Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

Documento

"Il regolamento Ue/2016/679 General Data Protection Regulation (GDPR): nuove regole comunitarie e precisazioni in materia di protezione dei dati personali"

Checklist di base per gli studi professionali

FNC

Aprile 2018

A CURA DEL GRUPPO DI LAVORO PRIVACY

CONSIGLIERE DELEGATO
VICEPRESIDENTE
Davide Di Russo

COMPONENTI
Paola Zambon (coordinatore)
Floriana Carlino
Gianfranco Gadda

RICERCATORE CNDCEC
Annalisa De Vivo

RICERCATORE FNC
Maria Adele Morelli

Indice

Presentazione

Il Regolamento UE 2016/679 (GDPR) impone ai professionisti un cambiamento culturale nell'approccio al modello di gestione della Privacy, che deve essere adeguatamente affrontato anche al fine di evitare l'assoggettamento a gravi sanzioni. 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. Ciò in quanto, diversamente dal passato, 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 dal Titolare stesso o dal Responsabile del trattamento.

In ciò risiede la principale criticità, ma anche la possibile opportunità insita in questo nuovo adempimento che, richiedendo un processo valutativo dinamico basato sulla *Risk Analisys* tipico dei sistemi di gestione di *Internal Auditing*, da onere per gli studi professionali può trasformarsi in una occasione per ampliare il perimetro delle attività di consulenza offerte dai Commercialisti.

L'attività di valutazione del rischio Privacy, infatti, è prima di tutto un'attività di interpretazione giuridica finalizzata a verificare che l'impianto di regole e documenti adottato sia sufficiente ad adempiere agli obblighi del GDPR in tema di dati trattati, di diritti degli interessati, di modalità di trattamento, di finalità di trattamento, di tempi di conservazione e di cancellazione, di sistemi di sicurezza, di requisiti di trasparenza. E poiché il Regolamento europeo richiede misure sufficienti, ma non fornisce indicazioni specifiche, la valutazione è una attività complessa che viene rimessa alla responsabilità del Titolare, il quale verosimilmente dovrà ricorrere all'ausilio di professionisti qualificati.

Le attività di seguito descritte rientrano a pieno titolo tra le competenze proprie delle professioni economico-giuridiche. Per tale motivo l'adeguamento alle nuove misure del GDPR, che pure costituisce l'ennesimo onere per gli studi professionali, può essere considerato al contempo quale opportunità di sviluppo per la consulenza in materia di Privacy, in relazione alla quale i Commercialisti possono porsi, da un lato, quali validi interlocutori verso le Autorità Competenti e, dall'altro, quali professionisti esperti verso la pubblica amministrazione, il mondo delle imprese e delle altre professioni.

Davide Di Russo
Vice Presidente CNDCEC

1. Inquadramento normativo

Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, emanato il 27 aprile 2016, relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (**Regolamento generale sulla protezione dei dati** – comunemente noto come *GDPR*, acronimo inglese di "*General Data Protection Regulation*").

Il regolamento troverà applicazione diretta a **partire dal 25 maggio 2018** in tutti i Paesi facenti parte dell'Unione Europea, alcuni dei quali risultano tuttora sprovvisti di un'apposita disciplina interna in materia di protezione dei dati personali. Non può dirsi lo stesso per il nostro Paese in cui, già con la legge n. 675 del 31 dicembre 1996, si era data attuazione alla Direttiva di armonizzazione 95/46/CE.

A questo primo intervento legislativo erano seguiti, principalmente, il D.P.R. 28 luglio 1999, n. 318 con il quale venivano individuate, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, e il D.Lgs. 28 dicembre 2001, n. 467, che apportava sostanziali modifiche alla disciplina in materia di privacy allora vigente.

L'intera materia è, infine, confluita nel **D.Lgs. 30 giugno 2003, n. 196 (Codice in materia dei dati personali)**, entrato in vigore il 1° gennaio 2004, che ha abrogato la disciplina previgente ed è stato, a sua volta, più volte aggiornato e modificato.

L'analisi delle fonti legislative non può, peraltro, essere considerata esaustiva, dovendo l'interprete sempre considerare i numerosi provvedimenti emanati dal Garante Italiano per la protezione dei dati personali e ovviamente il formante giurisprudenziale degli ultimi venti anni.

