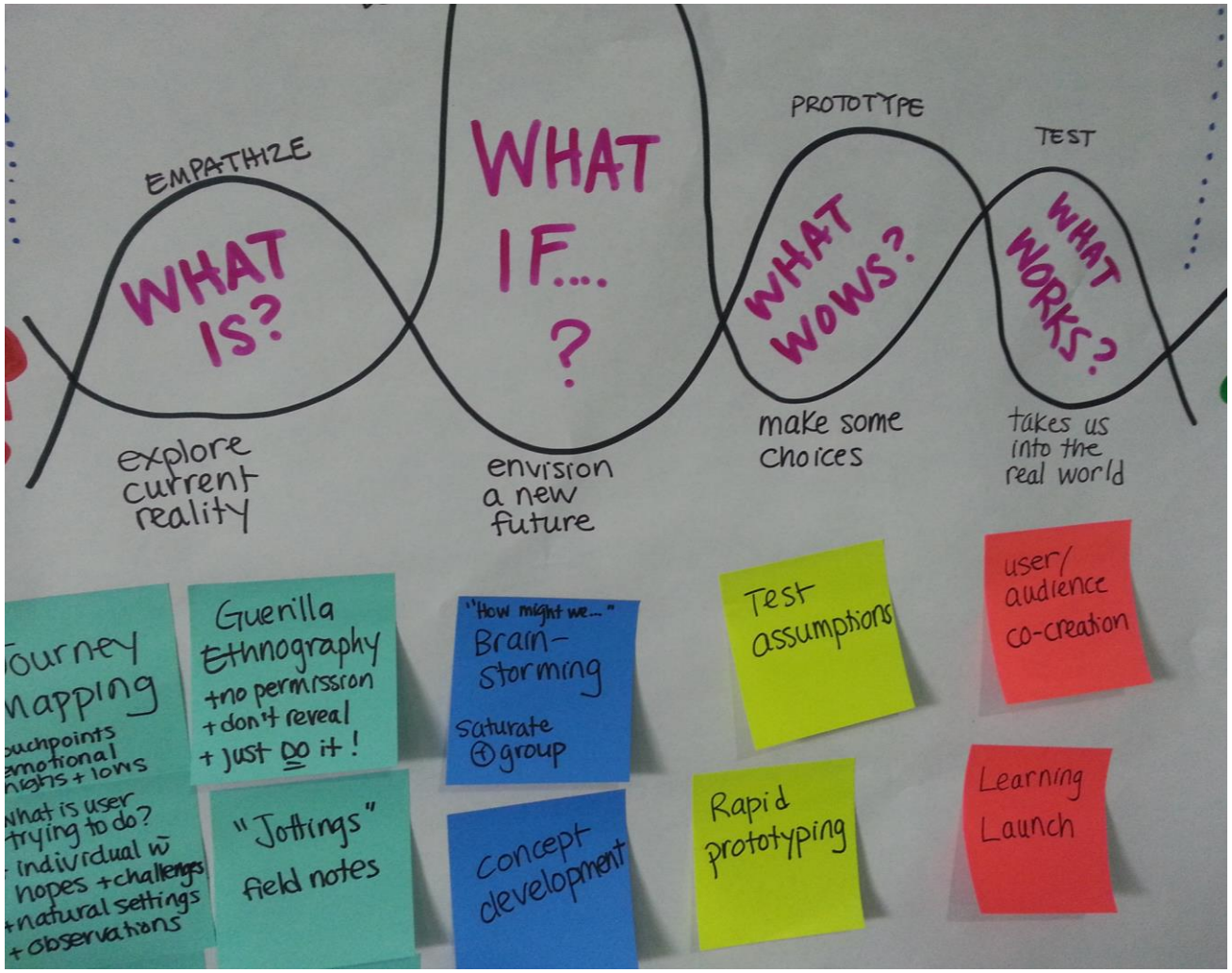
DIMOSTRABILE!!!

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**.’’

