

---

# **REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI: NOZIONI DI BASE AOSTA, 04 MARZO 2020**

AVV. VALERIA FADDA - INTRODUZIONE E SALUTI AIGA SEZIONE DI AOSTA

## **RELATORI:**

DPO APS S.P.A. E ORDINE AVVOCATI DI AOSTA - CRISTIANO PIVATO

DPO IRV S.R.L. - RONCARI LUCA

PARTNER REGIP E CONSULENTE PRIVACY D&L NET – FEDERICO CAPELLO





# AGENDA

- Introduzione e saluti Sezione Aiga di Aosta
- Cenni storici, quadro normativo attuale e futuro
- Terminologia e principi
- Regolamento UE sulla protezione dei dati: conferme, modifiche, novità
- Organigramma privacy e Data Protection Officer (DPO)
- La digitalizzazione della società e della professione
- Le criticità degli studi professionali: l'organizzazione fisica e digitale dello studio
- Domande e riflessioni finali
- Verifica la tua compliance

# AGENDA EVENTO DEL 23 APRILE 2020

- Introduzione e saluti Sezione Aiga di Aosta
- Il Regolamento UE
  - Disposizioni generali
  - I principi
  - L'informativa, il consenso e le altre condizioni di liceità
  - L'organigramma privacy
  - I registri obbligatori
  - Data breach
  - Valutazione del rischio e DPIA
  - Le sanzioni
- La digital disruption
- Organizzazione pratica dello studio professionale per i trattamenti digitali e non
- Esempi operativi
- Test per il rilascio del certificato ex art. 29 e 32 del GDPR



# REGOLAMENTO UE N. 679 DEL 27 APRILE 2016

DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO  
DEI DATI PERSONALI, NONCHE' DELLA LIBERA CIRCOLAZIONE DI TALI DATI

PUBBLICATO IN GAZZETTA UFFICIALE EUROPEA IL 4 MAGGIO 2016, ENTRATO IN VIGORE IL  
24 MAGGIO 2016 E DEFINITIVAMENTE APPLICABILE IN VIA DIRETTA IN TUTTI I PAESI UE DAL  
25 MAGGIO 2018

GDPR (GENERAL DATA PROTECTION REGULATION)

RGPD (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI)

# VIDEO GARANTE PRIVACY VISUALIZZABILE AL SEGUENTE LINK

<https://youtu.be/irsR4tb-eiw>





# **CENNI STORICI**



## CENNI STORICI 1/3

- Il diritto alla protezione dei dati personali si è sviluppato a partire dal diritto al rispetto della vita privata, tale diritto si riferisce agli essere umani (persone fisiche)
- Stati Uniti XIX secolo: articoli di stampa che espongono il concetto di privacy
- Corte suprema degli Stati Uniti (metà anni '50): prima giurisprudenza in tema di privacy

## CENNI STORICI 2/3

- Art. 12 del Dichiarazione universale dei diritti dell'uomo delle Nazioni Unite del 10/12/48: *“nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni”*



## CENNI STORICI 3/3

- Cambiamenti degli ultimi 40 anni che hanno comportato una sempre maggiore attenzione alla tutela del trattamento dei dati:
  - tecnologia: una sempre maggiore velocità e facilità di trasferire elevate quantità di dati a soggetti ovunque stabiliti
  - modalità di reperimento dei dati: spesso sono forniti in modo inconsapevole dagli stessi interessati
  - finalità del trattamento: attività quali la profilazione o altri strumenti di elaborazione automatizzata in grado di influenzare o interferire nella vita quotidiana di un individuo



# **QUADRO NORMATIVO**

## EVOLUZIONE QUADRO NORMATIVO 1/2

- Convenzione n. 108 del Consiglio d'Europa del 1981 sulla protezione dei dati di carattere personale, è il primo strumento internazionale vincolante per gli stati ratificata in Italia nel 1989 con la Legge n. 98
- Direttiva 95/46/CE del Parlamento Europeo e del Consiglio (c.d. Direttiva madre o Data Protection Directive) «Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati», recepita in Italia con la Legge n. 675 del 31/12/96 in vigore da maggio 1997. Con la successiva Legge 676/1996 il Governo è intervenuto in senso correttivo per garantire la piena aderenza della norma alle mutate esigenze di protezione



## EVOLUZIONE QUADRO NORMATIVO 2/2

- D.Lgs. 196 del 30 giugno 2003 «*Codice in materia di protezione dei dati personali*» con allegati codici di deontologia e di buona condotta
  - Nuove disposizioni connesse al quadro comunitario internazionale e della Direttiva 2002/58/CE
  - Completa e perfezione il recepimento della Direttiva 95/45/CE



## QUADRO NORMATIVO ATTUALE: REGOLAMENTO UE 679/2016

- Regolamento UE n. 679/2016:
  - 173 considerando e 99 articoli
  - Direttamente applicabile negli Stati membri a partire dal 25 maggio 2018
  - 2 anni di tempo dalla sua pubblicazione in G.U. per permettere ai legislatori nazionali o alle competenti autorità (Garante) di intervenire per agevolare l'adozione del GDPR o per disciplinare aspetti particolari che lo stesso regolamento prevede



## QUADRO NORMATIVO ATTUALE: D.LGS. 101/18

- D.Lgs. 101 del 10/08/18 «disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 679/2016»:
  - Provvedimento di armonizzazione del D.Lgs. 196/2003 al GDPR
  - In vigore dal 19 settembre 2018

## QUADRO NORMATIVO ATTUALE: ALTRE FONTI 1/3

- Il considerando 41 del Reg. UE prevede che *“qualora il presente Regolamento faccia riferimento a una base giuridica o a una natura legislativa, ciò non richiede necessariamente l’adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell’ordinamento costituzione dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte...”*

## QUADRO NORMATIVO ATTUALE: ALTRE FONTI 2/3

- Provvedimenti e autorizzazioni del Garante. Il considerando 41 quindi prevede che la base giuridica può essere rappresentata anche da un atto diverso da un atto legislativo, quindi anche da Provvedimenti del Garante nazionale
- Il D.Lgs. 101/18 prevede il censimento dei provvedimenti del Garante in vigore all'entrata del GDPR al fine di stabilire se gli stessi possano costituire o meno idonea base giuridica alla luce delle nuove disposizioni del GDPR



## QUADRO NORMATIVO ATTUALE: ALTRE FONTI 3/3

- **Regole deontologiche** (art. 2 quater del Codice Privacy): assegna al Garante la competenza dell'adozione di regole deontologiche individuando i soggetti pubblici e privati appartenenti alle categorie interessate che ritengano di avere titolo a sottoscrivere le regole deontologiche
- **Codici di condotta** (art. 40 e 41 Reg. UE). Secondo il considerando 77 i codici di condotta servono a fornire orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione della migliore prassi per attenuare il rischio

## EVOLUZIONE FUTURA

La continua evoluzione degli strumenti di trattamento e delle finalità fanno presumere la pubblicazione di nuovi provvedimenti in ambito di trattamento dati:

- Art. 97 e 98 GDPR: entro 25 maggio 2020 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio relazioni di valutazione e sul riesame dell'attuale Regolamento. Se del caso, la Commissione presenta proposte legislative di modifica di altri atti legislativi dell'Unione in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento
- Art. 95 GDPR: rapporti con la direttiva e-privacy e Regolamento e-privacy
- Regolamento sul trattamento dei dati delle persone giuridiche
- A livello nazionale: provvedimenti del Garante



# **TERMINOLOGIA E PRINCIPI**

## COSA SI INTENDE PER DATO PERSONALE? (ART. 4)

- per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)
- si considera «identificabile» la persona fisica che può essere riscontrata, direttamente o indirettamente, attraverso un dato «univoco» («identificativo») come il nome, un numero di identificazione, i dati relativi alla sua ubicazione, un identificativo online oppure uno o più elementi caratterizzanti della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

## INTERESSATO

- la persona fisica a cui si riferiscono i dati personali (es. clienti, fornitori, dipendenti, collaboratori, candidati, visitatori web, ecc.)