Nonostante la diretta applicabilità e vincolatività del *GDPR* in tutti i suoi elementi, in Italia l'art. 13 della Legge 25 ottobre 2017, n. 163 (cd. "Legge di delegazione europea 2016-2017") ha delegato il Governo ad adottare uno o più decreti legislativi, entro il 21 maggio 2018, al fine di adeguare il quadro normativo nazionale alle disposizioni ivi contenute.

Il nostro Codice in materia di trattamento dei dati personali, dunque, dovrà essere modificato in ossequio ai criteri di delega dettati dalla Legge di delegazione europea, che impongono: *i)* l'espressa abrogazione delle disposizioni del Codice incompatibili con quelle contenute nel regolamento; *ii)* la modifica del Codice stesso limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento. Più specificamente, nell'ambito delle suddette modifiche, dovrà prevedersi l'adeguamento del sistema sanzionatorio penale e amministrativo vigente alle disposizioni del GDPR, introducendo sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse; *iii)* il coordinamento delle disposizioni vigenti in materia di protezione dei dati personali con quelle recate dal regolamento (UE) 2016/679[1].

[1] È opportuno segnalare che, nel momento in cui si procede alla redazione del presente documento, il Consiglio dei Ministri ha provveduto a diffondere il seguente comunicato stampa del 21 Marzo 2018: "*Il Consiglio dei Ministri, su proposta del Presidente Paolo Gentiloni e del Ministro della giustizia Andrea Orlando, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. A far data dal 25 maggio 2018, data in cui le disposizioni di diritto europeo acquisteranno efficacia, il vigente Codice in*

La delega, inoltre, abilita il governo a prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali, nell'ambito e per le finalità previste dal regolamento.

A tale ultimo riguardo, si segnala che la recente Legge di bilancio 2018 (Legge 27 dicembre 2017, n. 205, pubblicata in G.U. n. 302 del 29.12.2017) all'art. 1, commi da 1020 a 1025, attribuisce al Garante, a tutela dei diritti fondamentali e delle libertà dei cittadini, determinati poteri di carattere regolamentare, di vigilanza e inibitori, e introduce direttamente alcune modifiche e innovazioni in materia di protezione dei dati personali, in relazione a determinati trattamenti, in vista della piena applicazione del GDPR.

Ad ogni buon conto, ad oggi i decreti legislativi delegati summenzionati non sono ancora stati emanati. Tuttavia, oltre a comportare l'abrogazione della direttiva 95/46/CE, il regolamento GDPR troverà **diretta applicazione** a partire dal 25 maggio 2018, con conseguente prevalenza sul diritto interno, eventualmente ancora vigente, che dovesse risultare incompatibile con le disposizioni previste dal regolamento medesimo.

Un primo tentativo di uniformazione della disciplina interna alle disposizioni del GDPR sembra essere stato compiuto dalla cd. *Legge europea* del 2017 (Legge 20 novembre 2017, n. 167), la quale ha modificato soltanto alcune disposizioni del Codice della privacy, in tema di responsabile del trattamento, di riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici, di conservazione dei dati relativi al traffico telefonico e telematico e di ruolo organico del personale alle dipendenze del Garante[2].

Peraltro, il Garante ha recentemente ribadito che non sono possibili proroghe rispetto alla data di piena e diretta applicazione del GDPR[3].

materia di protezione dei dai personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sarà abrogato e la nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del suddetto Regolamento 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".

[2] Nello specifico l'art. 28, recante *modifiche al Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196* ha previsto l'introduzione all'articolo 29 del codice, dopo il comma 4, del seguente: «4-bis. *Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento; i predetti atti sono adottati in conformità a schemi tipo predisposti dal Garante*» e la riscrittura del comma 5 come segue: «5. *Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4-bis*». Inoltre, il medesimo art. 28 della legge europea ha introdotto l'art. 110-*bis* (Riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici) al Codice il quale prevede: "*1. Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati. 2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza*».
Ulteriori informative sul GDPR sono reperibili, così come il testo normativo, sul sito istituzionale del Garante per la protezione dei dati personali (http://www.garanteprivacy.it/regolamentoue).

