Privacy 2018: gli adempimenti per i professionisti

7 maggio 2018 – Gruppo24ore – ODCEC Taranto

Avv. Giulia Escurolle

Dottore di ricerca - Università degli Studi di Torino

Perché proteggere i dati ?

https://www.youtube.com/watch?v=qYnmfBiomlo

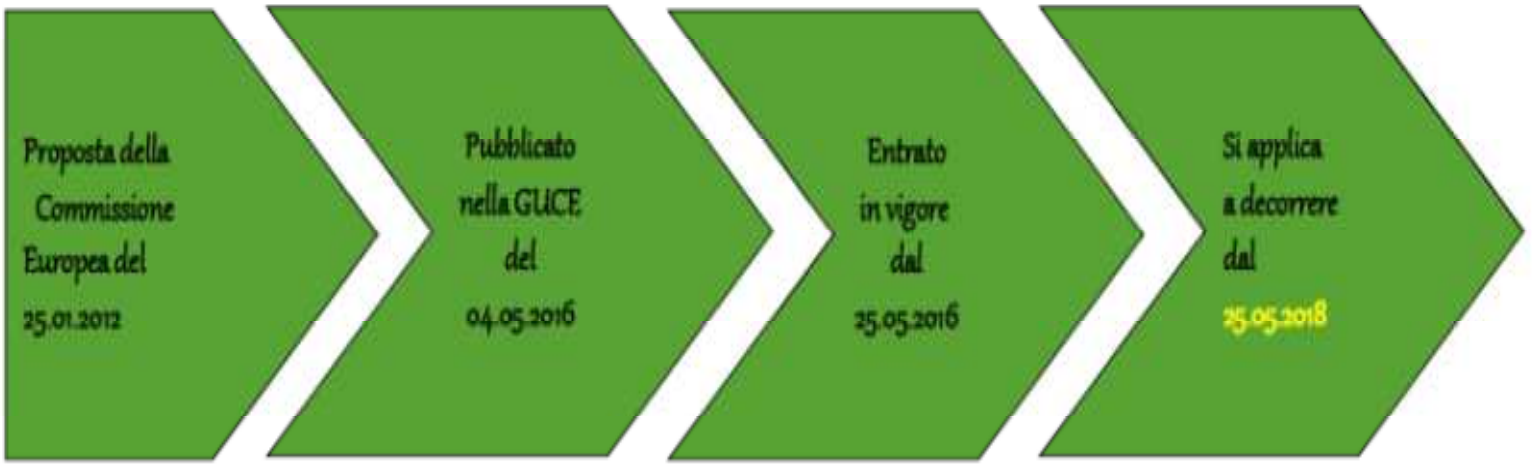
Perché proteggere i dati ?

...ormai ci siamo evoluti (o involuti?) in un nuovo modello di convivenza sociale e viviamo on line la nostra esistenza, dove i dati sono sempre di più una «merce di scambio»...

Dal Codice privacy al Regolamento UE 679/2016

- ✓**Regolamento 679/2016 «*relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché della libera circolazione dei dati*»;**
- ✓**Pubblicazione nella G.U. dell'Unione Europea n. 119/2016: 4 maggio 2016;**
- ✓**Entrata in vigore: 25 maggio 2016;**
- ✓**Applicabilità in tutti i Paesi dell'U.E.: 25 maggio 2018;**
- ✓ **99 articoli, 173 considerando;**
- ✓**Tutti i soggetti interessati hanno due anni di tempo per adeguare alle nuove norme le politiche di trattamento dei dati;**
- ✓**Il Regolamento sarà immediatamente applicabile senza necessità di adeguamento, art. 99: «*il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri*».**

Il percorso di approvazione del nuovo Regolamento



Il nuovo Regolamento UE 679/2016, c.d. GDPR «General Data Protection Regulation»

FINALITA':

- ridisegna il sistema normativo della privacy;
- offre un quadro più solido per la protezione dei dati;
- disciplina le nuove tecnologie;
- è incentrato sulla tutela dei dati delle persone fisiche;
- attua l'armonizzazione della privacy all'interno dell'UE, per evitare una normativa frammentaria che ostacoli la circolazione dei dati da una nazione all'altra e che si possa generare una disparità di trattamento tra uno S.M. e l'altro;
- rimozione degli ostacoli per gli investimenti.

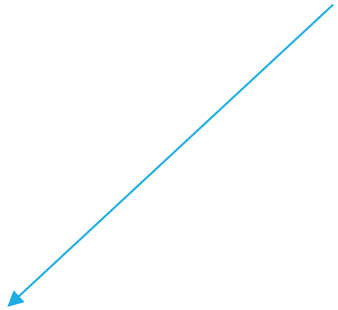
Il nuovo Regolamento UE 679/2016, c.d. GDPR «General Data Protection Regulation»

BENEFICI ATTESI:

- aumento della fiducia nei cittadini;
- certezza del diritto;
- creazione di maggiore trasparenza nei rapporti tra gli operatori economici infra/extra UE;
- determinazione dei medesimi obblighi e responsabilità per tutti gli operatori;
- tutela della concorrenza.

Il nuovo Regolamento UE 679/2016, c.d. GDPR «General Data Protection Regulation»

CONSEGUENZE NORMATIVE



abroga la Direttiva EU 95/46 (L. 675/1996)? Sì

Il nuovo Regolamento UE 679/2016, c.d. GDPR «General Data Protection Regulation»

Legge 25 ottobre 2017, n. 163:

1. **art. 13 delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;**
2. **Il Governo entro 6 mesi è delegato ad adottare uno o più decreti attuativi al fine di adeguare il quadro normativo nazionale;**
3. **Nell'attuazione della delega il Governo può:**

- abrogare le disposizioni del D.lgs. 196/2003 incompatibili con il GDPR;

- modificare il Codice privacy limitatamente a quanto necessario per dare attuazione al GDPR;

- coordinare le disposizioni vigenti in materia di protezione dei dati con le disposizioni recate dal GDPR.

Il nuovo Regolamento UE 679/2016, c.d. GDPR «General Data Protection Regulation»

Schema di D.lgs.(21 marzo 2018): ***«a far data dal 25 maggio 2018, il vigente Codice in materia di protezione dei dati personali (D.lgs. 196/03) sarà abrogato e la nuova disciplina in materia sarà rappresentata dalle disposizioni del Regolamento UE 679/2016, immediatamente applicabili, e da quelle recate dallo schema di decreto volte ad armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della privacy».***

Ambito di applicazione materiale

Il Regolamento si applica:

- **solo al trattamento dei dati relativi a persone fisiche = «*interessato*» *che si trovi nell'UE, a prescindere dalla nazionalità o dal luogo di residenza (c.14);***
- **al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (art. 2, co. 1).**

nozione di «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 2).