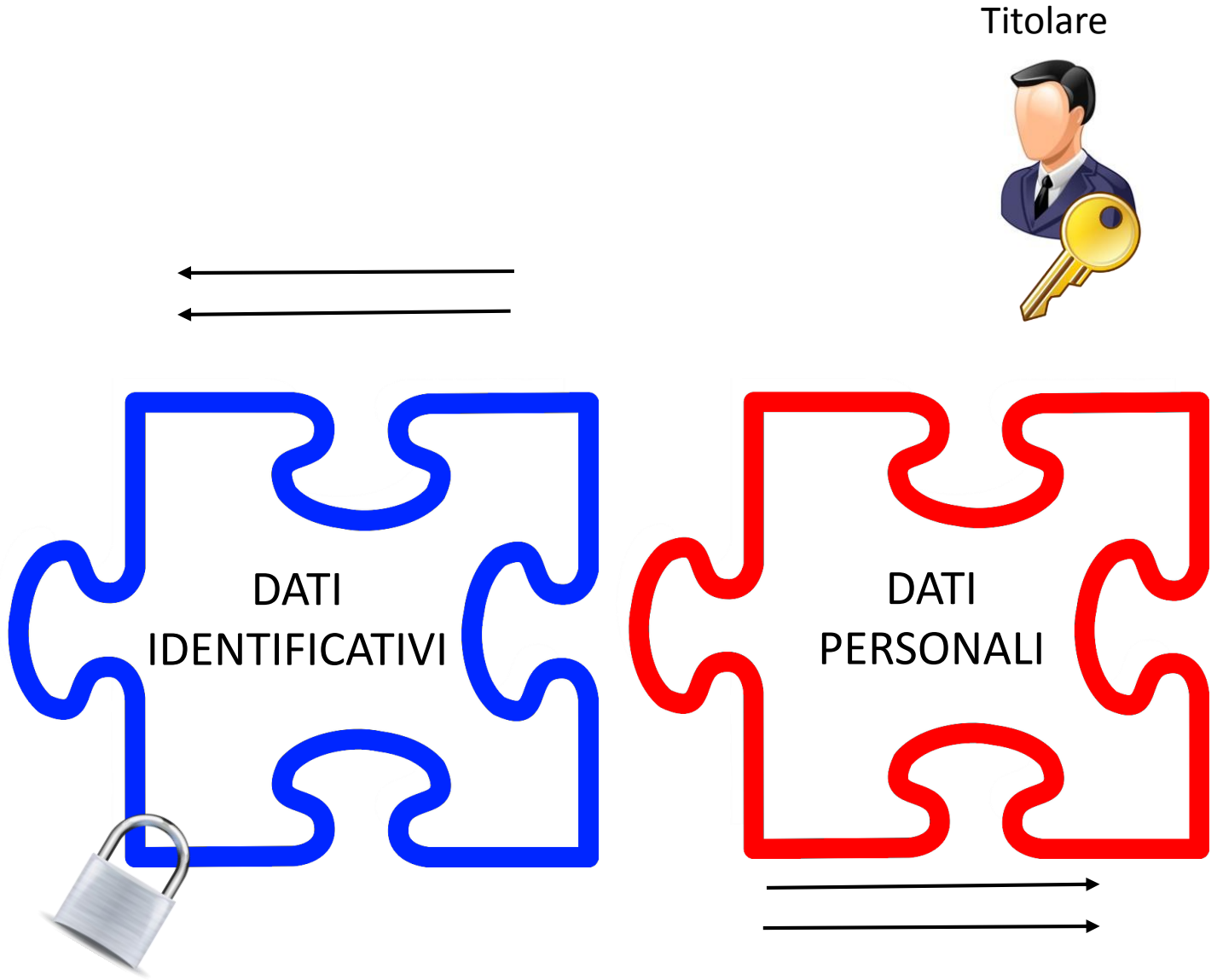
NEOSTUDIO
BUSINESS DATA PROTECTION

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.