[3] Si veda il comunicato stampa dell'Autorità Garante del 19 aprile 2018 reperibile al seguente link http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8469593.

2. Ambito di applicazione materiale e territoriale del GDPR

Il regolamento GDPR eleva ad oggetto di tutela il trattamento dei soli dati personali, al fine di assicurare la protezione dei diritti e delle libertà delle persone fisiche in maniera equivalente in tutti gli Stati membri e la libera circolazione dei dati, disciplinando, conseguentemente, i principi e le condizioni per procedere al legittimo trattamento di tali dati.

Sono, pertanto, esclusi dall'ambito di applicazione delle disposizioni del regolamento i trattamenti dei dati relativi alle persone giuridiche[4]: è evidente che in tal caso le disposizioni del GDPR troveranno applicazione con riferimento al trattamento dei dati personali del rappresentante legale.

La definizione di dato personale assunta dal GDPR risulta particolarmente ampia. L'art. 4 del GDPR stabilisce che per dato personale debba intendersi "***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*".

Gli obiettivi che il regolamento persegue richiedono una sensibile estensione dell'ambito di applicazione delle sue disposizioni. In tal senso opera l'art. 2 del GDPR che, quanto all'ambito di applicazione materiale, specifica che il regolamento si applica al trattamento "*interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali [che siano] contenuti in un archivio o destinati a figurarvi*"[5].

Quanto all'ambito di applicazione territoriale, il par. 1 dell'art. 3[6] accoglie come criterio generale il cd. *principio di stabilimento*. Di conseguenza, il regolamento si applica ai trattamenti effettuati dai titolari del trattamento[7] e dai responsabili del trattamento[8] **stabiliti**[9] nel territorio dell'Unione europea, a prescindere dalla circostanza che il trattamento sia o meno ivi concretamente effettuato

[4] In particolare, il considerando 14 chiarisce: "*È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali.* ***Il presente regolamento non disciplina il trattamento dei 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*".

[5] Il regolamento non trova applicazione con riguardo ai casi indicati nel par. 2 del medesimo art. 2, in particolare quando il trattamento è effettuato: *i)* per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; *ii)* in materia di politica estera e sicurezza comune (*PESC*); *iii)* 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 stesso. È inoltre escluso dall'ambito di applicazione del regolamento il trattamento che sia effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

[6] "*Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*".

[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*".

[8] "*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che* ***tratta dati personali per conto del titolare del trattamento****".*

[9] In punto, il considerando 22 chiarisce che "*lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica*".

e a prescindere dalla nazionalità o dal luogo di residenza dei soggetti (noti in Italia come "interessati" e così definiti dal GDPR) cui si riferiscono i dati personali trattati.

Ulteriormente, il par. 2 dell'art. 3 del GDPR rende vincolanti le sue norme anche al trattamento effettuato da titolari del trattamento e responsabili del trattamento **non stabiliti** nell'Unione europea, in due casi:

a) quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi nell'Unione europea, indipendentemente dall'obbligatorietà di un pagamento da parte dell'interessato[10];

b) quando il trattamento è riferito al monitoraggio (*rectius*: controllo) del comportamento degli interessati nella misura in cui tale comportamento ha luogo all'interno dell'Unione europea[11].

La *ratio* posta alla base del GDPR, volta a consentire la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei loro dati personali, ha condotto all'adozione, nell'ambito del presente lavoro, di un approccio "*garantista*" dei diritti degli interessati. In altre parole, nell'ipotesi in cui sorga il dubbio se ad una determinata fattispecie si applichi o meno il regolamento, è preferita l'opzione positiva.

3. Principi applicabili al trattamento dei dati personali e condizioni di liceità del trattamento

Il GDPR ribadisce i principi che dovranno trovare applicazione al trattamento dei dati personali, parte dei quali risultano ben noti e definiti, in quanto già previsti sia dall'attuale Codice privacy sia dalla direttiva 95/46/CE, anche grazie alle indicazioni emerse dalla prassi e dalla giurisprudenza che nel tempo si sono occupate della materia, rafforzandone talvolta la portata (*liceità, correttezza e trasparenza del trattamento, minimizzazione, limitazione della conservazione, finalità del trattamento*).