Ambito di applicazione materiale

Il Regolamento non si applica (art. 2, co.2):

- **ai dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto (c.14) → N.B. no rapporti B to B**

- **ai trattamenti di dati personali:**

a) **effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale;**

b) **effettuati da una persona fisica per attività di carattere esclusivamente personale o domestico →es. uso social network, attività on line (se scelgo di limitare l'accesso a contati scelti rientro nella deroga, diversamente se scelgo di non limitare l'accesso sono fuori dalla deroga).**

c) **effettuati da autorità di pubblica sicurezza ovvero dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse;**

d) **effettuati dagli Stati membri nell'esercizio di attività che riguardano i settori di politica estera e sicurezza dell'Unione (c.16);**

- **ai dati anonimi**

Ambito di applicazione territoriale

Il Regolamento si applica:

1. al trattamento di dati personali effettuato da un Titolare/Responsabile stabilito nell'UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'UE;
2. al trattamento di dati personali effettuato da Titolari/Responsabili non stabiliti nell'UE, se il trattamento ha ad oggetto dati personali di interessati che si trovano nell'UE e riguarda i) l'offerta di beni o la prestazione di servizi (anche non a pagamento) ai suddetti interessati oppure ii) il monitoraggio del loro comportamento nel territorio dell'UE;
3. al trattamento effettuato da un Titolare stabilito in uno Stato extra UE, soggetto al diritto di uno Stato UE in virtù del diritto internazionale pubblico →ad. es. navi, aeromobili, ambasciate, consolati nei quali si applica la legge dello Stato membro in virtù del diritto internazionale pubblico.

Nozioni di base: definizioni

- **«dato personale»** (art. 4.1): *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.*

DEFINIZIONE AMPIA

- ✓ nome, dati anagrafici
- ✓dati relativi all'ubicazione
- ✓numero di identificazione
- ✓identificativo on line
- ✓stato di salute, abitudini
- ✓immagine, voce
- ✓dati oggettivi o di origine soggettiva

Nozioni di base

Non si parla più di «dati sensibili» ma di «categorie particolari di dati personali» ovvero ***dati personali che rivelino l'origine etnica o razziale, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all' orientamento sessuale della persona.***

Nozioni di base : altre definizioni di dati personali

art. 4.13 - dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

art. 4.14 - dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

art. 4.15 - dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Nozioni di base: definizione di trattamento

Art. 4.2 «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto, l'interconnessione, la limitazione, la cancellazione o la distruzione».

Non tutti i trattamenti sono uguali → **PROFILAZIONE** (art. 4.4):

«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».

Nozioni di base: definizione di consenso

Art. 4.11

« qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo steso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano sono oggetto di trattamento».

La forma del consenso

Principi applicabili al trattamento dei dati

Paragrafo 1, articolo 5 – I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (idoneità dell'informativa per contenuto e modalità con cui viene resa - cfr. artt. 12, 13 e 14);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (le finalità di archiviazione nel pubblico interesse e quelle di ricerca scientifica o storica non sono considerate incompatibili con quelle iniziali - cfr. art 89)
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 (i dati inesatti devono essere rettificati o cancellati);

Principi applicabili al trattamento dei dati

e) conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono essere conservati per tempi più lunghi);

f) trattati in modo da garantire un'adeguata sicurezza, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Paragrafo 2 – Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (principio di responsabilizzazione o accountability)

La liceità del trattamento – art. 6

Il trattamento dei dati personali 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 per una o più specifiche finalità;

b) il trattamento è necessario per l'adempimento di obblighi contrattuali;

c) il trattamento è necessario per la salvaguardia degli interessi vitali della persona interessata o di terzi;

d) il trattamento è necessario per adempiere obblighi di legge cui è soggetto il titolare;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o esercizio di pubblici poteri;

f) il trattamento è necessario per il perseguimento dell' interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Novità del Regolamento

NUOVI PRINCIPI GENERALI

Principio di *accountability* (responsabilizzazione)

Principio privacy *by design* e *by default*

NUOVI DIRITTI DEGLI INTERESSATI

Diritto alla portabilità dei dati, diritto all'oblio, diritto di accesso

NUOVE FIGURE PROFESSIONALI

DPO (Data Protection officer) o RPD (Responsabile della protezione dei dati)

NUOVI ADEMPIMENTI

Registro dei trattamenti

Valutazione di impatto sulla protezione dei dati (DPIA)

NUOVE SANZIONI AMMINISTRATIVE

Il principio di accountability

Art. 24 Responsabilità del titolare del trattamento:

«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 titolale 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 ed aggiornate qualora necessario».

Il principio di accountability

Cambio di prospettiva → dal «one-size-fits-all» al «risk based approach»:

- **Il Regolamento UE 679/2016 rovescia la prospettiva della disciplina in materia di protezione dei dati personali in quanto tutto il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del titolare del trattamento.**

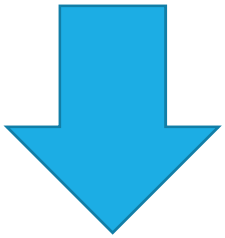
- **Il titolare, quale soggetto che determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza, ha maggiore discrezionalità nel decidere come conformarsi al GDPR, ma ha l'onere di dimostrare le ragion a supporto di tali decisioni e le motivazioni per cui si ritiene che le medesime siano *compliant* con il GDPR.**

Privacy by design e privacy by default

Privacy by design e privacy by default

Privacy by design= garantire la protezione del dati fin dalla progettazione→ significa ridurre al minimo il trattamento dei dati mediante misure tecniche ed organizzative; riguarda tutti i processi aziendali che hanno un impatto sul trattamento di dati

Privacy by default= protezione dei dati per impostazione predefinita



Art. 25 GDPR

Privacy by design e privacy by default

Cosa deve fare il titolare sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso?

- adottare misure tecniche ed organizzative;
- adottare procedure adeguate;
- adottare meccanismi predefiniti per garantire che, di *default* (art. 25, par. 2):
  - ✓siano trattati solo i dati necessari per ciascuna finalità di trattamento → minimizzazione, pseudonimizzazione;
  - ✓non siano accessibili ad un numero indeterminato di persone;
  - ✓siano conservati non oltre il tempo necessario;
  - ✓tale obbligo vale per la quantità dei dati personali raccolti e per la portata del trattamento.