**«PROPRIETARIO» DEI DATI PERSONALI  
DEVE POTER DISPORRE IN QUALSIASI MOMENTO**



## **ACCOUNTABILITY (ART. 5.2)**

- il titolare del trattamento deve garantire il rispetto della normativa sul trattamento dei dati e mettere in atto misure tecniche ed organizzative adeguate, idonee a garantire e dimostrare che le operazioni di trattamento avvengono secondo le disposizioni del GDPR
- il principio è strettamente connesso all'approccio basato sul rischio con la responsabilizzazione del titolare e del responsabile del trattamento circa l'adozione di comportamenti proattivi e la possibilità di dimostrare quanto è stato posto in essere per l'applicazione del Regolamento

## PRIVACY BY DESIGN E PRIVACY BY DEFAULT (ART. 25)

- La protezione dei dati personali deve rappresentare un importante obiettivo per tutte le organizzazioni piuttosto che un mero requisito di legge
- La privacy by design prevede che il Titolare del trattamento adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati
- La privacy by default prevede, invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari (minimizzazione e pertinenza) per ciascuna specifica finalità di trattamento
- Per ogni trattamento deve pertanto essere garantita la protezione dei dati fin dalla progettazione del trattamento e per impostazione predefinita, con la valutazione dei rischi e l'identificazione delle relative misure di sicurezza adeguate

## MISURE DI SICUREZZA ADEGUATE (ART. 32) 1/2

- Il Codice privacy, allegato B, elencava le misure di sicurezza MINIME da adottare (lunghezza password e tempi di revisione delle stesse, archivi con chiavi, ecc.)
- Il GDPR non prevede misure minime ma ADEGUATE in funzione dei trattamenti svolti, devono essere predisposte dal Titolare
- Il GDPR prescrive che i dati personali devono essere "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 («integrità e riservatezza»)



## MISURE DI SICUREZZA ADEGUATE (ART. 32) 2/2

- le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:
- misura tecnica
  - a) la pseudonimizzazione e la cifratura dei dati personali
- requisiti di sicurezza
  - b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
  - c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
  - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

## **CATEGORIE PARTICOLARI DI DATI PERSONALI (EX DATI SENSIBILI) (ARTT. 9 E 10)**

- dati che possono rilevare l'origine razziale/etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati sullo stato di salute, alla vita o orientamento sessuale
- dati relativi alla salute: 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

## **DATI GENETICI, BIOMETRICI E GIUDIZIARI (ARTT. 9 E 10)**

- dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite da 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: 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 (impronte digitali, foto digitali, scansione dell'iride)
- dati giudiziari: provvedimenti iscritti nel casellario giudiziale, nell'anagrafe delle sanzioni amministrative, dipendenti da reato e dei relativi carichi pendenti, la qualità di imputato o di indagato



## **TIPOLOGIE DI TRATTAMENTO (CARTACEO, INFORMATICO O MISTO)**

- qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, la messa a disposizione, il raffronto, l'interconnessione, la limitazione, la cancellazione e la distruzione dei dati

## PROFILAZIONE (ART 4.4)

- il termine profilazione indica l'insieme delle attività di raccolta e analisi di informazioni e comportamenti relativi alle persone, con il fine di elaborarle per “ripartire” gli individui in gruppi omogenei sulla base di caratteristiche selezionate e variabili in funzione dello scopo prefissato
- il GDPR definisce profilazione qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica. In particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica



## **DATA BREACH – ART. 33 E 34 DEL GDPR**

- tutte le violazioni dei dati personali (accidentali o dolose) vanno documentate e riferite tempestivamente al titolare del trattamento
- in caso di data breach il titolare deve attivare una procedura interna volta a valutarne la gravità e l'impatto
- il titolare deve valutare se procedere alla notifica al Garante e/o agli interessati o entrambi

## LICEITÀ DEL TRATTAMENTO – (ART. 6)

- i dati personali possono essere trattati solo tramite **consenso** o altre condizione di liceità:
  - adempimento di un obbligo contrattuale
  - obbligo di legge
  - interesse legittimo prevalente del titolare
  - interesse vitale
  - interesse pubblico o esercizio di pubblici poteri

## INFORMATIVA SUL TRATTAMENTO ALL'INTERESSATO

- è la comunicazione con la quale il titolare informa l'interessato del trattamento svolto e può essere fornita oralmente o per iscritto. Il titolare pertanto illustra ai soggetti ai quali i dati raccolti si riferiscono (interessati). E' sempre necessario fornire l'informativa prima di procedere al trattamento
- consente all'interessato di conoscere le intenzioni del titolare, di valutare le conseguenze del trattamento, di poter accettare o rifiutare il trattamento, di controllare i suoi dati
- deve essere chiara e concisa ma non generica
- il contenuto è disciplinato dagli artt. 13 e 14 del GDPR e deve essere revisionata periodicamente





# **REGOLAMENTO UE SULLA PROTEZIONE DEI DATI CONFERME, MODIFICHE E NOVITÀ**



## LE PRINCIPALI CONFERME

- Principi applicabili al trattamento di dati personali (art. 5 e seg.):
  - Trasparenza
  - Liceità
  - Correttezza
  - Minimizzazione, pertinenza e proporzionalità
  - Limitazione della conservazione
  - Sicurezza e integrità dei dati



# TRASPARENZA

- rafforzata con l'applicazione del Regolamento UE 679/2016
- le informazioni che il titolare deve fornire all'interessato sulle modalità del trattamento deve essere resa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro



## LICEITÀ E CORRETTEZZA

- senza il consenso o altra condizione di liceità il trattamento è illecito e quindi sanzionabile
- I dati trattati devono essere corretti



# MINIMIZZAZIONE, PERTINENZA E PROPORZIONALITÀ

- i dati devono essere raccolti per finalità determinate, esplicite e legittime ed in seguito trattati in modo non incompatibile con tali finalità



## **LIMITAZIONE DELLA CONSERVAZIONE**

- i dati devono essere conservati in forma che consenta l'identificazione degli interessati per un arco temporale non superiore al conseguimento delle finalità per i quali sono stati trattati, salvo eccezioni particolari



## SICUREZZA E INTEGRITÀ DEI DATI

- i dati devono essere trattati in modo da garantire un'adeguata sicurezza e protezione dei dati personali, mediante misure tecniche e organizzative adeguate per limitare trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione, o dal danno accidentale



## LE PRINCIPALI MODIFICHE

- Informativa
- Consenso
- Diritti dell'interessato
- Analisi dei rischi e delle misure di sicurezza
- Rafforzamento del diritto di oblio
- Rafforzamento delle sanzioni pecuniarie