A questi ultimi si aggiunge, tra le altre novità, l'inedito principio di "*responsabilizzazione*" o "*accountability",* in forza del quale il titolare del trattamento è tenuto a porre in essere tutte le misure tecniche e organizzative adeguate per garantire **ed essere in grado di dimostrare** che il

[10] Il considerando 23 chiarisce che è idonea a configurare un'offerta rilevante anche la mera intenzione di offrire beni o prestazioni desumibile ad esempio da "*l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione*".

[11] Rientra in tali ipotesi, come evidenziato dal considerando 24, la profilazione delle persone fisiche, che consente, in conseguenza del tipo di trattamento effettuato, di assumere decisioni che riguardano gli interessati i cui dati sono trattati ovvero di analizzarne o prevederne le preferenze, i comportanti e le posizioni personali. In punto, si rileva che la definizione di profilazione ai fini del GDPR è dettata dal n. 4, par. 1, dell'art. 4 il quale stabilisce che per profilazione si intende: "*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*".

trattamento dei dati personali degli interessati è effettuato nel rispetto dei principi dettati dall'art. 5, par. 1[12] e delle altre norme del GDPR.

Costituiscono attuazione concreta dei principi di cui al predetto art. 5, par. 1, del GDPR le disposizioni successive dedicate ai **diritti dell'interessato**, trattati dall'intero Capo III del GDPR (artt. da12 a 23).

Il GDPR conferma poi, la regola per cui, ai fini della sua liceità, ogni trattamento deve trovare fondamento in un'*idonea base giuridica* che, **oltre al consenso**, è individuata nella sussistenza delle seguenti condizioni:

a) 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;

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

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

d) 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;

e) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del medesimo 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.

Non si tratta, anche in questo caso, di condizioni di liceità del trattamento del tutto sconosciute al diritto nazionale. È, infatti, possibile cogliere traccia delle predette basi giuridiche nella disciplina dettata dal Codice della privacy, in particolare da quanto previsto nell'art. 24[13].

---

[12] L'art. 5, par.1 del GDPR rubricato "*Principi applicabili al trattamento dei dati personali*" prevede:
"*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»);
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»)".

[13] Art. 24 (*Casi nei quali può essere effettuato il trattamento senza consenso*)
1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:
a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

Ai fini che qui interessano non vi è dubbio che, a seguito dell'entrata in vigore del GDPR, assumono particolare rilievo le nuove disposizioni dedicate al consenso dell'interessato.

L'art. 4 del GDPR definisce il consenso dell'interessato come una "*qualsiasi manifestazione di volontà*[14] *libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

Come evidenziato nei primi contributi di commento al regolamento, tale definizione apre la strada alla possibilità che la dichiarazione di consenso non risulti necessariamente da una documentazione resa per iscritto, purché tale dichiarazione sia stata prestata in maniera inequivocabile.

In punto, il considerando 32 specifica che "*il consenso dovrebbe essere espresso mediante un* ***atto positivo inequivocabile*** *con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio* ***mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale (principio di libertà delle forme).*** *Potrebbe comprendere* ***la selezione di un'apposita casella in un sito web****, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.* ***Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle.*** *Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".*

---

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;
i-bis) riguarda dati contenuti nei curricula, nei casi di cui all'articolo 13, comma 5-bis;
i-ter) con esclusione della diffusione e fatto salvo quanto previsto dall'articolo 130 del presente codice, riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'articolo 2359 c.c. ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti ad essi aderenti, per le finalità amministrativo contabili, come definite all'articolo 34, comma 1-ter, e purché queste finalità siano previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa di cui all'articolo 13.

[14] Da tale definizione sembrerebbe trarre un sensibile conforto la teoria negoziale della natura giuridica del consenso.

Quanto alla **libera espressione** del consenso, il considerando 42 esclude che lo stesso possa essere ritenuto liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio. In tal senso, quindi, il regolamento si pone nel solco degli orientamenti già espressi dal Garante in tema di libera espressione del consenso[15].

Stesso dicasi in relazione al requisito relativo alla **specificità** del consenso, quale elemento già richiesto dal Codice della privacy. Il requisito della specificità è soddisfatto nel momento in cui il consenso sia applicato a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Differentemente, qualora il trattamento sia effettuato per la realizzazione di più finalità, il consenso dovrebbe essere prestato per ciascuna di esse.