NEOSTUDIO
BUSINESS DATA PROTECTION

Privacy by Design

Minimizzazione dei dati

Limitazione nel trattamento dei dati:

- Adeguati;
- Pertinenti;
- Limitati;
- Conservazione

Solo

i dati necessari rispetto alle finalità perseguite

NEOSTUDIO
BUSINESS DATA PROTECTION

Privacy by Default

Art. 25.2 - – General Data Protection Regulation

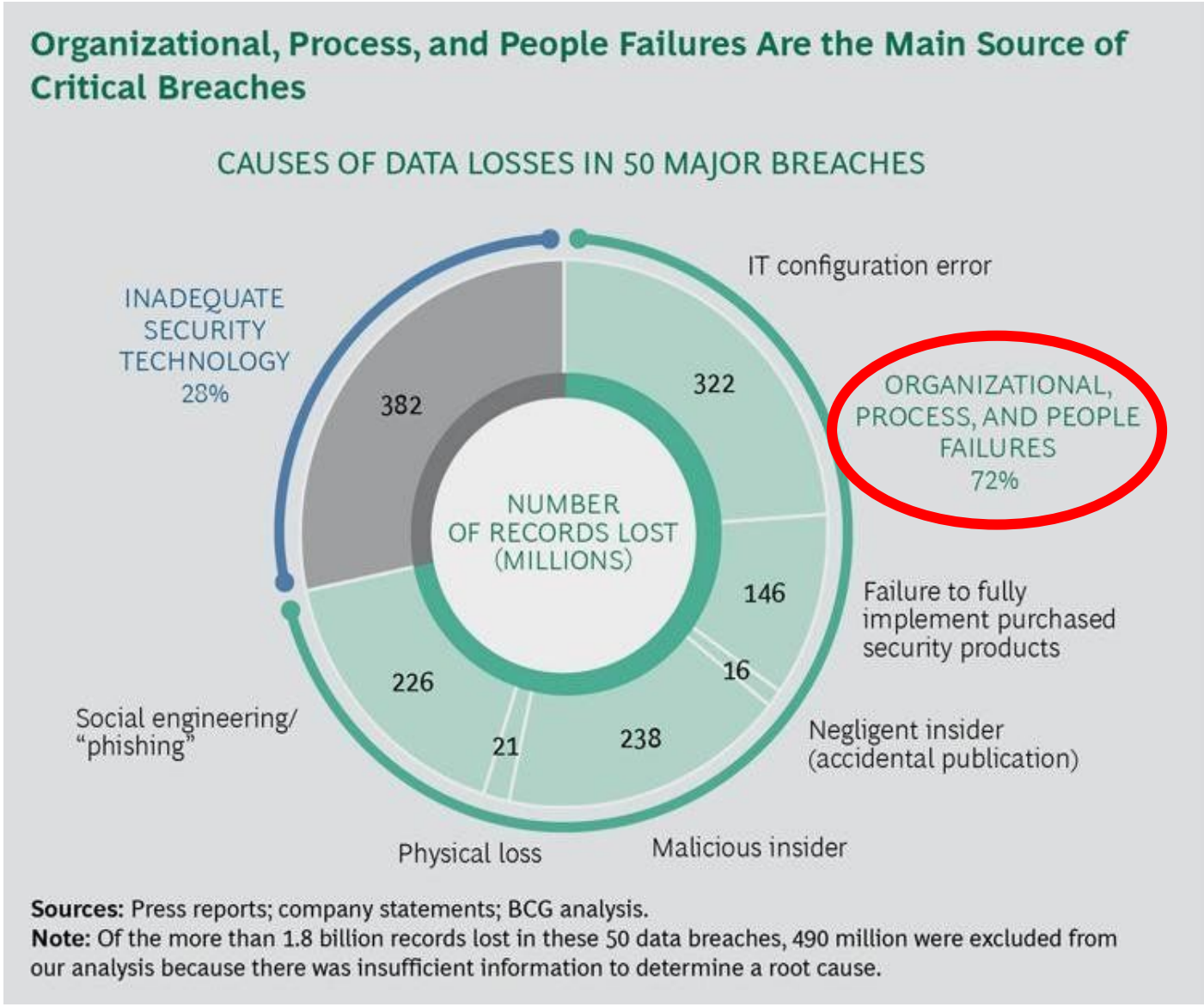
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, **solo i dati personali necessari** per ogni **specifica finalità** del trattamento. Tale obbligo vale per la **quantità** dei dati personali raccolti,[…]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