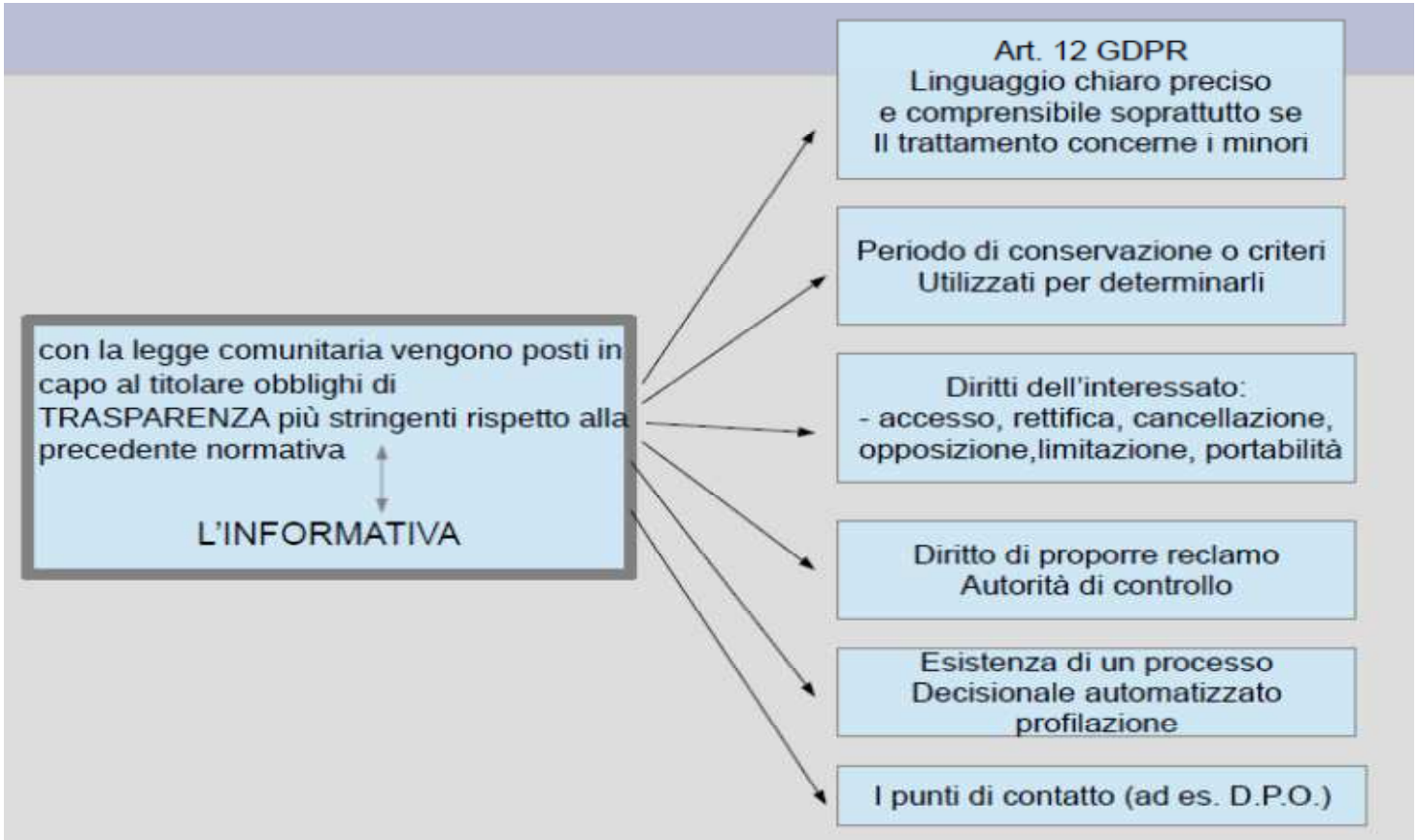
Privacy by design e privacy by default

Esemplificazione:

- per conservare le pratiche, un conto è adibire un armadio senza ante e metterlo in una sala riunioni/sala d'attesa ove inevitabilmente chi rivolge lo sguardo incontra inevitabilmente i dati raccolti nelle pratiche; un altro è adibire un armadio con ante chiuse a chiave in un luogo accessibile solo a soggetti prefiniti (archiviazione *ad hoc*).
- nella gestione di una pratica un conto è assegnare il singolo caso ad un dipendente nominativamente autorizzato, il quale ogni volta che apre il fascicolo deve annotare la data di consultazione, la ragione di accesso ed al termine deve ripristinare l'integrità del fascicolo, così da rendere riconoscibile ogni accesso.

progettazione sin dall'inizio e la progettazione come opzione predeterminata= scelta obbligata del titolare

I diritti degli interessati



L’informativa

- **COS’E’**

➢ **dichiarazione del Titolare all’interessato**

- **SCOPO**

➢ **mettere in grado l’interessato di conoscere le intenzioni del Titolare;**

➢ **consentire all’interessato di valutare le conseguenze del trattamento;**

➢ **consentire all’interessato di rifiutare o accettare il trattamento;**

➢ **consentire all’interessato di controllare il seguito dei suoi dati.**

L'informativa

- L'informativa privacy da rilasciare all'interessato è «rafforzata» ovvero prevede informazioni aggiuntive rispetto a quanto previsto dal Codice privacy (art. 13), deve essere fornita in modo conciso, trasparente e facilmente accessibile, con linguaggio semplice e chiaro.
- L'informativa va resa per iscritto o con altri mezzi anche elettronici; anche oralmente purché sia richiesto dall'interessato e sia comprovata da altri mezzi di identità dell'interessato.
- Le informazioni possono essere fornite anche con icone standardizzate per dare, in modo facilmente visibile e chiaramente leggibile, un quadro di insieme del trattamento previsto.

L'informativa

L'informativa deve contenere (art. 13):

- i dati di contatto e l'identità del titolare del trattamento e, ove applicabile, del DPO;
- le finalità del trattamento, ovvero la base giuridica del trattamento;
- qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti;
- l'ambito di trasferimento all'estero, ove applicabile;
- i destinatari o le eventuali categorie di destinatari dei dati personali;
- Il periodo di conservazione dei dati personali o i criteri utilizzati per determinare tale periodo;
- l'esistenza dei diritto di accesso ai dati dell'interessato;

L’informativa

- l’esistenza del diritto di revocare il consenso in qualsiasi momento;
- il diritto di cancellazione dei dati, della limitazione del trattamento e del diritto di opporsi al trattamento;
- il diritto di proporre reclamo al Garante della protezione dei dati personali;
- l’eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione;
- la fonte da cui hanno origine i dati personali;
- le categorie di dati personali oggetto del trattamento.

Il consenso

- **COS'E'**
  - *è la condizione necessaria per potere trattare i dati in modo lecito, in assenza di una delle altre condizioni previste dalla legge (es. esecuzione di un contratto, obbligo di legge, etc.);*
  - *deve essere richiesto in chiusura dell'informativa;*
  - *è la risposta dell'interessato all'informativa.*
- **SCOPO**
  - *Autorizzare o negare l'uso dei dati*
- **CONDIZIONI DI VALIDITA'**
  - INFORMATO, *invalido se non preceduto da informativa;*
  - SPECIFICO, *richiesto in modo chiaro e distinguibile dal resto;*
  - LIBERO, *svincolato da costrizioni* es. l'esecuzione del contratto non deve essere subordinata al rilascio del consenso per l'invio di pubblicità;
  - CONSAPEVOLE ED INEQUIVOCABILE, basato su dichiarazione o azione positiva – no caselle pre-barrate

Il consenso

- **PLURALITA' DEI CONSENSI**
  - **Diritto di esprimere il consenso per una o più finalità**
  - **Esempi di finalità aggiuntive:**
    - ✓ ***Profilazione;***
    - ✓ ***Invio di pubblicità non richiesta;***
    - ✓ ***Comunicazione a soggetti terzi diversi dal Titolare/Responsabile;***
    - ✓ ***Trasferimenti del dati in Paesi extra-UE.***
- **GRANULARITA'**
  - **Richiesta del consenso distinto e separato per ciascuna finalità;**
  - **Visibilità dei consensi e delle revoche.**

I soggetti del trattamento

I RUOLI e LE RESPONSABILITÀ nel Regolamento UE:

Con il Regolamento UE viene in parte ridisegnato l'organigramma privacy, con l'introduzione di nuove figure soggettive e l'attribuzione di nuovi compiti e responsabilità:

- **Titolare del trattamento** (*data controller*) (art 4 punto 7): 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (ved. Artt. 24 e ss) ;
- **Contitolare** (*joint controller*) (art. 26);
- **Responsabile del trattamento** (*data processor*) (art. 4 punto 8): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento (ved. art 28);
- **Sub-responsabile** (*subprocessor*) (vd. Art. 28) ;
- **Responsabile della protezione dei dati** o *Data Protection Officer* (**DPO**) (artt. 37 e seguenti).