Le condizioni che devono essere soddisfatte affinché la prestazione del consenso possa ritenersi legittima sono ulteriormente specificate dall'art. 7 del GDPR, il quale si riferisce a situazioni che assumono particolare interesse e sulle quali occorre, pertanto, soffermarsi.

Nello specifico la norma in esame esplicita la regola generale in base alla quale, in linea con il principio di *accountability*, il titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato - *inequivocabilmente* - il proprio consenso al trattamento dei suoi dati personali, con la conseguenza che è necessario porre particolare attenzione a tale "onere probatorio" nell'ipotesi in cui il consenso non venga acquisito per iscritto.

Qualora, al contrario, il consenso sia prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente *distinguibile* dalle altre materie, in *forma comprensibile* e facilmente *accessibile*, utilizzando un *linguaggio semplice e chiaro*. Nessuna parte di una tale dichiarazione che costituisca una violazione del GDPR è vincolante.

Quando il trattamento è basato sul consenso, l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Tuttavia, la revoca non è idonea a pregiudicare la liceità del trattamento già effettuato e basato sul consenso precedentemente prestato. Il diritto di revocare il consenso prestato deve essere indicato nell'informativa comunicata all'interessato *prima* di esprimere il consenso medesimo.

Particolare rilevanza riveste poi la regola in base alla quale "*il consenso è revocato con la stessa facilità con cui è accordato*", comportando l'obbligo di prevedere le medesime forme e/o misure tecniche per la revoca del consenso già utilizzate al momento della raccolta del medesimo.

[15] Si riporta il testo del considerando 43 che prevede: "*per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione*".

4. Formazione e consulenza in materia di privacy

Com'è noto, i professionisti iscritti all'Albo dei Dottori Commercialisti e degli Esperti Contabili possono avere maturato esperienza professionale in tema di privacy (ciascuno nel proprio ambito e grazie al proprio percorso formativo) già a partire dalla Legge 675/96, passando poi all'attuale D. Lgs. 196/03 e approfondendo anche l'analisi del GDPR.

La privacy, peraltro, rientra tra le materie oggetto della formazione professionale continua a cura degli Ordini territoriali e degli altri enti accreditati. Vi è, dunque, una moltitudine di iscritti all'Albo che da anni svolge attività di consulenza in tema di privacy, poiché ha seguito l'evolversi della norma accanto alle aziende clienti.

Attualmente non sono previsti specifici requisiti professionali e/o obblighi formativi da assolvere per i soggetti che intendano fornire consulenza in materia di privacy o assumere l'incarico di Data Protection Officer[16] (Responsabile della Protezione dei Dati, nel prosieguo anche: DPO). Bisognerà, quindi, attendere che la disciplina trovi una sua compiuta determinazione, grazie all'emanazione dei decreti delegati di cui in premessa, e che il Garante elabori eventuali ulteriori indicazioni.

Nell'attesa di tali interventi normativi, si ritiene che l'iscritto all'Albo possa proseguire la propria attività di consulenza in materia di privacy e, in forza delle specifiche competenze maturate, ricoprire, in questa fase di iniziale applicazione del GDPR, l'incarico di DPO per società ed enti. In tal caso, però, dovranno tenersi in apposita considerazione i requisiti di indipendenza prescritti dal GDPR; in particolare, dovranno essere valutate attentamente eventuali situazioni potenzialmente idonee a generare un conflitto di interesse.

Per quanto attiene ai chiarimenti intervenuti nella prassi sul punto, in una risposta ai *quesiti in materia di certificazione delle competenze ai fini della prestazione di consulenza in materia di protezione dei dati personali*[17] il Garante ha evidenziato: "*come in altri ambiti delle cosiddette "professioni non regolamentate", si vanno diffondendo schemi di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del Regolamento (UE) 2016/679), rilasciate anche all'esito della partecipazione ad attività formative e alla verifica dell'apprendimento, se possono rappresentare, al pari di altri titoli, uno strumento per valutare il possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del DPO, né, allo stato, possono sostituire in toto la valutazione della p.a. nell'analisi del possesso dei requisiti del DPO necessari per svolgere i compiti da assegnargli in conformità all'art. 39 del Regolamento (UE) 2016/679*".