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**»)



Notifica del Data Breach (art. 33)

NEOSTUDIO
BUSINESS DATA PROTECTION

In caso di data breach (violazione dei dati personali) il Titolare dovrà comunicare **entro 72 ore** al Garante l'evento e se tale violazione comporti **elevati rischi** per i diritti e le libertà degli interessati andrà comunicato tempestivamente anche agli stessi.

Notifica del Data Breach (art. 33)

Come notificare?

NEOSTUDIO
BUSINESS DATA PROTECTION

1. Descrizione della violazione e indicazione dell'estensione e categoria dei dati violati:
2. Descrizione possibili rischi derivanti dal data breach:
3. Misure adottate per ripristinare la sicurezza dei dati;

PARTE TERZA

- Nuova gestione dei rischi e valutazione d’impatto Privacy;
- Sito dello studio e digitalizzazione;
- Provvedimenti Generali del Garante Privacy e Linee guida in materia di specifici trattamenti di dati personali

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)

NEOSTUDIO
BUSINESS DATA PROTECTION

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;

DPIA: Data Protection Impact Assessment (art. 35)

NEOSTUDIO
BUSINESS DATA PROTECTION

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)*

Applicabilità del Diritto nazionale

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.]

PROVVEDIMENTI A CARATTERE GENERALE E LINEE GUIDA DEL GARANTE

NEOSTUDIO
BUSINESS DATA PROTECTION

- Informativa e Consenso per l'uso dei cookie nei sito/blog
- Linee guida in materia di posta elettronica e internet
- Dismissione o trasferimento di apparecchiature elettroniche
- Videosorveglianza

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE - 1

Il Provvedimento del Garante nel rispetto della Direttiva 2009/136/CE 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 COOKIE - 2

COSA SONO I COOKIES?

I cookie sono brevi frammenti di codice/testo (lettere e/o numeri) memorizzati sul vostro browser sullo specifico dispositivo da voi utilizzato (*computer, tablet, smartphone*) inviati dal Sito visitato **e successivamente ritrasmessi allo stesso** che contengono informazioni da utilizzare nel corso della medesima visita o in seguito, anche a distanza di giorni. I cookie vengono memorizzati, in base alle preferenze dell'utente.

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE - 3

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 - 4

NEOSTUDIO
BUSINESS DATA PROTECTION

OBBLIGHI DI INFORMATIVA

SEMPRE!

Privacy Policy o *Cookie Policy*

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE - 5

NEOSTUDIO
BUSINESS DATA PROTECTION

MODALITA' DI INFORMATIVA con BANNER

Analytics Terze parti	• Nella raccolta **NON** sono adottati strumenti che riducono il potere identificativo. (mascheramento IP)
Profilazione propria	• Sono raccolti per analizzare le preferenze e le scelte di consumo, per inviare messaggi pubblicitari mirati.
Profilazione terze parti	• Sono raccolti da TERZI per analizzare le preferenze e le scelte di consumo e per inviare messaggi pubblicitari mirati.

PROVVEDIMENTO DEL GARANTE IN MATERIA DI COOKIE - 7

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.*

INTERNET E FLUSSI INFORMATIVI

LE LINEE GUIDA PER POSTA ELETTRONICA E INTERNET - 1

Il Garante privacy, con un provvedimento generale fornisce concrete indicazioni in ordine all'uso dei computer sul luogo di lavoro.

Perché ad esempio dall'analisi dei siti web visitati si possono trarre informazioni anche sensibili sui dipendenti e i messaggi di posta elettronica possono avere contenuti a carattere privato.

Il datore di lavoro è inoltre chiamato ad adottare *ogni misura in grado di prevenire* il rischio di utilizzi impropri e la lesione della riservatezza dei lavoratori.