I soggetti del trattamento

E i vecchi incaricati *ex* D.lgs. 196/2003?

«*il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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*» (art. 29)

i titolari ed i responsabili del trattamento hanno l'obbligo di formazione e istruzione nei confronti dei soggetti (persone fisiche) che trattano dati personali (denominati anche quali «*persone autorizzate al trattamento*» ovvero «personale che partecipa ai trattamenti – indirettamente si riprende la figura degli incaricati».

→*problema delle vecchie nomine, cosa fare*?

→*importanza della formazione*

L'outsourcing

COS'E'

- **esternalizzazione di un'attività da parte dell'azienda ad un soggetto esterno;**
- **attività che comporta il trattamento dei dati personali, viene svolta dal soggetto esterno «per conto» di un altro soggetto → mappatura nel registro dei trattamenti**

Ad. es.:

-predisposizione cedolini paga → consulente del lavoro;

-call center;

- gestione del sistema informatico;

-gestione eventi

L'outsourcing

Cosa prevede il GDPR in caso di *outsourcing?*

- **chi svolge attività «per conto di.....» è obbligatoriamente responsabile del trattamento → persona fisica o persona giuridica;**
- **Art. 28 GDPR → al responsabile devono essere assegnati i compiti;**
- **l'azienda che commissiona il servizio è titolare del trattamento;**
- **la società esterna che svolge l'attività «per conto dell'azienda» è responsabile del trattamento → deve presentare adeguate garanzie rispetto al GDPR → culpa in eligendo del Titolare;**
- **il dipendente della società terza ha il ruolo di incaricato/autorizzato (dalla società esterna – responsabile del trattamento);**

L'outsourcing

Necessità di un contratto scritto che disciplini la relazione tra i due soggetti:

- **il contratto deve disciplinare la materia esternalizzata, la durata, la natura e la finalità del trattamento, il tipo di dati, le categorie di interessati, gli obblighi e i diritti del Titolare;**
- **il Responsabile deve:**

-trattare i dati solo su istruzioni documentate del Titolare;

- adottare misure di sicurezza adeguate;

- garantire che gli autorizzati siano obbligati al rispetto della privacy;

- divieto di sub-appalto senza accordo preventivo con il Titolare;

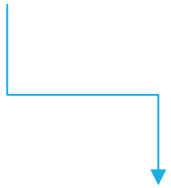
- cancellare i dati o restituirli al Titolare alla fine del servizio;

-consentire attività di verifica, controllo e ispezione del Titolare;

-informare il Titolare dei casi di violazione della privacy.

L'outsourcing

Ad es. un consulente del lavoro esterno si occupa della elaborazione dei cedolini paga dei dipendenti dello studio professionale / la dichiarazione dei redditi viene memorizzata e conservata su un server esterno allo studio, di proprietà del fornitore del software



- nell'informativa all'interessato deve essere specificato che i dati trattati sono trasmessi a tali soggetti;
- il contratto/atto giuridico tra titolare e responsabile deve indicare le misure di sicurezza adottate per garantire l'integrità dei dati, il loro corretto trattamento e la loro corretta conservazione, *ex* art. 32;
- tali soggetti devono essere menzionati nel registro dei trattamenti.

Data Protection Officer (DPO) o RPD Responsabile della protezione dei dati

Nozione:

- **si tratta di una nuova figura professionale introdotta dal GDPR;**
- **svolge un ruolo misto di vigilanza dei processi interni, di consulenza per il titolare/responsabile del trattamento dei dati, di contatto rispetto agli interessati/Autorità garante;**
- **è una figura apicale, collocato diversa per ruolo e funzioni dal responsabile del trattamento → *analogie con Odv ex 231/01***
- **il DPO può essere un dipendente del preponente (titolare o responsabile) o un soggetto esterno, vincolato in tal caso da un contratto di servizi (art. 37 co. 6);**
- **deve essere tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati dal titolare/responsabile**

Data Protection Officer (DPO) o RPD Responsabile della protezione dei dati

Designazione

- deve essere nominato dal titolare o dal responsabile a seconda delle necessità → obbligo di pubblicazione dei dati (info che consentono di raggiungere facilmente il DPO, come indirizzo posta elettronica, numero telefonico dedicato, o predisposizione canali ulteriori come modulo specifico pubblicato sul sito);
- Il DPO deve essere designato sulla base delle qualità professionali, della conoscenza specialistica della normativa in materia di protezione dei dati e dalla capacità di assolvere i compiti di cui all'art. 39;
- i dati di contatto del DPO devono essere comunicati al Garante per la protezione dei dati e resi pubblici → grande ritardo nelle comunicazioni, poche nomine di DPO;
- può essere nominato da gruppi di imprese (art. 37, co. 2)
- più autorità pubbliche/organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione, evitando ovviamente le situazioni di conflitto di interesse (es. più comuni di piccole dimensioni possono nominare un unico DPO, al fine di contenere i costi; nella prima versione del GDPR era previsto il DPO sono nelle imprese con più di 250 dipendenti).

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

La designazione del DPO è obbligatoria (da parte del Titolare/Responsabile) solo se (art. 37, co. 1):

a) il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

Presupposti di obbligatorietà della designazione:

a) **attività principali** (c. 97): «*nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*» = le operazioni essenziali che sono necessarie al raggiungimento degli obbiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte le attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare/responsabile (WP29).

→ es. il trattamento di dati relativi alla salute (cartelle cliniche) è da ritenersi una delle attività principali ospedali, case di cura, laboratori di analisi → obbligo designazione DPO

→tutti gli organismi (pubblici/privati) svolgono tra le varie attività la retribuzione del personale→ funzione di supporto ai fini dello svolgimento dell'attività principale ma pur essendo necessaria è considerata attività accessoria e non annoverata tra le attività principali.

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

b) Per il WP29 per stabilire se un trattamento è su *larga scala* occorre tener conto dei seguenti fattori:

- **numero dei soggetti interessati dal trattamento, in termini assoluti o 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.**

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

TRATTAMENTO SU LARGA SCALA

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

-trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (ad.es. il loro tracciamento attraverso titoli di viaggio);

-trattamento di dati relativi alla clientela da parte di una banca o di una compagnia assicurativa nell'ambito delle ordinarie attività;

-trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

-trattamento di dati da parte di fornitori di servizi telefonici o telamatici.

TRATTAMENTO NON SU LARGA SCALA

-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 professionista

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

c) monitoraggio regolare e sistematico → il concetto non trova definizione

Per il WP l'aggettivo «*regolare*» ha almeno uno dei seguenti significati:

-che avviene in modo continuo ovvero a intervalli definiti per un arco temporale definito;
-ricorrente o ripetuto ad intervalli costanti;
-che avviene in modo costante o a intervalli periodici.

Per il WP l'aggettivo «*sistematico*» ha almeno uno dei seguenti significati:

-che avviene per sistema;
-predeterminato, organizzato o metodico;
-che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
-svolto nell'ambito di una strategia.