[16] Si tratta, come disciplinato dall'art. 37 del GDPR, di una figura dotata di particolari qualità professionali, in specie di conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali, nonché di capacità di assolvere all'adempimento di specifici compiti, anch'essi previsti dal GDPR. Il DPO si caratterizza per la sua indipendenza ed autonomia nell'assolvimento dell'incarico ad esso affidato, ancorché possa trattarsi di un dipendente del titolare del trattamento o di un soggetto ad esso legato da un rapporto di prestazione di servizi.

[17] Documento Web n. 7057222 del 28 luglio 2017, disponibile al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7057222.

In merito, più specificatamente, alle certificazioni di cui all'art. 42 del GDPR[18] è opportuno riportare quanto previsto dal comunicato congiunto, pubblicato sul sito del Garante per la protezione dei dati personali il 18 luglio 2017 (doc. web n. 6621723), con il quale l'Autorità e ACCREDIA (l'Ente unico nazionale di accreditamento designato dal Governo italiano) - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - hanno ritenuto necessario sottolineare che «*al momento, le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679*", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione».

In tema è possibile anche citare la norma UNI 11697:2017 dal titolo "*Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza*" emanata con lo scopo di "*definire terminologia, principi, caratteristiche e requisiti relativi alla qualificazione di attività professionali e/o professioni non regolamentate e non rientranti nelle competenze di altre commissioni tecniche ed Enti Federati*". La norma in esame si riferisce ai meri requisiti di conoscenza che i soggetti non iscritti all'Albo dei Dottori Commercialisti (e più in generale non iscritti in alcun albo professionale) dovrebbero possedere per poter svolgere un'attività finalizzata a trattare con adeguata competenza la protezione dei dati personali.

[18] L'art. 42 del GDPR rubricato *Certificazione* prevede: "*1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, 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 presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.*
2. Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.
3. La certificazione è volontaria e accessibile tramite una procedura trasparente.
4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.
5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.
6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.
7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.
8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato".

5. Checklist di base per gli studi professionali

Alla luce della disciplina del GDPR accennata e, soprattutto, dell'introduzione del cd. principio di *accountability,* la capacità di proteggere i dati personali diventa basilare e si sostanzia nell'adozione di *adeguati assetti e modelli organizzativi che ne consentano la reale applicabilità*. Le sanzioni previste dal GDPR in caso di inadempimento sono molto elevate e, dunque, è necessaria un'adeguata formazione e preparazione in modo da pervenire, entro la scadenza di legge, alla conformità richiesta dalla norma.

A tal fine, il CNDCEC ritiene opportuno fornire ai propri iscritti alcune indicazioni di formazione e di informazione che possano costituire una efficace forma di auto-valutazione preventiva dei propri studi, ancorché non sufficiente, alla luce della disciplina introdotta dal GDPR.

Traendo ispirazione dal modello sassone[19] il CNDCEC ritiene utile proporre l'allegato documento "*Regolamento generale sulla protezione dei dati – check list di base per gli studi professionali*"[20] da utilizzare al fine di valutare il livello di adeguamento degli studi professionali alle nuove disposizioni del GDPR.

Pur apparendo evidente, alla luce delle disposizioni del GDPR, risulta ugualmente opportuno rimarcare che la mera compilazione della *checklist* non va intesa come strumento sufficiente per ottenere la conformità dell'organizzazione dello studio alle disposizioni del GDPR.

Anche per gli studi professionali, come per tutti i soggetti che effettuano trattamenti di dati personali, vige il principio di responsabilizzazione o *accountability* e, pertanto, a prescindere dall'adozione delle misure suggerite dalla predetta *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.