INTERNET E FLUSSI INFORMATIVI

LE LINEE GUIDA PER POSTA ELETTRONICA E INTERNET - 2

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.

INTERNET E FLUSSI INFORMATIVI

LE LINEE GUIDA PER POSTA ELETTRONICA E INTERNET - 4

POSTA ELETTRONICA :

- L’utilizzo di indirizzi di posta elettronica condivisi tra più lavoratori, oltre a quelli individuali;
- l'inserzione nei messaggi di un disclaimer che informi i destinatari sulla la natura non personale del messaggio e che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;

PROVVEDIMENTI DEL GARANTE RELATIVI ALLA GESTIONE INFORMATICA

DISMISSIONE DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE - 1

NEOSTUDIO
BUSINESS DATA PROTECTION

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

PROVVEDIMENTI DEL GARANTE RELATIVI ALLA GESTIONE INFORMATICA

DISMISSIONE DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE - 2

a. Per il reimpiego e/o il riciclaggio di apparecchiature elettriche ed elettroniche devono essere seguite le procedure che consentano l'effettiva cancellazione dei dati o garantire la loro non intelligibilità.

   Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti.

PROVVEDIMENTI DEL GARANTE RELATIVI ALLA GESTIONE INFORMATICA

DISMISSIONE DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE - 3

b. Per lo smaltimento di apparecchiature elettriche ed elettroniche devono essere seguite le procedure che consentono l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature ciò può anche comportare la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l’acquisizione indebita di dati personali.

VIDEOSORVEGLIANZA

L'utilizzo di sistemi di videosorveglianza è consentito soltanto in garanzia delle libertà fondamentali ed un elevato livello di tutela dei diritti dell'interessato e rispettando le seguenti regole:

1) Principio di liceità;
2) Principio di necessità;
3) Principio di proporzionalità;
4) Principio di finalità;
5) Indispensabile accordo sindacale o accettazione di conforme istanza presentata ad ufficio provinciale del lavoro.

VIDEOSORVEGLIANZA - 3

NEOSTUDIO
BUSINESS DATA PROTECTION

CONSERVAZIONE:

La conservazione delle immagini deve essere commisurata al *tempo necessario* al raggiungimento delle finalità perseguite.

Pertanto, fatte salve speciali esigenze, possono essere registrate le ultime **24, 48 o 72 ore** in base ad orari apertura o in caso di attività particolarmente rischiose o per esigenze di ulteriore conservazione è necessario sottoporre il progetto di videosorveglianza a verifica preliminare del Garante.

PERTANTO…

- Adeguarsi vuol dire attuare una reale procedura di trattamento dei dati personali conforme alla legge, non soltanto produrre carta!
- Adeguarsi comporta un attento lavoro di analisi personalizzata.
- Rivolgersi a chi ha esperienza specifica nel settore tutela della riservatezza permette di ottenere un reale adeguamento in tempi rapidi con la certezza di una piena conformità alla normativa che è sempre in evoluzione.

…PER NON RISCHIARE

NEOSTUDIO
BUSINESS DATA PROTECTION

- Identificazione dei principi di liceità e delle finalità del trattamento;
- Analisi dei rischi in base alla probabilità e gravità;
- Selezione solo di partner conformi alle norme privacy (Outsourcing);

- Adeguate misure di sicurezza dei dati, nei sistemi tecnologici e nei processi aziendali;
- Nomina delle figure interne/eserne autorizzate al trattamento;
- Compliance ai provvedimenti delle Autorità Garanti

TEMPI DI ADEGUAMENTO AL GDPR

NEOSTUDIO
BUSINESS DATA PROTECTION

OGNI TITOLARE DEL TRATTAMENTO

DOVRA' ESSERE CONFORME ENTRO

NEOSTUDIO
BUSINESS DATA PROTECTION

Questions & Answers

What?

Who?

Where?

When?

Why?

How?

NEOSTUDIO
BUSINESS DATA PROTECTION

NEO STUDIO 2000 S.R.L.
Largo Villaura, 27 – PALERMO
Tel. 091 364924 - neostudio@neostudio.it