Data Protection Officer (DPO) o RPD Responsabile della protezione dei dati

Esempi di monitoraggio regolare e sistematico:

-monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;

-tracciamento dell'ubicazione, per es. da parte di app su dispositivi mobili;

-programmi di fidelizzazione;

-pubblicità comportamentale;

-utilizzo di telecamere a circuito chiuso;

-attività di marketing basate sull'analisi dei dati raccolti;

-profilazione e scoring per finalità di valutazione del rischio (es. a fini di valutazione del rischio creditizio, definizione di premi assicurativi, prevenzione delle frodi o accertamento di forme di riciclaggio);

Data Protection Officer (DPO) o (RPD) Responsabile della protezione dei dati

Il DPO:

-deve essere autonomo ed indipendente (c.97) «*i responsabili della protezione dei dati dovrebbero adempiere alle funzioni ed ai compiti loro incombenti in modo indipendente»;*

- non deve ricevere dal Titolare/Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare per l'adempimento dei propri compiti;

-deve avere le risorse necessarie per assolvere ai suoi compiti, accedere ai dati personali ed ai trattamenti, aggiornare le proprie competenze →*DPO come funzione →valutare se una sola persona è sufficiente in base alla complessità organizzativa;*

-riferisce direttamente al vertice gerarchico;

-può svolgere altri incarichi purché non in conflitto di interessi (potenziale con ruoli manageriali come responsabile IT, direzione risorse umane, direzione marketing, responsabile finanziario ed operativo ma anche posizioni inferiori= valutazione caso per caso);

-può essere contattato direttamente dagli interessati→ *necessità di una adeguata comunicazione esterna circa le modalità per raggiungere il DPO (es. spazio sul sito aziendale)*

Data Protection Officer (DPO) o (RPD) Responsabile della protezione dei dati

Il Regolamento individua il nucleo minimo di compiti assegnati al DPO (art. 39):

- informare e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati nonché delle politiche in materia del Titolare o del Responsabile del trattamento, incluso il riparto di responsabilità e la formazione del personale;
- fornire, se richiesto, pareri sulla DPIA e sorvegliarne lo svolgimento;
- cooperare con l'Autorità di controllo;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento= è interlocutore privilegiato

Data Protection Officer (DPO) o RPD
Responsabile della protezione dei dati

Responsabilità del DPO

il DPO non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare/responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, pertanto un'eventuale responsabilità in merito ad un trattamento illegittimo ricadrà sul titolare/responsabile del trattamento.

MA

responsabilità contrattuale del DPO nei confronti della società

Data Protection Officer (DPO) o RPD Responsabile della protezione dei dati

In linea generale il singolo commercialista non è obbligato a nominare un DPO poiché il Garante non ritiene obbligatoria la nomina del DPO "*in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale*» → tale nomina "*in ogni caso, resta comunque raccomandata, anche alla luce del principio di accountability che permea il Regolamento*"

si suggerisce in ogni caso di indicare per ciascuno studio professionale almeno un "Referente GDPR" al quale fare riferimento (c.d. "punto di contatto") sia ai fini di eventuali verifiche e controlli sia al fine di consentire un migliore e agevole esercizio dei diritti degli interessati.

Il registro dei trattamenti

Art. 30 GDPR → deve redigerlo titolare/responsabile del trattamento – in forma scritta o elettronica (→ *non deve essere modificabile)*

deve contenere tutti i trattamenti di dati personali realizzati e deve essere aggiornato nel tempo

rappresenta l'elemento fondamentale in relazione all'obbligo di elaborare un sistema di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, redatti per soddisfare i requisiti di conformità al GDPR (*accountability)* – sarà uno dei documenti che verranno richiesti dalla Gdf in caso di controllo

Il registro dei trattamenti

REGISTRO DEL TITOLARE

a) nome e dati di contatto titolare, contitolare, rappresentante del titolare, DPO;

b) finalità del trattamento;

c) categorie interessati e categorie dati personali;

d) categorie di destinatari a cui i dati personali sono stati o saranno comunicati → *flussi interni ed esterni*

e) ove applicabile i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

f) ove possibile, i termini ultimi per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

REGISTRO DEL RESPONSABILE

a) nome e dati di contatto responsabile, del titolare per cui egli agisce, rappresentante del titolare/rappresentane, DPO;

b) categorie di trattamenti effettuati per conto del titolare;

c) categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

Il registro dei trattamenti

- **Imprese o organizzazione con numero di dipendenti pari o superiore a 250: obbligo di redazione del registro (anche in formato elettronico) del Titolare/Responsabile del trattamento e deve essere esibito su richiesta dell'Autorità;**

- **Imprese o organizzazione con numero di dipendenti inferiori a 250: obbligo di redazione se il trattamento da esse svolto**

(i) **può presentare un rischio per i diritti e le libertà dell'interessato;**

(ii) **non è occasionale;**

(iii) **include il trattamento di categorie di dati particolari o dati personali giudiziari**

il commercialista non è obbligato a tenere il registro *ma*.....

Il registro dei trattamenti

Il registro dei trattamenti ha una doppia funzione:

1. **Strumento operativo che consente di:**

- **censire le banche dati e i trattamenti in essere;**
- **rappresentare l'organizzazione sotto il profilo delle attività di trattamento ai fini di informazione, consapevolezza e condivisione interna;**
- **costruire lo strumento di pianificazione e controllo delle attività di trattamento dei dati personali in modo da garantire la loro integrità, riservatezza e disponibilità,**
- **ridurre i rischi di eventuali trattamenti illeciti.**

2. Il registro consente di conservare in maniera ordinata e verificabile da terzi, le informazioni relative all'adozione di misure tecniche ed organizzative adeguate ed efficaci, finalizzate all'attuazione del principio di responsabilizzazione.

Il registro dei trattamenti

Guida del Garante per la protezione dei dati personali all'applicazione del GDPR (luglio 2017)

- **La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. *Per tale motivo si invitano* i titolari e i responsabili del trattamento, a prescindere dalle dimensioni dell'azienda, a compiere passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'adeguata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.**

= il registro è un atto fondamentale per il rispetto del principio di *accountability* ed è il primo documento da esibire (*disclosure)* in caso di controllo → *ne deriva che il commercialista deve predisporre il registro delle attività di trattamento*

Il registro dei trattamenti

Quali erano i contenuti del «vecchio» DPS (Documento programmatico sulla sicurezza)?

Il punto 19 dell'Allegato B del Codice privacy prevedeva che, entro il 31 marzo di ogni anno, ogni titolare di un trattamento di dati sensibili o dati giudiziari, dovesse redigere il DPS, contenente informazioni riguardo:

1. **elenco dei trattamenti di dati personali;**
2. **la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;**
3. **l'analisi dei rischi che incombono sui dati;**
4. **le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;**
5. **la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito alla distruzione o danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;**
6. **la previsione di interventi formativi degli incaricati del trattamento (…);**
7. **la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare;**
8. **per i dati personali idonei a rivelare lo stato di salute e la vita sessuale….l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati da altri dati personali dell'interessato.**

Il registro dei trattamenti

Aggiornamento del registro dei trattamenti?