6. Indicazioni per l'utilizzo della checklist

Passando ad analizzare le indicazioni operative per l'utilizzo della checklist in allegato, deve anzitutto premettersi che la compilazione della stessa si articola nei seguenti tre passaggi:

1. ***Mappatura delle categorie di dati raccolti, trattati e conservati***

Al riguardo, si suggerisce di partire dai più importanti processi che interessano le principali attività di studio. Sulla base del tipo di consulenza svolta, infatti, si potranno detenere tipologie di dati personali diversi e trattarli secondo particolari modalità. Le informazioni catalogate andranno poi completate con la stima del periodo di conservazione di tali dati, secondo quanto specificato nel successivo paragrafo 7, termine che potrà essere diversificato a seconda delle diverse categorie di dati personali trattati (colonna 8 di pag. 2 dell'allegata checklist).

[19] Ci si riferisce, in particolare, alle indicazioni elaborate dai Garanti irlandesi e inglesi, reperite tramite i rispettivi siti istituzionali http://gdprandyou.ie/ e https://ico.org.uk/.

[20] Il progetto pilota è stato avviato già dallo scorso anno dall'Ordine dei Dottori Commercialisti ed Esperti Contabili di Torino che ha condotto anche un apposito "Tavolo congiunto GDPR" con l'Ordine degli Avvocati e degli Ingegneri di Torino.

Tale disamina dovrà essere poi estesa a tutti gli interessati e, dunque, anche al comparto fornitori e, ove presenti, ai dipendenti e tirocinanti, seguendo le stesse modalità utilizzate per la mappatura dei trattamenti riferiti ai clienti.

2. ***Compilazione (risposte «Sì» o «No»), con possibilità di commenti, ad ogni check di azioni possibili***

La *check list* proposta investe i diversi ambiti regolamentari per i quali occorre raggiungere la conformità dell'organizzazione dello studio, con singoli richiami agli articoli del regolamento che coinvolgono l'azione di monitoraggio per facilitare la verifica della maggiore o minore adeguatezza della propria organizzazione al regolamento stesso. Sul punto sono individuate le seguenti sotto-sezioni:

- Dati personali trattati (pag. 4)
- Diritti degli interessati (pagg. 5-6)
- Accuratezza e conservazione (pag. 78)
- Requisiti di trasparenza (pag. 8)
- Altri obblighi del titolare (pag. 9)
- Sicurezza del trattamento (pagg. 10-11)
- Data breaches (pag. 12)
- Trasferimento dati personali (pag. 13)

La compilazione in autovalutazione delle singole tabelle, facilitata dai richiami agli articoli del Regolamento, permette in primo luogo di individuare gli ambiti di intervento per conformarsi al regolamento stesso, andando ad analizzare tutte le misure mancanti (colonna NO), con una prima sintetica individuazione delle azioni di rimedio da porre tempestivamente in essere in ottemperanza al GDPR. Nell'ipotesi in cui determinate attività di trattamento non risultino applicabili alla struttura in esame, sarà sufficiente indicare "non applicabile" nella relativa casella e neutralizzarne conseguentemente l'impatto sulla disamina complessiva.

3. Individuazione, al termine della compilazione, delle misure relative all'adeguato trattamento dei dati non ancora attuate.

Il risultato complessivo dell'analisi, desunto dalle varie tabelle, conduce, poi, al completamento della tabella (colonna 9 di pag. 2 dell'allegata checklist) illustrata al precedente punto 1 della presente sezione; la corretta e completa compilazione della stessa può costituire una semplice base per la redazione del registro delle attività di trattamento di cui all'art. 30 del GDPR, ovviamente completo delle indicazioni ivi prescritte, di cui si dirà nel prosieguo (cfr. pag. 19 e nota 27).

In particolare, con riferimento all'attività svolta generalmente dagli studi professionali, dovrà essere prestata particolare attenzione ai seguenti elementi:

a. elencazione delle categorie di interessati e delle categorie di dati personali raccolti e conservati: tutti gli interessati vanno puntualmente censiti e raggruppati in categorie omogenee avendo cura di

uniformare, all'interno di ciascuna categoria, i dati raccolti e il relativo trattamento (cfr. check list punto 1);

b. *individuazione delle basi legittime tipiche* sulle quali è fondato il trattamento dei dati nello studio professionale (es. contratto, obbligo normativo, consenso, interesse legittimo) *e tipo di trattamento effettuato*, con particolare attenzione ai minori (cfr. check list punto 1);

