ADEGUARSI AL GDPR
IN 6 (+ 10 + 1) MOSSE

1. CONOSCERE GDPR (Regolamento UE 2016 679)

I PRINCIPI BASE PER IL TRATTAMENTO DEI DATI

ART. 5

ART. 6

1. CONOSCERE GDPR
ART. 5 GDPR

Principi applicabili al trattamento di dati personali
1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono
trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

(segue)

1. CONOSCERE GDPR
ART. 5 GDPR

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) 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»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

1. CONOSCERE GDPR
ART. 5 GDPR

- Liceità, correttezza e trasparenza
- limitazione della finalità
- minimizzazione dei dati
- esattezza
- limitazione della conservazione
- integrità e riservatezza
- responsabilizzazione

1. CONOSCERE GDPR
ART. 6 GDPR

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

1. CONOSCERE GDPR
ART. 6 GDPR

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti

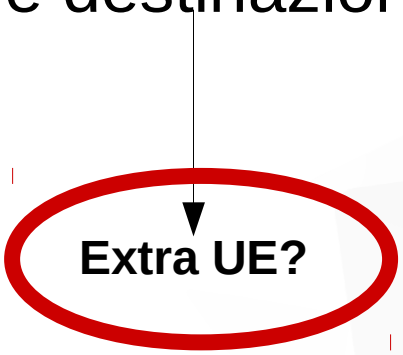
1. CONOSCERE GDPR
ART. 6 GDPR

- consenso
- esecuzione di un contratto
- adempiere un obbligo legale
- (perseguimento del legittimo interesse del titolare)

2. MAPPA DEI TRATTAMENTI

IDENTIFICARE

- I DIVERSI TRATTAMENTI
- LE CATEGORIE DI DATIGLI OBIETTIVI DEI TRATTAMENTI
- LE PERSONE (INTERNE O ESTERNE) CHE TRATTANO I DATI
- I FLUSSI DEI DATI (origine e destinazione)



2. MAPPA DEI TRATTAMENTI

«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali,come

- 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

2. MAPPA DEI TRATTAMENTI

«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come

- Il nome
- un numero di identificazione
- dati relativi all'ubicazione
- un identificativo online
- uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2. MAPPA DEI TRATTAMENTI

Per ogni trattamento bisogna porsi le seguenti domande

- CHI?
  - CHI TRATTA I DATI
- CHE COSA?
  - CHE DATI SONO TRATTATI
- PERCHÉ?
  - QUALI SONO LE FINALITÀ DEL TRATTAMENTO
- DOVE?
  - DOVE SONO CUSTODITI I DATI (ANCHE IN CHE PAESE)
- FINO A QUANDO?
  - PER QUANTO TEMPO SONO CONSERVATI
- COME?
  - CHE MISURE DI SICUREZZA UTILIZZIAMO

2. MAPPA DEI TRATTAMENTI

Avete appena fatto il

Registro dei Trattamenti

3. PIANO DI AZIONE

VERIFICARE

- UTILIZZIAMO SOLO I DATI STRETTAMENTE NECESSARI?
- QUALE BASE GIURIDICA DI TRATTAMENTO?
  - Consenso? Contratto? Obbligo legale? Interesse legittimo?
- LA NOSTRA INFORMATIVA È AGGIORNATA?
- I RESPONSABILI DEL TRATTAMENTO SONO INFORMATI DEI NUOVI OBBLIGHI DEL GDPR?
- ABBIAMO PREVISTO LE MODALITÀ DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO E COME ADEMPIERE?
  - Diritto di accesso, di rettifica, ritiro del consenso, diritto alla portabilità dei dati, etc.
- ABBIAMO VERIFICATO LE MISURE DI SICUREZZA?

4. GESTIRE IL RISCHIO

IN ALCUNI CASI è NECESSARIO FARE **PIA**
(*PRIVACY IMPACT ASSESSMENT,*
VALUTAZIONE D'IMPATTO PRIVACY)

ART. 35 GDPR

"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare ***un rischio elevato per i diritti e le libertà delle persone fisiche****, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali"*

4. GESTIRE IL RISCHIO

QUANDO È NECESSARIA PIA?

Linee guida di art. 29 WP

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)

4. GESTIRE IL RISCHIO

QUANDO È NECESSARIA PIA?

Linee guida di art. 29 WP

1) valutazione o assegnazione di un punteggio
2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3) monitoraggio sistematico
4) dati sensibili o dati aventi carattere altamente personale
5) trattamento di dati su larga scala
6) creazione di corrispondenze o combinazione di insiemi di dati
7) dati relativi a interessati vulnerabili
8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
9) quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"

Se il trattamento soddisfa 2 criteri, è altamente consigliato fare PIA.

4. GESTIRE IL RISCHIO

QUANDO NON È NECESSARIA PIA?

Linee guida di art. 29 WP

Quando non è richiesta una valutazione d'impatto sulla protezione dei dati? Quando il trattamento non è tale da "presentare un rischio elevato" oppure qualora esista una valutazione d'impatto sulla protezione dei dati analoga, o qualora il trattamento sia stato autorizzato prima del maggio 2018 oppure abbia una base giuridica o sia incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate.

"Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate" (considerando 171).

4. GESTIRE IL RISCHIO

QUANDO NON È NECESSARIA PIA?

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Autorizzazione n. 4/2016 - Autorizzazione al trattamento dei dati sensibili da parte dei liberi professionisti - 15 dicembre 2016 [5797347]

AUTORIZZA

i liberi professionisti iscritti in albi o elenchi professionali a trattare i dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, secondo le prescrizioni di seguito indicate.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5797347

5. ORGANIZZARE I PROCESSI INTERNI

- Privacy by default e by design
  - VALUTARE ASPETTI PRIVACY FIN DALL'ORIGINE
- Formare i collaboratori
  - UNA CATENA È FORTE SOLTANTO COME IL SUO ANELLO PIÙ DEBOLE
- Trattare i reclami e le domande degli interessanti in ordine ai loro diritti
  - DIRITTO ACCESSO, RETTIFICA, RITIRO DEL CONSENSO, PORTABILITÀ
- Prevedere notifica a Garante in caso di Data Breach
  - SAPERE COSA FARE IN CASO DI INCIDENTE

6. DOCUMENTARE LA CONFORMITÀ

- **LA DOCUMENTAZIONE DEI TRATTAMENTI DEI DATI PERSONALI**
  - REGISTRO DEI TRATTAMENTI
  - VALUTAZIONE IMPATTO PRIVACY (PIA)
  - QUADRO DEI TRASFERIMENTI DEI DATI EXTRA-UE
- **INFORMAZIONI AGLI INTERESSATI**
  - IL MODELLO DI INFORMATIVA
  - PROCEDURE PER ESERCIZIO DEI DIRITTI
- **CONTRATTI CHE DEFINISCONO I RUOLI DEGLI ATTORI**
  - CONTRATTI CON I RESPONSABILI
  - PROCEDURE IN CASO DI VIOLAZIONI O PERDITA DI DATI
  - PROVA CHE GLI INTERESSATI HANNO FORNITO IL CONSENSO

6. DOCUMENTARE LA CONFORMITÀ

Félicitations ! Vous êtes prêts !

(sicuri?)

7. CHECKLIST DEL PROFESSIONISTA*

1.
Ho predisposto la modulistica per procedere, durante il primo incontro con il Cliente, alla raccolta dei dati fornendo al medesimo una informativa completa, con un linguaggio semplice e chiaro?

La raccolta dei dati deve essere accompagnata – se non preceduta – da una informativa che contenga tutte le informazioni richieste dall'art. 13 (oggi del Testo Unico[1], dal 25 maggio 2018 del Regolamento[2]). Tra le novità del Reg.to figura il requisito del “linguaggio semplice e chiaro” dell'informativa.

* Articolo di Paolo Marini da Altalex
http://www.altalex.com/documents/news/2018/03/29/gdpr-privacy-il-decalogo-per-il-professionista

7. CHECKLIST DEL PROFESSIONISTA

2

Ho organizzato le mie attività in modo da raccogliere e trattare solo ed esclusivamente i dati che mi sono necessari o utili in vista del miglior espletamento del mandato professionale ricevuto?

Il principio generale è presente tanto nel T.U. (art. 11) quanto nel Reg.to (art. 5, c.d. “minimizzazione dei dati”): si raccolgono e si trattano esclusivamente i dati personali che non siano “eccedenti” rispetto alle finalità del trattamento, ovvero che siano “limitati a quanto necessario rispetto alle finalità per le quali sono trattati”.

La disponibilità di dati estranei alla finalità esplicitata segnala la sussistenza di un trattamento 'abusivo', ulteriore e distinto.

7. CHECKLIST DEL PROFESSIONISTA

3

Ho organizzato la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato?

Qui si congiungono le esigenze generali della disponibilità e della riservatezza delle banche dati. La loro traduzione concreta è una gestione ordinata dei dati e delle informazioni – ovvero dei fascicoli cartacei e delle cartelle digitali - che ponga i rispettivi contenuti al riparo da sguardi indiscreti ovvero da accessi di estranei ma che allo stesso tempo consenta al titolare di gestire con efficienza le attività.

7. CHECKLIST DEL PROFESSIONISTA

4

Ho nominato e adeguatamente istruito i miei collaboratori ed altresì ho formalizzato i rapporti con i professionisti ai quali mi rivolgo per la gestione e lo sviluppo delle attività dello studio?