- **a differenza di quanto prevedeva il Codice privacy per il DPS, il GDPR non prevede una data e un obbligo espresso di aggiornamento del registro delle attività di trattamento**

→ *cosa fare? Bisogna aggiornare periodicamente il registro?* Si!

Principio di accountability: il titolare deve non solo garantire che i trattamenti che effettua siano conformi al GDPR, ma anche essere in grado di dimostrarlo!!!!!

Il registro dei trattamenti

Ambito Finalità	Categorie di interessati	Categoria di dati personali	Categoria destinatari	Modalità trattamento	Liceità del trattamento	Misure di sicurezza	Comunicaz. All'interno	Comunicazione all'esterno (indicare se paese terzo o organizzazione	Luogo custodia File	Luogo di custodia cartaceo	Tempi di conservazione/termini ultimi per la cancellazione	Cessazione trattamento (Come avviene)

Data breach (1/5)

Art. 34 «Comunicazione di una violazione dei dati personali all'interessato»

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo, e ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (se oltre le 72 ore la notifica deve contenere i motivi del ritardo).

Per «violazione di dati» si intende 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

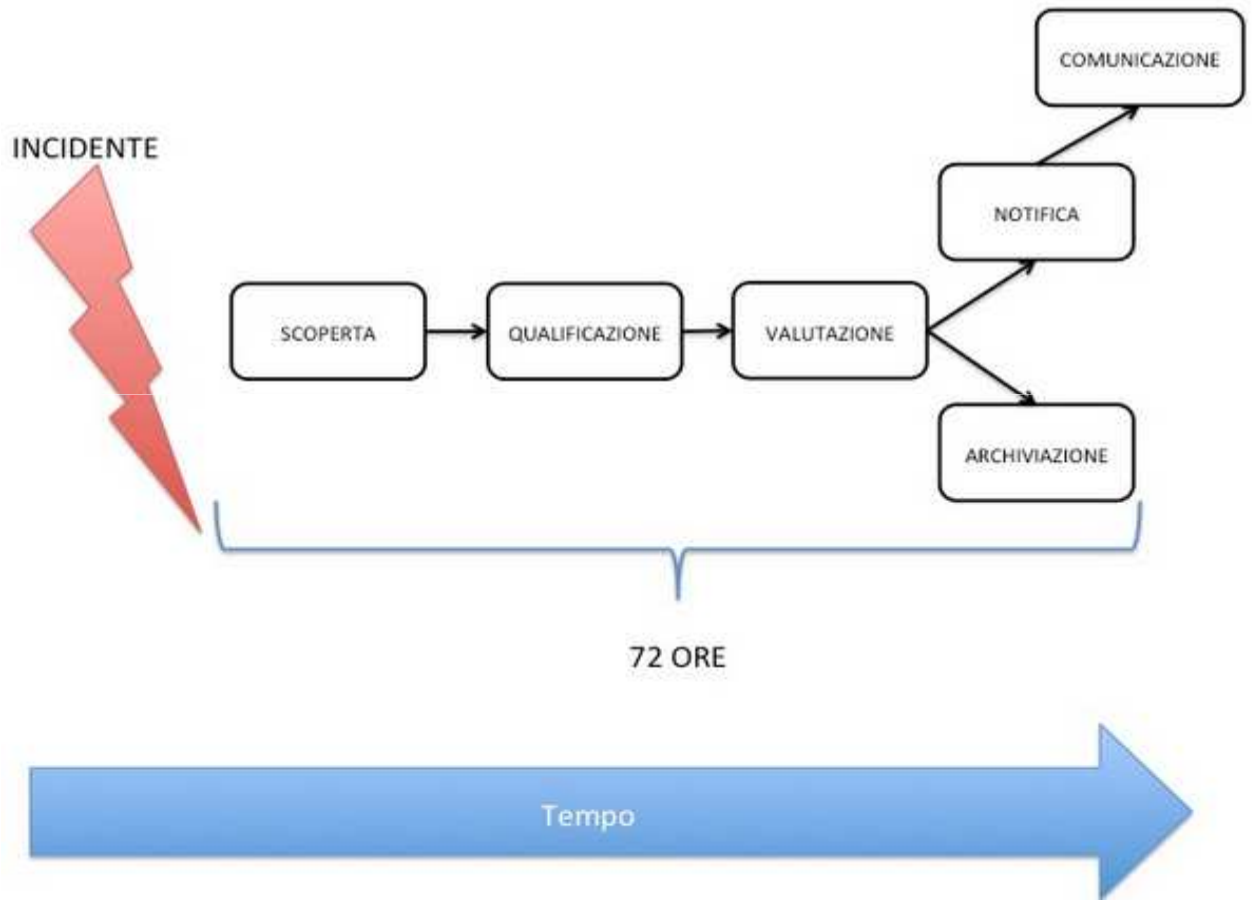
Data breach

Dato che l'obbligo di notifica **spetta al titolare**, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda **idonee clausole contrattuali** (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente **il dovere** per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

Scoprire l'incidente non è sufficiente, il titolare deve essere **in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati**.

Data breach


INCIDENTE
SCOPERTA
QUALIFICAZIONE
VALUTAZIONE
NOTIFICA
COMUNICAZIONE
ARCHIVIAZIONE
72 ORE
Tempo

Le sanzioni amministrative

A) sanzioni amministrative pecuniarie fino a 10.000.000€, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione degli obblighi aventi ad oggetto (art. 83, par. 4):

-consenso dei minori (art.8)
-trattamenti senza l'identificazione degli interessati (art.11);
-privacy by design/privacy by default (art. 25);
-contitolarità del trattamento (art. 26);
-nomina del rappresentante del titolare (art. 27);
-responsabili del trattamento (art. 28);
-istruzioni ed autorità del titolare (art. 29);
-registri del trattamento (art. 30);
-coooperazione con l'autorità di vigilanza (art. 31);
-sicurezza del trattamento (art. 32);
-notificazione del data breach all'Autorità e agli interessati (artt. 33,34);
-DPIA (art. 35);
-designazione, posizione, compiti DPO (artt. 37,38,39);
-codici di condotta e processi di certificazione (artt. 41,42,43)

Le sanzioni amministrative

B) sanzioni amministrative pecuniarie fino a 20.000.000€, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione degli obblighi aventi ad oggetto (art. 83, par. 5):

-principi applicabili al trattamento (art.5);

-liceità del trattamento (art. 6);

-condizioni per il consenso (art. 7);

-trattamento di categorie particolari di dati (art.8);

-tutti i diritti degli interessati (artt. 12- 22);

-trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale (artt. 44-49);

-qualsiasi violazione riguardante il capitolo IX avente ad oggetto «disposizioni relative a specifiche situazioni di trattamento»;

-l'inosservanza degli ordini impartiti dall'autorità di controllo derivante dai poteri in capo ad esso (art. 58par. 1 e 2)

Cosa deve fare il professionista per adeguarsi alla nuova normativa?