## INFORMATIVA (ART 12 E SEG.)

- è sempre necessaria, anche se non deve essere richiesto il consenso al trattamento
- mette in grado l'interessato di conoscere le intenzioni del Titolare, di valutare le conseguenze del trattamento, di poter accettare o rifiutare il trattamento, di controllare i suoi dati
- deve essere chiara, concisa ma non generica
- è consentita anche in forma orale, ma serve l'onere della prova
- il contenuto è previsto dal Regolamento (art. 13 e 14). È quindi necessario rivedere tutte le informative in essere antecedenti

## CONSENSO (ART. 7)

- è la condizione necessaria per poter trattare i dati in modo lecito in assenza di una delle altre condizioni previste dalla legge
- deve essere libero, informato, specifico, consapevole e inequivocabile
- il consenso deve essere distinto e separato per ciascuna finalità del trattamento
- deve essere reso prima del trattamento
- può essere revocato dall'interessato in qualsiasi momento



## **DIRITTI DELL'INTERESSATO (ARTT. 15-22)**

- l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso al suo fascicolo
- sono compresi il diritto di accesso, di rettifica, di oblio, di limitazione del trattamento e di portabilità dei dati

## RAFFORZAMENTO DEI DIRITTI DEGLI INTERESSATI (ARTT. 15-22)

Diritti conoscitivi	Diritti di controllo
diritto all'informativa (artt. 13 e 14)	diritto di rettifica e di integrazione (art. 16)
diritto di accesso (art. 15)	diritto di cancellazione/oblio (art. 17)
diritto alla comunicazione di una violazione di dati (art. 34)	diritto di limitazione (art. 18)
	diritto alla portabilità dei dati (art. 20)
	diritto di opposizione (art. 21)
	diritto a non subire decisioni basate unicamente su trattamenti automatizzati (art. 22)

## **ANALISI DEI RISCHI E DELLE MISURE DI SICUREZZA (ART. 32) 1/2**

- tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, 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 per garantire un livello di sicurezza adeguato del rischio

## ANALISI DEI RISCHI E DELLE MISURE DI SICUREZZA (ART. 32) 2/2

- in questo contesto gioca un ruolo importante il settore IT in quanto deve fornire misure quali:
  - la pseudonimizzazione o la cifratura dei dati
  - la capacità di ripristinare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
  - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
  - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del dato



## **RAFFORZAMENTO DELLE SANZIONI (ART. 83 E SEG.) 1/2**

- sanzioni amministrative (avvertimento, ammonimento, inibizione al trattamento)
- sanzioni amministrative pecuniarie: devono essere effettive, proporzionali e dissuasive
- risarcimento del danno
- sanzioni penali (rimando alle disposizioni nazionali)

## **RAFFORZAMENTO DELLE SANZIONI (ART. 83 E SEG.) 2/2**

- le sanzioni amministrative pecuniarie possono essere somministrate fino a un valore massimo di 10.000.000 € o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazioni relative agli obblighi del titolare e del responsabile del trattamento
- sanzioni amministrative pecuniarie possono essere somministrate fino a un valore massimo di 20.000.000 € o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per violazioni relative ai principi di base del trattamento a condizioni relative al consenso o per violazione dei diritti degli interessati o per trasferimenti di dati personali a destinatario in paese terzo all'organizzazione
- sanzioni penali, introdotte dal D.Lgs. 101 del 10 agosto 2018, possono essere somministrate in caso di gravi illeciti nel trattamento dei dati personali





## LE PRINCIPALI NOVITA'

- Diritto alla portabilità dei dati (diritto a ottenere il trasferimento dei dati da un fornitore all'altro)
- Responsabilizzazione ed obbligo di prova (c.d. accountability)
- Figura del Data Protection Officer (D.P.O.)
- Formazione continua
- Registro dei trattamenti
- Data breach
- Valutazione d'impatto
- Codici di condotta e certificazioni

## FORMAZIONE CONTINUA SULL PRIVACY

- il GDPR prevede l'obbligo della formazione per le pubbliche amministrazioni, imprese, studi professionali in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione delegate ai trattamenti di dati (ad es. dipendenti, collaboratori)
- la centralità della formazione è confermata anche dall'art. 32 “Sicurezza del trattamento” paragrafo 4 che prevede che: *“il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”*
- la formazione deve essere pianificata, periodica e dimostrabile in caso di verifica da parte delle Autorità

## REGISTRO DEI TRATTAMENTI (ART. 30)

- l'art. 30 del Regolamento (EU) n. 679/2016 (di seguito “RGPD”) prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento
- costituisce uno dei principali elementi di Accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività
- sono previste eccezioni limitate a imprese con meno di 250 dipendenti a meno che il trattamento non sia occasionale, includa dati particolari o possa provocare rischi per diritti e libertà degli interessati



Esempio registro  
semplificato

## DATA BREACH (ARTT. 33-34)

- a partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque “senza ingiustificato ritardo”, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85)
- la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare
- NB: non tutti i “data breach” determinano l'obbligo di notificazione al Garante ; inoltre non tutti quelli notificati vanno poi comunicati ai soggetti interessati. L'elemento dirimente è costituito dalla valutazione del rischio stimato per i diritti e le libertà degli interessati, quale conseguenza della violazione dei dati personali
- la notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali; si veda il modello del Garante Privacy



Modello Garante  
Data Breach

## VALUTAZIONE D'IMPATTO (ART. 35)

- il titolare è obbligato a valutare preliminarmente l'impatto dei trattamenti che presentano rischio elevato per i diritti/libertà dell'interessato, in particolare per un elenco pre-definito di trattamenti quali:
  - la valutazione sistematica di aspetti personali, basata su trattamenti automatici, inclusa la profilazione su cui si fondano decisioni che hanno effetti giuridici sulle persone
  - i trattamenti su larga scala di dati particolari o penali
  - la sorveglianza sistematica su larga scala di zone accessibili al pubblico