Tutto l'organigramma 'privacy' dello studio deve essere coinvolto nella politica di protezione dei dati. E' un organigramma ampio, in cui rientrano gli incaricati (collaboratori, praticanti, dipendenti) ma anche i responsabili dei trattamenti, cioè i professionisti esterni che a vario titolo collaborano con lo studio (avvocati di altri fori, commercialista, consulente del lavoro, ecc.). Osservando che:

- per gli incaricati occorre una nomina (art. 30 T.U.) contenente peraltro le istruzioni operative per i trattamenti (di cui anche all'art. 29 Reg.to)

- per i responsabili dei trattamenti, occorre un contratto (o altro atto giuridico) che vincoli i medesimi a specifici obblighi (art. 28 Reg.to)

7. CHECKLIST DEL PROFESSIONISTA

5	
I miei pc sono protetti dalle minacce esterne? Dispongo, in caso di bisogno, del nominativo di un tecnico-informatico di fiducia al quale chiedere la soluzione di specifici problemi?	Il riferimento è all'implementazione di software adeguati a prevenire attacchi o minacce di vario genere e provenienza. In tal senso può essere saggio affidarsi alla competenza e all'esperienza di un professionista, rammentando che il Reg.to richiede misure “adeguate” rispetto alle caratteristiche, modalità e contesto dei trattamenti.

7. CHECKLIST DEL PROFESSIONISTA

6

Pc portatili e altri strumenti informatici rimovibili sono utilizzati nelle attività al di fuori dello studio in modo da minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari?

L'esempio lampante è nell'uso della penna Usb: premessa l'operatività di una valida password di accesso, è necessario caricare/lasciare nella penna esclusivamente i dati che debbano essere trattati nel corso della sessione esterna.

7. CHECKLIST DEL PROFESSIONISTA

7

Provvedo ad eseguire un salvataggio integrale (back up) di tutti i dati su pc perlomeno 1 volta alla settimana?

A parte la prescrizione di cui all'Allegato B al T.U., questa operazione è davvero fondamentale per la protezione dei dati dello studio. In relazione alla intensità delle modifiche/inserimenti quotidiani, è prudente programmare una frequenza maggiore di quella minima.

7. CHECKLIST DEL PROFESSIONISTA

8

Ho definito un tempo di conservazione dei dati personali in linea con le finalità dei trattamenti?

Anche il professionista è tenuto, come ogni titolare, a definire il periodo di conservazione dei dati (che non possono essere conservati ad libitum) e, peraltro (novità del Reg.to), a farne oggetto di apposita menzione nell'informativa (in alternativa al periodo di conservazione sarà sufficiente indicare i criteri utilizzati per determinarlo).

7. CHECKLIST DEL PROFESSIONISTA

9

Quando devo rottamare pc, notebooks e altri strumenti elettronici utilizzati per le attività dello studio, mi assicuro che la dismissione avvenga nel rispetto della esigenza di protezione dei dati?

La c.d. 'spazzatura elettronica', quando non gestita, è malaugurata fonte di informazioni a tutto discapito degli interessati e con rischi per lo stesso titolare del trattamento. E' doveroso il rinvio a quanto stabilito dal Garante nel provvedimento del 5 dicembre 2008 (con le connesse istruzioni operative).

7. CHECKLIST DEL PROFESSIONISTA

10

Mi sono preoccupato della sicurezza fisica dello studio, nel senso di adottare misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretantesi nella lesione della riservatezza, della disponibilità, della integrità delle banche dati?

E' sempre in evidenza il problema della sicurezza dei trattamenti. Stavolta, però, esso è valutato attraverso la disamina dei locali/luoghi fisici in cui si svolgono le attività dello studio. Le misure di protezione “adeguate”, anche qui, possono variare in ragione del contesto (ad es., studio localizzato in stanza all'interno di unità immobiliare dove sono presenti altri professionisti, studio localizzato al piano terra di un condominio, ecc.).

8. COME CAMBIA INFORMATIVA

- Informativa comprensibile e con linguaggio semplice e chiaro, adeguato rispetto a chi si rivolge (anche minore)
- Durata del trattamento
- Possibilità di ricorso ad Autorità di controllo
- Possibilità di revoca (con stesse modalità di consenso)

8. COME CAMBIA INFORMATIVA

- l’identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- le finalità del trattamento:
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l’intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un’organizzazione internazionale;

8. COME CAMBIA INFORMATIVA

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- il diritto di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

8. COME CAMBIA INFORMATIVA

per un raffronto tra la vecchia e la nuova informativa
vedi l'articolo di Paolo Marini "Informativa privacy: ecco come redigerla"
su Altalex
http://www.altalex.com/documents/news/2016/10/25/informativa-privacy-e-regolamento-europeo

9. DOBBIAMO NOMINARE DPO?

Quando è necessario nominare DPO (DATA PROTECTION OFFICER)?

Obbligatorio in 3 casi:

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

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

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici

9. DOBBIAMO NOMINARE DPO?

Cosa dice WP29.

Attività principale: le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria" (considerando 97).

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento.

Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente.

9. DOBBIAMO NOMINARE DPO?

Cosa dice WP29.

Su larga scala: “che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato” (considerando 91).

Occorre tenere conto dei seguenti fattori:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in

percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell’attività di trattamento;
- la portata geografica dell’attività di trattamento.

9. DOBBIAMO NOMINARE DPO?

Cosa dice WP29.

Alcuni esempi di trattamento **non** su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un **singolo avvocato**.

T.HANKS