Sistema di gestione Data Protection:

L'organizzazione cambia → il sistema aziendale *data protection* si basa su 4 pilastri

1. **supervisione del sistema da parte di uno specifico organo indipendente (DPO), nei casi obbligatori o sulla base di una scelta volontaria;**
2. **tenuta della documentazione di sistema (= art. 30 registro dei trattamento);**
3. **progettualità e struttura del modello connotato dal rispetto del principio di *accountability* (art. 24), approccio basato sul rischio, adozione di misure tecnico-organizzative specifiche per la conformità e per la sicurezza (art. 32), effettuazione di valutazioni di adeguatezza tra cui la DPIA (art. 35);**
4. **modello organizzativo *data protection* caratterizzato da attribuzione di compiti e responsabilità; rapporti con parti terze.**

Cosa deve fare il professionista per adeguarsi alla nuova normativa?

1. **analizzare il GDPR ed individuare l'impatto sul proprio studio professionale= il GDPR deve essere applicato in base alla realtà dello studio** → *risk base approach = check up*
2. **esaminare le procedure di trattamento di dati eventualmente vigenti;**
3. **esaminare quali tipologie di dati vengono trattati:**

a) **dati dei propri dipendenti per l'esecuzione del rapporto di lavoro (busta paga può contenere categorie particolari di dati);**

b) **dati relativi ai propri clienti**

c) **dati relativi a società** → GDPR non si applica a rapporti B to B

Cosa deve fare il professionista per adeguarsi alla nuova normativa?

4. esaminare i flussi di dati (*a chi trasmetto il dato*? es. agenzia delle entrate);

5. preparare una lista di azioni di intervento;

6. sviluppare un piano di formazione interno;

7. approvare il piano di azione;

8. attuare il piano di azione;

9. garantire la conformità;

10. aggiornamento costante della documentazione in caso di variazioni dei soggetti (incaricato, responsabile, etc), degli strumenti informatici e/o del software.

I principali adempimenti per il professionista

a) **verificare le informative rilasciate ai dipendenti ai fini degli obblighi derivanti dal rapporto di lavoro → informativa chiara e precisa con indicazione, ad es., del soggetto che si occupa della elaborazione della busta paga;**

b) **revisione delle informative rilasciate ai clienti** → specificare a chi sono trasmessi i dati es. Agenzia delle entrate

c) **verificare le lettere di incarico → sono indicati i dati a cui hanno accesso gli incaricati? le designazioni degli incaricati del trattamento sono ancora attuali? sono state fornite agli incaricati istruzioni scritte sulle modalità di trattamento dei dati? è stata fatta la formazione agli incaricati?**

d) **procedere alle nomine dei responsabili del trattamento es. consulente del lavoro che elabora le buste paghe dei dipendenti/ software house;**

e) **cautela nel trattamento dei dati particolari;**

I principali adempimenti per il professionista

e) rivedere tutti i contratti di *outsourcing* → *specificare che il trattamento avviene nel rispetto delle norme di cui al GDPR, con l'adozione di misure di sicurezza idonee a garantire la sicurezza del trattamento medesimo;*

f) trasferire tutti i flussi mappati nel registro dei trattamenti= *tracking delle informazioni;*

g) analizzare l'archivio e verificare il rispetto dei tempi di conservazione;

h)qualora lo studio disponga di un sito internet e vengano pubblicati i dati relativi ai dipendenti e/o collaboratori, con eventuali fotografie degli stessi, deve essere fatto sottoscrivere agli interessati un apposito consenso per la pubblicazione dei dati e delle immagini;

i) adottare idonee misure di sicurezza in caso di perdita del controllo del flusso del dato e in caso di data breach

Il trattamento dei dati particolari

Dichiarazione dei redditi = ***quali dati può contenere?***

1) **dati relativi all'orientamento politico (devoluzione 2x1000);**
2) **dati relativi all'orientamento religioso (devoluzione 8x1000);**
3) **spese sanitarie anche dei familiari a carico; eventuali patologie correlate**
4) **agevolazioni fiscali per eventuali disabili;**

= categorie di dati particolari = sono dati che devono essere protetti come gli altri ma che richiedono una maggiore attenzione ed un rafforzamento della protezione poiché la loro diffusione illecita potrebbe determinare danni ingenti per gli interessati

Il trattamento dei dati particolari

- spesso tali dati vengono richiesti via mail da dipendenti e/o collaboratori o trattati solo dai medesimi = è necessario predisporre regolamento interno da sottoporre e far sottoscrivere ai propri dipendenti/collaboratori;

- specificare nel registro e nella informativa che i dati di cui al punto 1) e 2) vengono comunicati anche alla Agenzia delle entrate

Il trasferimento dei dati

Nello studio professionale vi è un flusso costante di dati che transitano nello studio verso altri clienti, verso uffici, verso database e applicativi, e sono condivisi tra colleghi ed impiegati → rischio connesso allo spostamento dei dati → possibile perdita di controllo sul dato o rischio che il soggetto che riceve il dato non garantisca lo stesso livello di protezione delle informazioni

3 aspetti che il professionista deve considerare:

1. trasparenza di tutte le procedure e *tracking* delle informazioni;
2. verificare il rapporto contrattuale che lega il professionista ai soggetti esterni che trattano il dato;
3. misure di sicurezza da adottare se si perde il controllo dei dati, soprattutto in caso di data breach.

Il trasferimento dei dati

1. l'interessato deve essere sempre informato anche del percorso dei suoi dati, che deve poter controllare, come il tempo di conservazione ed i destinatari → il *tracking* è molto difficile da effettuare nella società dei *social network* e del *cloud* per questo è di grande importanza l'informativa che viene consegnata agli interessati;

2. analisi e conseguente revisione di tutti i contratti *outsourcing* → fondamentale sapere il modo in cui tali soggetti trattano il dato e che percorsi gli stessi subiscono;

2. misure di sicurezza adeguate ed efficaci che devono essere messe in atto dal titolare del trattamento→ *accountability* → cifratura/crittografia e pseudonimizzazione sono le misure da preferire negli studi professionali, strumenti efficaci per garantire la protezione delle informazioni

La conservazione dei dati

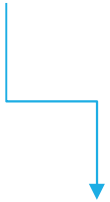
- ✓la determinazione del periodo di conservazione dei dati deve avvenire nel rispetto del principio di *limitazione della conservazione dei dati* (art. 5, par. 1, GDPR);
- ✓il termine di conservazione deve essere specificato → informativa;
- ✓la conservazione dei dati potrà estendersi ad un arco temporale non superiore a quello strettamente necessario per il raggiungimento delle finalità per cui i dati sono trattati;
- ✓onde assicurare che i dati personali non siano conservati più a lungo del necessario, il professionista dovrebbe stabilire *ex ante* un termine per la cancellazione o per la verifica periodica del rispetto del principio di limitazione.

La conservazione dei dati

- ✓è condivisibile il criterio civilistico che individua in dieci anni il periodo di conservazione dei documenti rilevanti ai fini contabili, tributari e antiriciclaggio, in conformità con quanto previsto dalle norme di riferimento anche in relazione alla decorrenza dell'obbligo;
- ✓il commercialista dovrebbe evidenziare sempre nel contratto concluso con il cliente il periodo di conservazione e, in assenza di riferimenti normativi, i criteri necessari ai fini dell'individuazione del periodo di conservazione = potrà restituire periodicamente i documenti secondo quanto concordato con il cliente (es. consegna della denuncia dei redditi o di situazioni contabili, ecc.), con espressa manleva dall'obbligo di custodia degli stessi, eventualmente previsto dal contratto.