# CODICI DI CONDOTTA E CERTIFICAZIONI

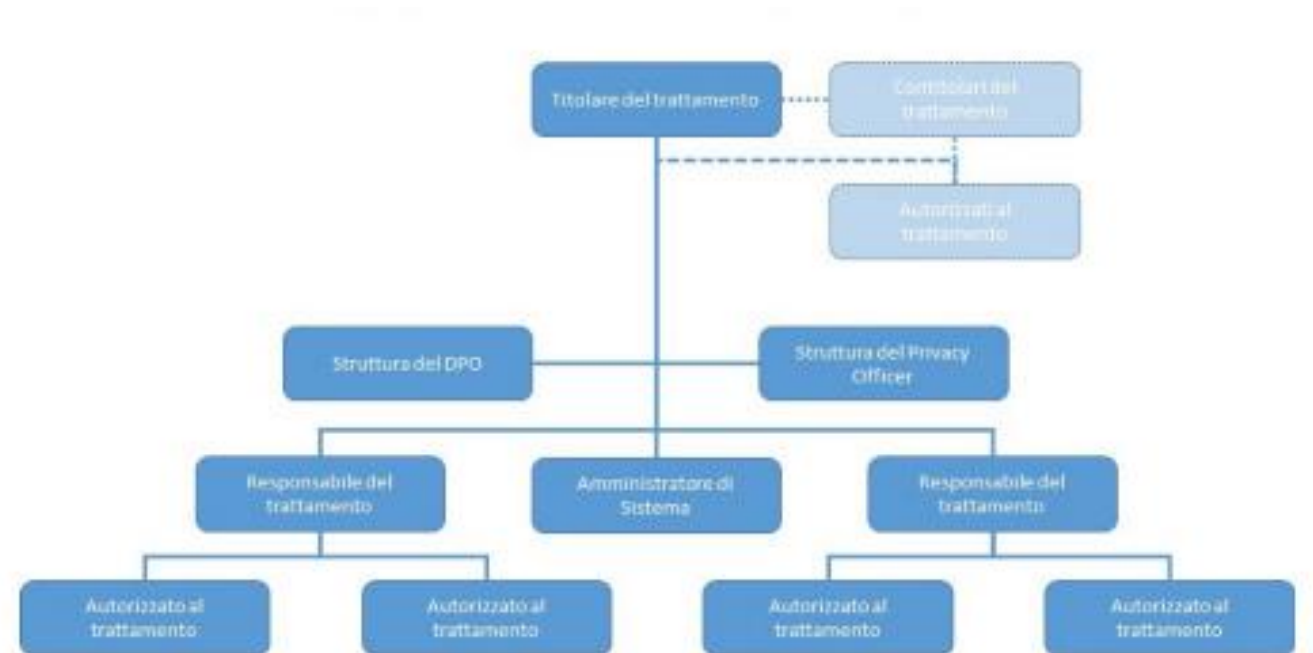
- codici di Condotta e Certificazioni sono due strumenti attraverso i quali le organizzazioni testimoniano la propria attenzione alla conformità alle normativa (artt. da 41 al 43 GDPR)
- il Regolamento incoraggia “... l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al regolamento ...” (Reg. art. 42) dei trattamenti effettuati da Titolari e Responsabili
- nel 2019 sono stati adottati due diverse tipologie di codici di condotta:
  - 1) codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali
  - 2) codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti
- con riferimento alle certificazioni, è stata recentemente siglata la convenzione Garante Privacy – Accredia sulle attività di accreditamento e certificazione previste dal Gdpr . Accredia avrà il compito nei prossimi mesi di attestare la competenza e l'adeguatezza degli organismi che ne faranno richiesta per certificare con maggiori garanzie i servizi di tutela della privacy



# **ORGANIGRAMMA PRIVACY E RUOLI IL DATA PROTECTION OFFICER (DPO)**

# ORGANIGRAMMA PRIVACY

- l'organigramma privacy raffigura in maniera sintetica la struttura che tratta dati personali dentro e fuori all'organizzazione
- le figure privacy chiave disciplinate dal GDPR sono il Titolare (e i co-titolari), il Responsabile (e sub-responsabili), il DPO e gli Autorizzati (o soggetti incaricati del vecchio D.lgs. 196)







## **LE SCELTE ORGANIZZATIVE**

Le scelte organizzative hanno un impatto su:

- **RUOLI**
- **RESPONSABILITA'**
- **SANZIONI**
- **RAPPORTI CON GLI INTERESSATI**

Le scelte devono corrispondere ai rapporti realmente instaurati (Garante, Parere del 30 giugno 1997)

# I SOGGETTI DEL TRATTAMENTO



Soggetti Attivi	Soggetti passivi	Responsabile della protezione dei dati personali
Titolare del trattamento ed eventuali contitolari	Interessati	DPO
Responsabile del trattamento		
Rappresentante del titolare o del responsabile del trattamento		
Gli incaricati al trattamento		

## TITOLARE DEL TRATTAMENTO

- titolare del trattamento: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**. Il titolare del trattamento, oltre che le finalità e i mezzi del trattamento dei dati personali, spetta anche il potere/dovere di stabilire le misure di sicurezza da adottare a tali trattamenti
- il titolare del trattamento è colui che mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento

## RESPONSABILE DEL TRATTAMENTO (ART. 28) 1/2

- il responsabile del trattamento (data processor) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
- il responsabile deve garantire di mettere in atto misure tecniche ed organizzative adeguate per la protezione dei dati trattati per conto del titolare

### ATTENZIONE

definizione già presente nel Codice privacy ma ora assume un  
significato diverso

## RESPONSABILE DEL TRATTAMENTO (ART. 28) 2/2

- responsabile «esterno» (GDPR): i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto, o altro atto giuridico, che vincoli il responsabile del trattamento (persona fisica o giuridica) al titolare del trattamento al rispetto di una serie di vincoli prestabiliti ex art. 28 del Regolamento
- responsabile «interno» (Codice privacy): l'«incaricato» era previsto nel Codice Privacy. Il Regolamento non menziona tale figura, ma all'art. 29 si parla di soggetti autorizzati al trattamento che trattano dati su istruzione del titolare o del responsabile del trattamento. In caso di organizzazione complessa è consigliata la nomina di un referente interno. Deve essere una persona con adeguate garanzie di competenza in materia

## INCARICATI (ART. 29)

- le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite
- si tratta di una volontaria responsabilizzazione di questi soggetti attraverso una specifica lettera di attribuzione di incarico che individui puntualmente l'ambito del trattamento consentito

## **RAPPRESENTANTI DI TITOLARI DEL TRATTAMENTO O DEI RESPONSABILI DEL TRATTAMENTO NON STABILITI NELL'UNIONE (ART. 27)**

- qualora il GDPR sia applicabile anche a titolari o responsabili del trattamento **NON stabiliti nell'UE**, ai sensi dell'articolo 3 (2) GDPR, **questi ultimi debbano designare per iscritto un rappresentante nell'Unione** (qualora debbano trattare dati personali o sensibili di persone fisiche stabilite nell'UE)
- la designazione di un rappresentante a cura del titolare del trattamento o del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento

## **RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO) – ART. 37 1/3**

- il Data Protection Officer (DPO) o responsabile della protezione dei dati (RPD), è una figura professionale designata dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR all'interno dell'organizzazione
- il DPO coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali
- il DPO ha il compito di analizzare, valutare e disciplinare la gestione del trattamento e della salvaguardia dei dati personali all'interno dell'organizzazione, affinché i dati personali siano trattati in modo lecito e pertinente



## DATA PROTECTION OFFICER 2/3

- il DPO rappresenta una figura di «garanzia» all'interno delle organizzazioni con diversi compiti
- la sua nomina è obbligatoria per:
  - enti pubblici
  - privati: quanto le attività principali consistono in trattamenti che per loro natura, ambito di applicazione e/o finalità richiedono il monitoraggio regolare e sistematico di interessati su larga scala oppure il trattamento su larga scala di “dati particolari” o “dati penali”

## DATA PROTECTION OFFICER 3/3

- il DPO deve avere requisiti di professionalità, esperienza e capacità di assolvere i compiti previsti dalla normativa
- può essere un dipendente del titolare o del responsabile oppure un soggetto esterno con “contratto di servizi”
- il DPO esegue le proprie funzioni in completa indipendenza (senza ricevere alcuna istruzione o imposizione gerarchica dal Titolare) e riferisce sul suo operato direttamente ai vertici aziendali, i quali, per la piena esecuzione dei suoi compiti dovranno fornire risorse adeguate



# **LA DIGITALIZZAZIONE DELLA SOCIETA' E DELLA PROFESSIONE**



**VIDEO VISUALIZZABILE AL SEGUENTE LINK**

<https://youtu.be/4JqfChAKSfE>

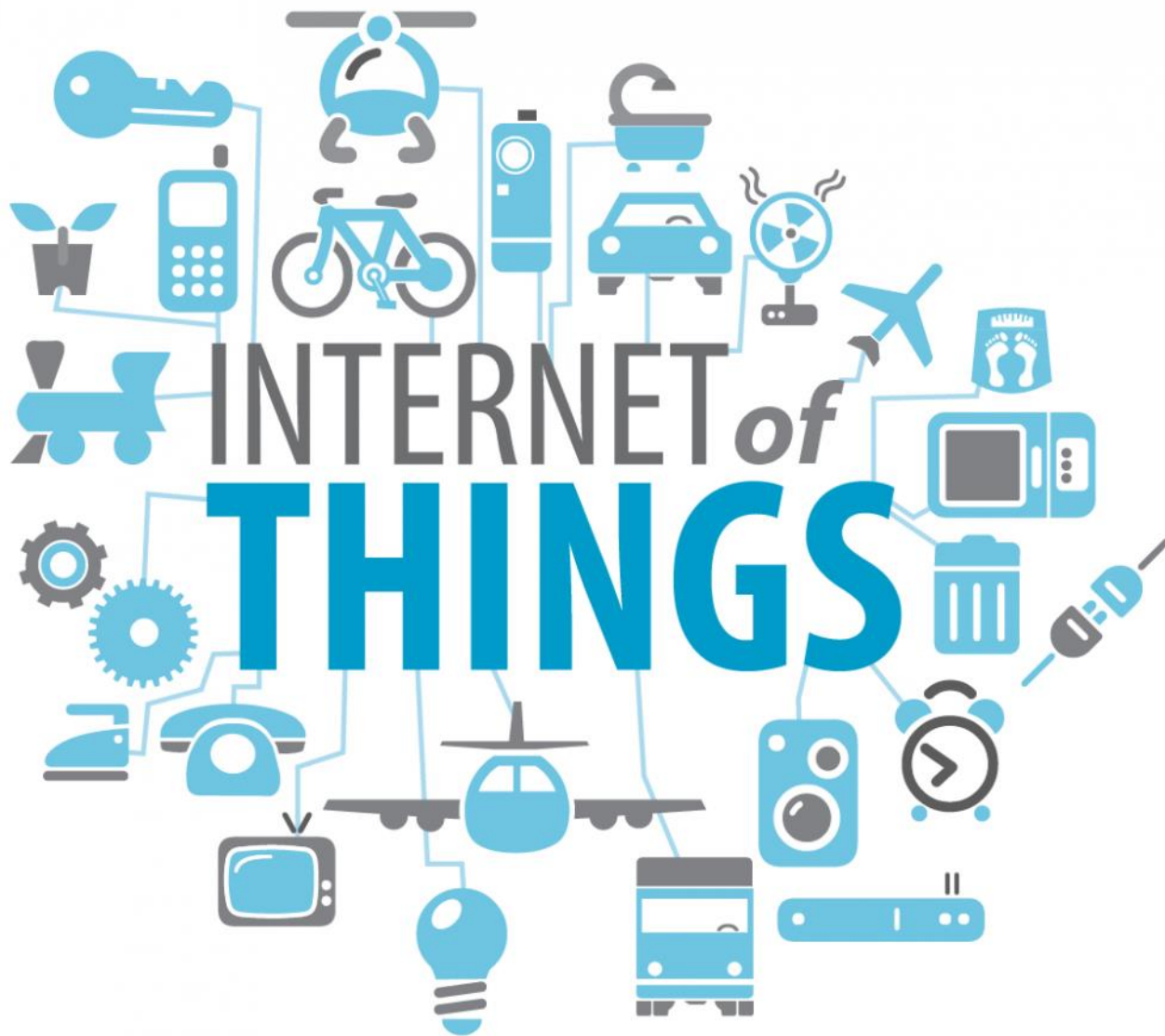
# IL DIGITALE CI HA E CI STA CAMBIANDO LA VITA



# LA DIGITAL DISRUPTION HA COMPLETAMENTE CAMBIATO IL MODO DI FARE LE COSE





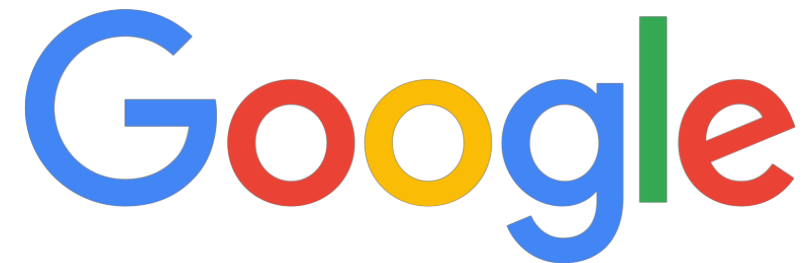


l'interconnessione, mediante Internet,  
di miliardi di oggetti intelligenti  
che ci circondano,  
ciascuno identificabile e  
indirizzabile univocamente,  
in grado di raccogliere  
memorizzare, elaborare e comunicare  
informazioni relative all'ambiente  
circostante

---

# BIG DATA

tecnologia che consente grandi elaborazione di dati in tempi molto ridotti





# LA NASCITA DELLA CITTADINANZA DIGITALE



L'insieme di diritti/doveri che, grazie al supporto di una serie di strumenti (l'identità, il domicilio, le firme digitali) e servizi, mira a semplificare il rapporto tra cittadini, imprese e pubblica amministrazione tramite le tecnologie digitali.

# IL DIGITALE È DIVENTATO IL MOTORE DELL'ECONOMIA E IL SUO CARBURANTE SONO LE INFORMAZIONI



# LA TRASFORMAZIONE DIGITALE POSSIAMO VIVERLA O SUBIRLA

Queste trasformazioni hanno attribuito maggiore importanza al diritto alla privacy perché ci hanno fatto perdere la consapevolezza dei pericoli.

Siamo passati da “the right to be let alone” all’esigenza di un diritto alla privacy sempre più tutelato dalla legge

Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire

EDWARD SNOWDEN



---

**“SE IL SERVIZIO È GRATIS, IL PRODOTTO SEI TU”**



# IL PROFESSIONISTA 2.0

Asset hardware (PC, scanner, firma digitale, server, nas, firewall, smartphone, tablet, ecc...)



Asset software (word processor, redattore PCT, gestionale di studio, sistemi operativi, antivirus, programmi di backup, ecc...)