Tenuta dei fascicoli relativi ai clienti

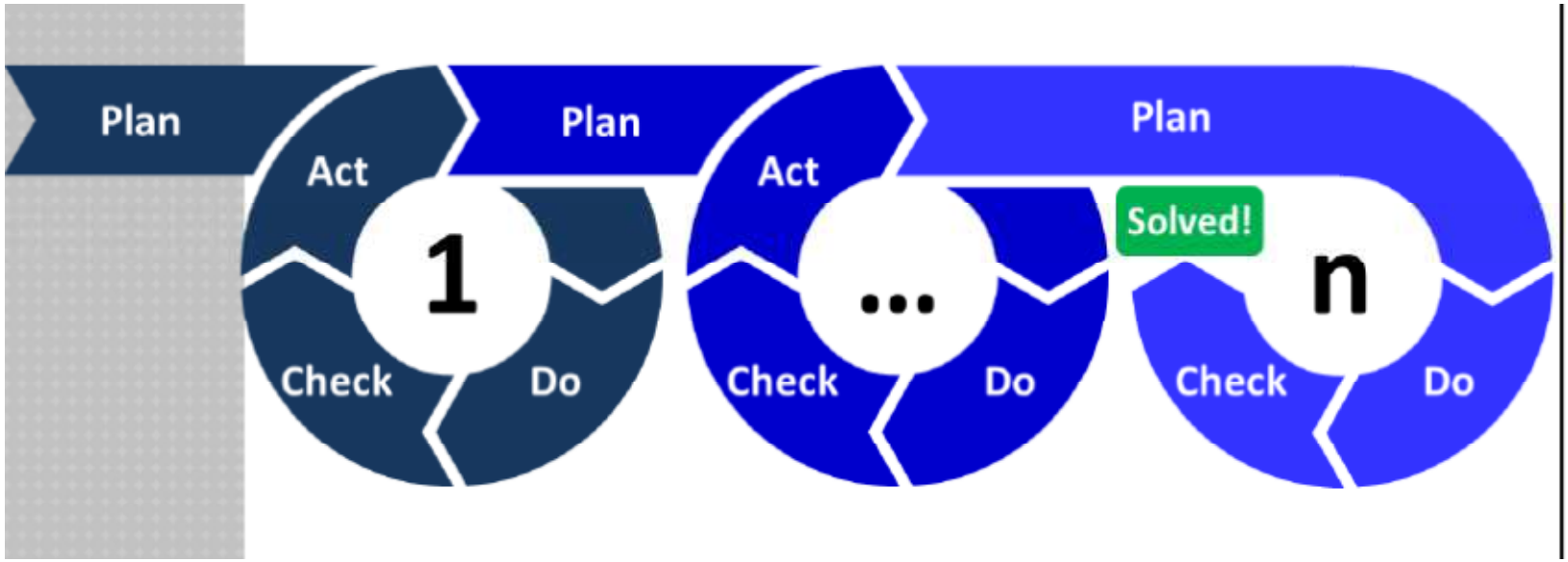
Contrariamente a quanto ritenuto nella prassi professionale, non occorre depennare, per motivi attinenti alla privacy, il nome dei clienti dalla copertina dei fascicoli cartacei, utilizzando numeri identificativi. Resta invece necessario adottare opportune modalità per rendere i fascicoli e la relativa documentazione accessibile agli autorizzati al trattamento nei casi e per le finalità previsti



Parere Garante del 3 giugno 2004 reso al Consiglio Nazionale Forense + *Considerando 15* « *non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine*».

Come prepararsi al 25 maggio?

Il ciclo PDCA



Breve check list per prepararsi al GDPR

- ✓ documento del Consiglio nazionale dei dottori commercialisti ed esperti contabili (Cndcec) e della Fondazione commercialisti (FNC) sull'applicazione del GDPR del 27 aprile 2018;
- ✓ la check list consente una auto-valutazione del proprio studio;
- ✓ la compilazione della check list non deve essere intesa come strumento sufficiente per ottenere la conformità dell'organizzazione dello studio alle disposizioni del GDPR;
- ✓ anche per gli studi professionali vige il principio di *accountability* e, pertanto, a prescindere dall'adozione delle misure suggerite dalla *checklist*, ciascun titolare del trattamento (studio) dovrà dimostrare di avere valutato con discernimento la propria posizione in termini di rischiosità e di adozione di adeguati modelli organizzativi con una strategia trasparente nei confronti degli interessati.

Breve check list per prepararsi al GDPR

« *Il Regolamento UE 2016/679 (GDPR) impone ai professionisti un cambiamento culturale nell'approccio al modello di gestione della Privacy* (…). *La normativa europea richiede infatti un ripensamento delle misure di sicurezza da adottarsi negli studi professionali, che devono essere adeguate al singolo contesto organizzativo ed elaborate caso per caso attraverso una preventiva, consapevole e responsabile mappatura dei rischi di trattamento dei dati gestiti (..)*».

→ **il nuovo modello proposto dal legislatore comunitario non è più basato su un disciplinare tecnico delle misure minime di sicurezza, essendo posta a carico del titolare dello studio professionale la responsabilità (c.d. principio di *accountability*) di definire, all'esito di un'attenta analisi dei rischi, le misure di sicurezza idonee a garantire la privacy dei dati personali trattati.**

Breve check list per prepararsi al GDPR

I 9 step per la privacy negli studi commercialisti:

1. **categorie di dati e di interessati:** il primo step da compiere secondo il Cndcec è quello di elencare le categorie di interessati e di dati raccolti e conservati, come i dati relativi al personale dell'ufficio ed in congedo, i dati relativi alla clientela;
2. **elementi del trattamento:** elencare ciascun tipo di dato all'interno di ogni categoria (nome, indirizzo, eventuali dettagli bancari, cronologia della navigazione on line) e tracciarne il flusso;
3. **fonti dei dati:** elencare la fonte dei dati personali (se sono raccolti direttamente o da parti terze);
4. **finalità del trattamento:** lo scopo del trattamento deve essere chiaro e limitato all'obiettivo dichiarato del trattamento, determinato con accuratezza (ad. es. esecuzione di un contratto, marketing, etc.);

Breve check list per prepararsi al GDPR

5. **base giuridica:** bisogna indicare la base giuridica per cui viene effettuato il trattamento (es. consenso, contratto, base legale *ex art. 6 GDPR);*

6. **categorie speciali di dati:** nel caso in cui vengano raccolti categorie particolari di dati personali occorre specificare la natura di tali dati (es. dati sanitari, dati che rivelano l'orientamento religioso o politico, dati biometrici, etc.);

7. **base giuridica dei dati speciali:** in casi di dati particolari occorre specificare la base giuridica per cui sono trattati (es. consenso esplicito);

8. **periodo di conservazione:** per ogni categoria di dati personali deve essere indicato il periodo di conservazione, in generale periodo non superiore a quello necessario per lo scopo per il quale sono raccolti;

9. **azioni richieste:** occorre identificare le azioni necessarie per garantire che le operazioni di trattamento dei dati siano conformi al GDPR, es. la cancellazione dei dati ove non vi siano più ragioni in linea con lo scopo originario per conservarlo.

Grazie per l'attenzione!

g.escurolle@studiopenalisti.it