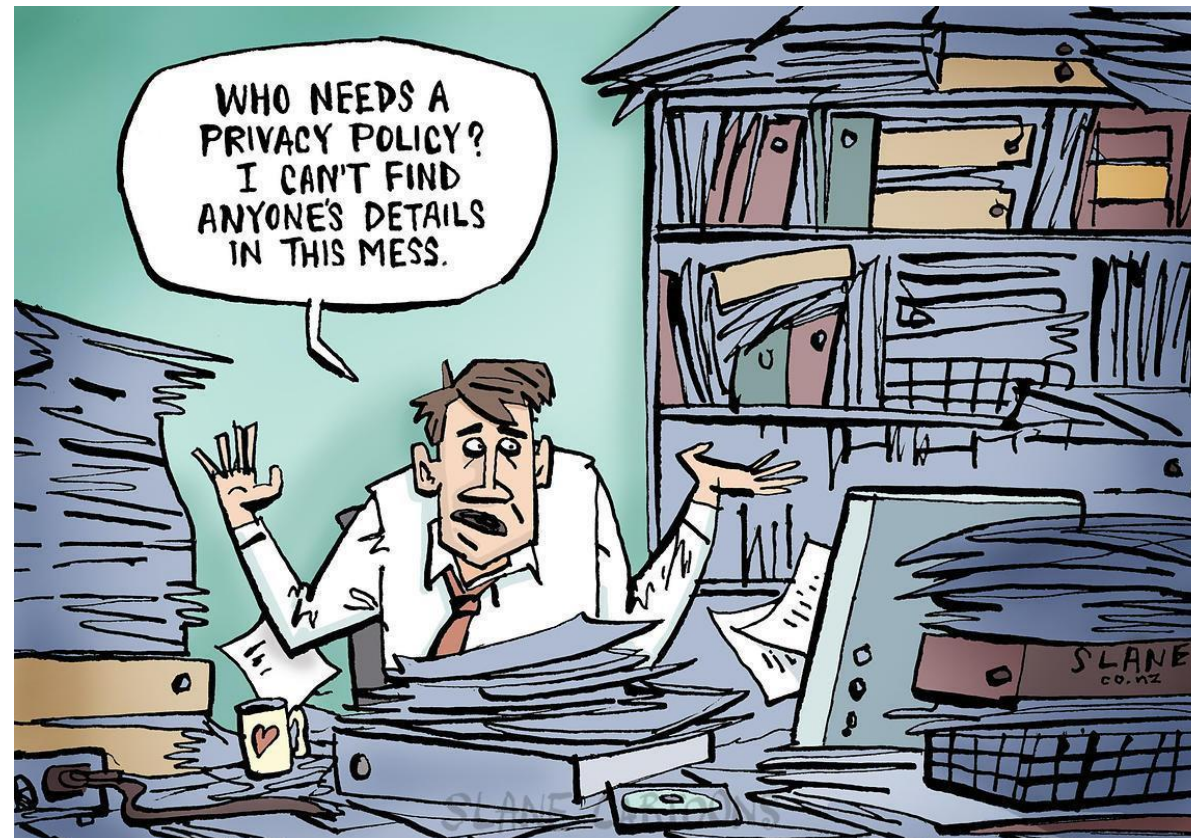
# IL PROFESSIONISTA 2.0

Connettività ad Internet (fissa e mobile), posta elettronica (ordinaria e certificata), depositi telematici, cloud, wifi, VPN, ecc...





# LE CRITICITA' DEGLI STUDI PROFESSIONALI: L'ORGANIZZAZIONE FISICA E DIGITALE DELLO STUDIO





In campo comunitario si è sviluppata l'esigenza di legiferare facendo sempre più riferimento a principi generali invece che a tecnicismi e norme che prevedessero tutte le possibili casistiche di trattamento



## ART. 24 GDPR

*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 presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento**. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.*

## ART. 25 GDPR

*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

*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, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*

## ART. 32 GDPR

*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, 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** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

*[...]*



ADDIO MISURE MINIME

BENVENUTE MISURE ADEGUATE

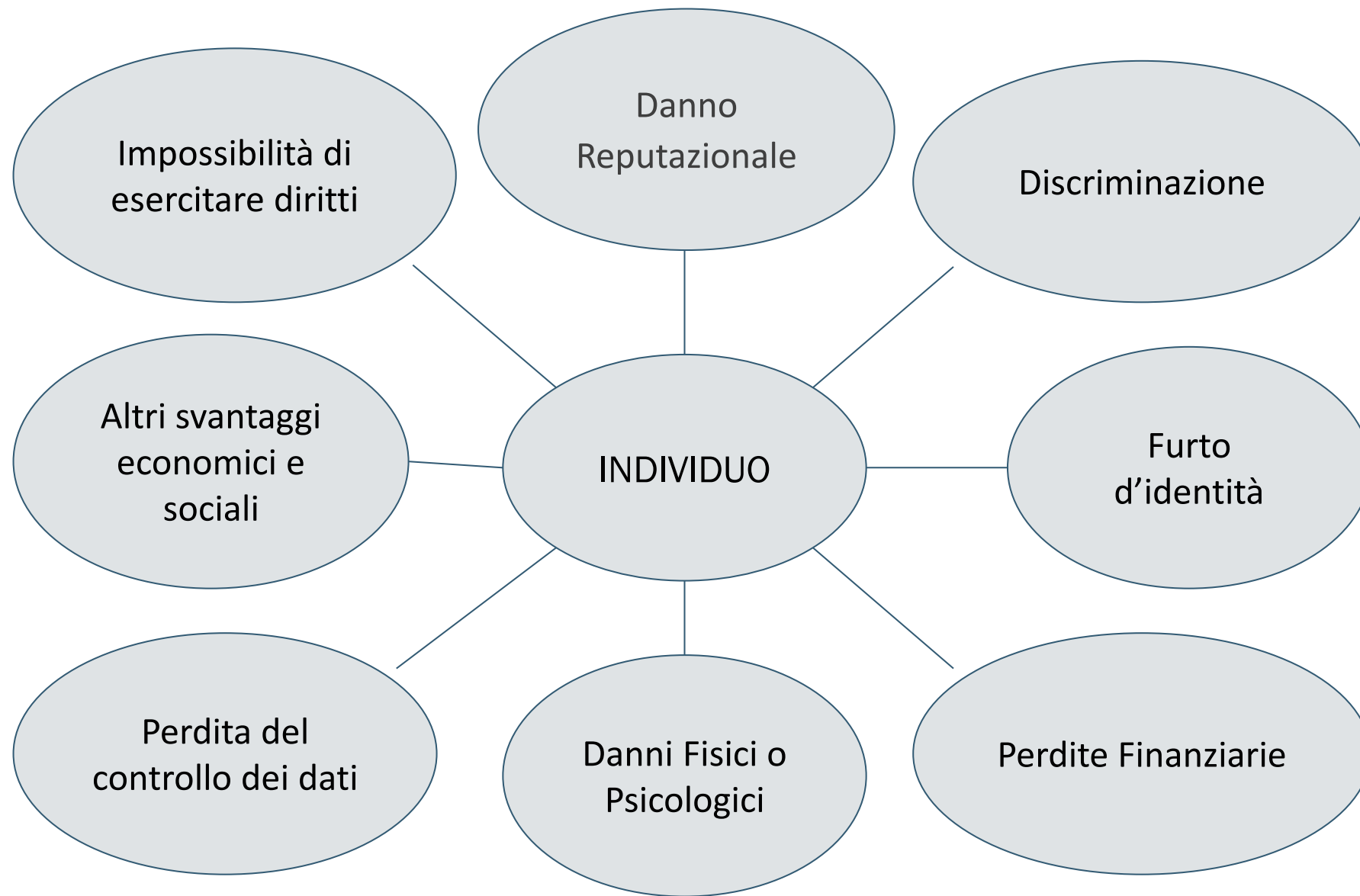
# VALUTAZIONE DEL RISCHIO

W.P. Art. 29

*“Per rischio si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità”* per i diritti e le libertà

Gravità x Probabilità = RISCHIO

Possibili Eventi: sottrazione di credenziali di autenticazione, disattenzione o incuria, comportamenti sleali o fraudolenti, azione di virus informatici o di programmi dannosi, spamming o tecniche di sabotaggio, intercettazione, eventi distruttivi naturali o artificiali, ecc...



# LE CRITICITÀ DEGLI STUDI PROFESSIONALI





## CLEAN DESK POLICY

E' la gestione sicura dei dati sul posto di lavoro in quanto un intruso o un semplice curioso può raccogliere numerosissime informazioni da:

**Cestino dei rifiuti:** dove ci sono documenti cartacei gettati appallottolati...

**Documenti:** se lasciati in giro possono contenere informazioni su clienti e fornitori, ecc...

**Agende:** se accessibili possono contenere nomi dei clienti, scadenze e informazioni simili

**Post-it (appunti):** dove spesso vengono annotate le password

**Stampante:** frequentemente le stampe vengono dimenticate nelle stampanti

**Archivi:** spesso facilmente accessibili all'interno dell'ufficio

**Chiavette USB:** molto pratiche... anche per i malintenzionati



I principali benefici di una politica della scrivania pulita sono:

- 1) buona impressione a clienti e fornitori che visitano gli uffici;
- 2) la riduzione della possibilità che i dati siano visti da persone non abilitate a conoscerle;
- 3) la riduzione della possibilità che documenti confidenziali possano essere sottratti.

#### Buone prassi:

Non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza di tali dati.

Prima di lasciare la propria postazione riporre in luogo sicuro i dati cartacei.

Ove possibile, evitare la stampa di documenti digitali.

Rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax.

Eliminare i documenti cartacei in modo adeguato.

Bloccare i computer quando ci si allontana dalla postazione di lavoro.

## VANNO DEPENNATI I NOMI DALLE PRATICHE???

*“Per quanto riguarda l'organizzazione del lavoro quotidiano di studio, va osservato che, contrariamente a quanto ipotizzato in alcuni quesiti formulati dai singoli professionisti, non occorre depennare il nome delle parti dalla copertina dei fascicoli cartacei, utilizzando al suo posto solo numeri identificativi. Resta invece necessario seguire opportune modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti”*

(Provvedimento del 3 giugno 2004 - Principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense)

Tuttavia

Art. 25 GDPR: “pseudonimizzazione”

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

# PASSWORD

Il Messaggero.it

MENU CERCA

## ITALIA

› ROMA

### Anonymous buca le mail di 30.000 avvocati. Virginia Raggi: «Grave violazione della privacy»

ITALIA

Martedì 7 Maggio 2019 di Mauro Evangelisti e Fabio Rossi



L'anno scorso avevano attaccato e diffuso i dati del Cnr, delle Ferrovie, del ministero dello Sviluppo economico, del consiglio regionale della Sardegna e del Comune di Palermo, persino della Polizia e di Fratelli d'Italia. Ieri invece Anonymous, il collettivo globale di hacker, ha acquisito e diffuso

#### Le password:

87 "avvocato"

32 "1234567"

25 "forzaroma"

19 "lorenzo"

18 "francesco"

18 "camilla"

17 "francesca"

16 "alessandro"

15 "federica"

15 "stefano"

Il 33% delle password erano di soli 8 caratteri (2.354 di 7 caratteri)



# BUONE PRASSI

**Il National Institute of Standards and Technology ha pubblicato le nuove regole per la sicurezza delle password:**

- 1) Decade l'obbligo di modifica periodica delle password in quanto spinge l'utente ad utilizzare password banali, prevedibili e strettamente correlate tra loro.
- 2) Decade l'obbligo di composizione complessa (numeri, maiuscole, minuscole, simboli) in quanto statisticamente gli utenti usano la maiuscola all'inizio e numeri e caratteri speciali in fondo.
- 3) Non utilizzare le domande di sicurezza perché troppo banali
- 4) Incentivare l'utilizzo di password manager
- 5) Attivare l'autenticazione in due fattori utilizzando il sistema "Multi-Factor OTP Device", cioè la generazione del token attraverso un'app e non con l'invio di un sms.

Modificare al primo accesso la password.

Mantenere la password segreta nei confronti di chiunque.

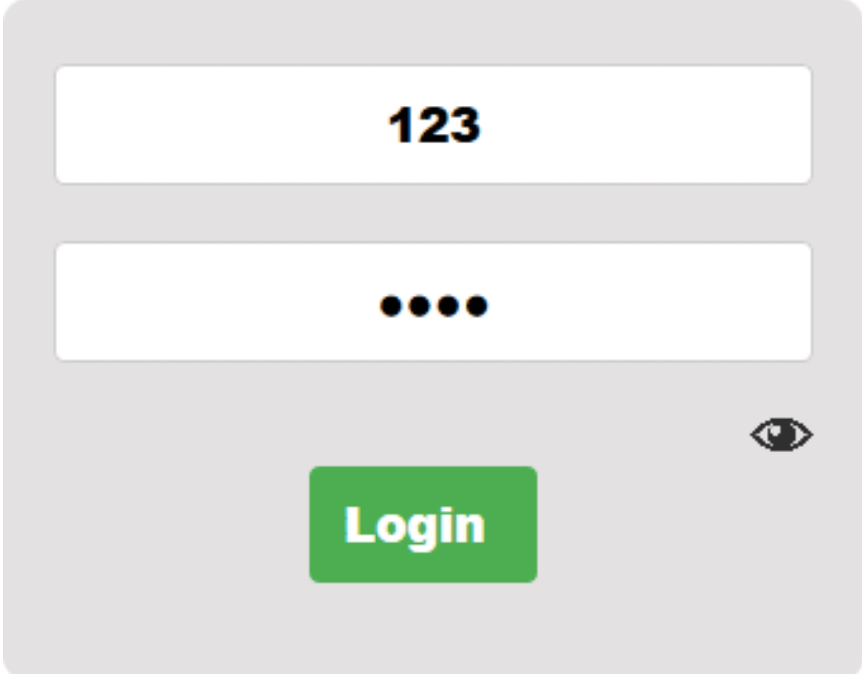
Sostituire la password anche in caso di semplice sospetto circa la venuta meno della sua segretezza.

Comporre le password con almeno 8-14 caratteri

Non memorizzare la password su supporti facilmente intercettabili (Post-It, agende, ecc...)

# NON UTILIZZARE COME PASSWORD

Nome, cognome e loro parti;  
Username assegnato;  
Indirizzo di posta elettronica (e-mail);  
Parole comuni (in Inglese e in Italiano);  
Date, mesi dell'anno e giorni della settimana, anche in lingua straniera;  
Parole banali e/o di facile intuizione;  
Ripetizioni di sequenze di caratteri (es. abcabcabc);  
Anche solo parzialmente il nome dell'utente;  
Password utilizzate in attività o situazioni non lavorative;



The illustration shows a login interface on a light gray background. It features two white input fields. The top field contains the text '123'. The bottom field contains four black dots. Below the input fields is a green rectangular button with the word 'Login' in white. To the right of the button is a small black icon of an eye, used for toggling password visibility.

# INVIO DATI PARTICOLARI A MEZZO MAIL



La comunicazione (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata (Articolo 4 D.lgs. 30 giugno 2003, n. 196 - Abrogato).

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 GDPR).

Tenendo conto della **natura, dell'oggetto, del contesto, delle finalità del trattamento e del rischio** il titolare del trattamento mette **in atto misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato (la pseudonimizzazione, la **cifratura dei dati personali**, ecc...). Nel valutare l'adeguato livello di sicurezza, si tiene conto dei **rischi** di distruzione, perdita, modifica, divulgazione o **accesso dati personali trasmessi**. (Art. 32 GDPR)

# INFORMATIVA

L' informativa ex articoli 13 e 14 deve essere concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. (Art. 12 GDPR)

*“Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione [...]” (Considerando 58 GDPR)*





# BASI GIURIDICHE

Liceità del trattamento (art. 6 GDPR)

Consenso

Esecuzione di un contratto o di misure precontrattuali

Adempiere un obbligo legale

Legittimo interesse del titolare del trattamento



# BASI GIURIDICHE

## Trattamento di categorie particolari di dati (art. 9 GDPR)

### Consenso

Assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale

Il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

Accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

Finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale

## CLOUD COMPUTING



# CLOUD COMPUTING



In informatica con il termine inglese cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone il Titolare a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati in server farms di aziende che spesso risiedono in uno stato diverso da quello del Titolare.

Pertanto è prioritario considerare la sicurezza dei dati. I dati devono essere sicuri e integri e tutelati da normative adeguate (GDPR - ISO 27001)

## AMBITO DI APPLICAZIONE TERRITORIALE ART. 3

Qui si raggiunge la massima espansione possibile del diritto europeo in materia di protezione dei dati personali che radica la propria competenza, non sulla base del luogo dove il titolare o il responsabile del trattamento sono “stabiliti” (ancorché con l’ampia accezione con la quale il concetto di stabilimento deve essere interpretato precedentemente descritta) ma in ragione di quello ove si trova il “target” del loro trattamento.



## APPLICAZIONE TERRITORIALE

	Interessati in UE	Interessati fuori UE
Stabilimento in UE	Si anche se il trattamento è effettuato fuori UE	
Stabilimento fuori UE	Si per offerte di beni e servizi	No

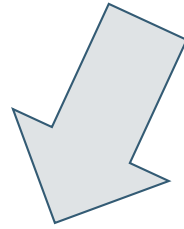
# TRASFERIMENTO VERSO PAESI EXTRA UE



I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono consentiti a condizione che l'adequatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento UE 2016/679).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679).

# POSSONO COSTITUIRE GARANZIE ADEGUATE



## **senza autorizzazione da parte del Garante**

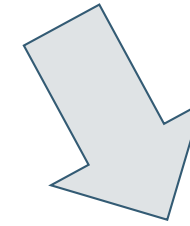
gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);

le norme vincolanti d'impresa (art. 46, par. 2, lett. b)

le clausole tipo (art. 46, par. 2, lett. c e lett. d)

i codici di condotta (art. 46, par. 2, lett. e)

i meccanismi di certificazione (art. 46, par. 2, lett. f)



## **previa autorizzazione del Garante**

le clausole contrattuali ad hoc (art. 46, par. 3, lett. a)

gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b)



# DECISIONI DI ADEGUATEZZA



Andorra  
Argentina  
Australia (Passenger Name Record)  
Canada  
Faer Oer  
Giappone  
Guernsey  
Isola di Man  
Israele  
Jersey  
Nuova Zelanda  
Svizzera  
Uruguay  
USA Privacy Shield  
USA (Passenger Name Record)



# FATTURAZIONE ELETTRONICA

Comunicato del 16 novembre 2018

Il nuovo obbligo della fatturazione elettronica presenta rilevanti criticità in ordine alla compatibilità con la normativa in materia di protezione dei dati personali.

La fatturazione elettronica presenta un rischio elevato per i diritti e le libertà degli interessati, comportando un trattamento sistematico, generalizzato e di dettaglio di dati personali su larga scala, potenzialmente relativo ad ogni aspetto della vita quotidiana dell'intera popolazione, sproporzionato rispetto all'obiettivo di interesse pubblico, pur legittimo, perseguito.

La fattura contiene informazioni di dettaglio come la descrizione delle prestazioni sanitarie o legali.

Provvedimento del 20 dicembre 2018

I soggetti che erogano prestazioni sanitarie non dovranno emettere fattura elettronica

E gli altri ?????



# CYBERSECURITY

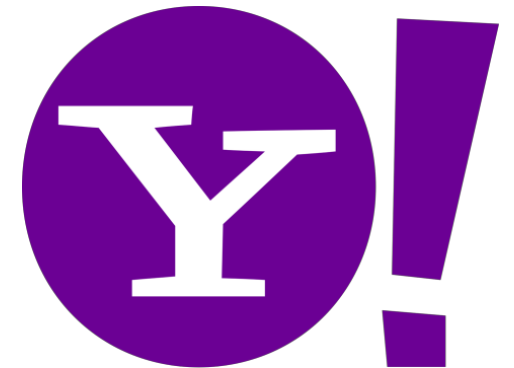
- 1) Il pop up che appare chiedendo di aggiornare i programmi non serve a misurare la vostra velocità nel cliccare no;
- 2) Gli antivirus o anti malware non sono degli optional che si possono installare a piacimento sui dispositivi elettronici;
- 3) Il backup non è una prassi obbligatoria solo per le grandi aziende;
- 4) Non basta un semplice programma per essere compliance;
- 5) I programmi gratuiti (mail, antivirus, redattori, ecc....) non garantiscono, quasi mai un adeguato sistema di sicurezza



# MINACCE ALLA SICUREZZA E CONTROMISURE

*“Ci sono due tipi di aziende, quelle che sono state hackerate e quelle che ancora non sanno di esserlo state”*

John Chambers



# CANALI DI ATTACCO

Email Phishing  
Telefonate  
Incontri faccia a faccia  
Dumpster diving  
Shoulder Surfing  
Baiting



Nella sicurezza l'anello più vulnerabile è il fattore umano.

Per questo motivo È importante educare e sensibilizzare il personale, con lo scopo di applicare, con la migliore accuratezza possibile, le politiche di sicurezza.

# SOCIAL ENGINEERING



L'atto di manipolare le persone per farle compiere azioni o divulgare informazioni riservate



# **RIFLESSIONI FINALI**

# BUONE PRASSI



Non fornire informazioni personali o riguardanti l'organizzazione se non si è sicuri dell'identità dell'interlocutore e della sua necessità di avere accesso a tali informazioni

Non cliccare su link sconosciuti

Se non si è certi della legittimità dell'email ricevuta o di quanto in essa contenuto verificare direttamente il mittente della stessa

Fare attenzione all'url dei siti

I luoghi ove si svolge il trattamento dei dati personali devono essere opportunamente protetti da indebite intrusioni

Policy per l'uso della strumentazione informatica

Conservazione dei dati solo per il tempo strettamente necessario



# PROFESSIONISTI E PRIVACY:

## BREVE GUIDA AGLI ADEMPIMENTI



- 1) Rivedere informative e condizioni di liceità
- 2) Nominare i responsabili esterni, gli autorizzati al trattamento e gli eventuali contitolari
- 3) Creare il registro delle attività di trattamento ex art. 30 (Seppur non gravi un obbligo di adozione del registro in capo ai professionisti, il Garante ne raccomanda l'adozione)
- 4) Valutazione del rischio per l'adozione di misure tecniche ed organizzative adeguate
- 5) Creare il registro e la policy "Data Breach"
- 6) Stabilire una politica di "Data Retention"
- 7) Creare una policy per l'esercizio dei diritti degli interessati
- 8) Creare un regolamento interno
- 9) Formazione



**VI RINGRAZIAMO PER LA PARTECIPAZIONE**