c. *focus sui diritti degli interessati:* la checklist focalizza l'attenzione sui diritti riconosciuti agli interessati dal GDPR. Ci si riferisce in particolare al diritto di accesso ai dati personali, alla portabilità dei dati, al diritto di rettifica e di cancellazione, al diritto alla limitazione di trattamento, al diritto di opposizione. L'esito di tale fase di analisi dovrebbe essere utile all'elaborazione di un adeguato documento informativo comprensivo di tutte le prescrizioni di cui all'art. 13 del Regolamento, completato dalla previsione e documentazione delle adeguate misure per garantire l'esercizio di tali diritti agli interessati (cfr. check list punto 2);

d. *individuazione delle finalità del trattamento*: lo scopo del trattamento deve essere chiaro e limitato all'obiettivo dichiarato del trattamento, determinato con accuratezza, e la conservazione dei dati deve essere effettuata evitando duplicazioni inutili (cfr. check list punto 3);

e. garanzia di trasparenza verso i clienti e i dipendenti: opera *in materia di redazione di corretta informativa affinché un trattamento possa considerarsi equo (fair) e chiaro per l'interessato e in modo che non costituisca violazione ad alcun elemento ai fini del GDPR* (cfr. check list punto 4[21]);

f. adempimento degli altri obblighi del titolare: riveste un'importanza basilare nell'organizzazione degli studi, per non incorrere nelle pesanti sanzioni previste dal regolamento. Ci si riferisce principalmente alla corretta formalizzazione delle autorizzazioni al trattamento nei confronti degli incaricati al trattamento (dipendenti, *collaboratori e tirocinanti* dello studio) o di eventuali responsabili esterni del trattamento per conto del titolare, come prescritto dall'art. 29 del regolamento; analogamente, il titolare dello studio può figurare come responsabile del trattamento per conto di terzi. In questi casi, il trattamento dei dati da parte del responsabile del trattamento *è consentito* in presenza di esplicita istruzione da parte del titolare[22] (cfr. check list punto 5);

g. garanzia della sicurezza del trattamento e dimostrazione di aver posto in essere le misure idonee a tal fine: va dimostrato che, all'entrata in vigore del regolamento, il titolare/responsabile del trattamento abbia posto in essere tutte le misure di sicurezza fisiche, organizzative e tecnologiche adeguate, ovvero finalizzate a preservare sostanzialmente la sicurezza dei dati personali trattati. A titolo esemplificativo e non esaustivo, si segnalano quali misure di sicurezza dispositivi anti intrusione, allarmi , porte blindate, armadi chiusi a chiave per gli archivi cartacei, adeguati software di protezione quali antivirus e firewall, adeguata politica di utilizzo delle strumentazioni elettroniche e di tutti i dispositivi utilizzati, cambiamento periodico delle credenziali di accesso alla rete, monitoraggio degli accessi, salvataggi periodici e programmati dei dati trattati elettronicamente, valutazione dell'adozione di tecniche di pseudonimizzazione, con costante verifica e aggiornamento delle misure di sicurezza adottate. Il tutto è finalizzato a prevenire violazioni, anche accidentali, dei dati trattati (cfr. check list punto 6);

[21] L'ultimo quesito previsto dall'indicata sezione della check list va risolto non solo con riferimento ai clienti di studio ma ogni qual volta il Dottore Commercialista effettui il trattamento di dati di ulteriori interessati.
[22] Cfr. artt. 29 e 82 , co. 2 del GDPR.

h. chiara individuazione delle procedure da mettere in atto in caso di Data breaches, al fine di adempiere agli obblighi imposti dal GDPR in tali circostanze: in caso di violazione dei dati (cd. *Data breach*) il titolare del trattamento deve tempestivamente valutare se si presentino gli estremi per la comunicazione all'Autorità di controllo, da effettuarsi comunque entro le 72 ore dalla conoscenza dell'intrusione, ponendo conseguentemente in atto tutte le prescrizioni di cui all'art. 33 del regolamento. Occorre altresì valutare, in caso di rischio elevato per i diritti e le libertà delle persone fisiche, l'effettuazione della comunicazione agli interessati eventualmente coinvolti (cfr. check list punto 7)*;*

i. comunicazione del trasferimento di dati personali a titolari extra UE: i dati personali possono essere trasferiti verso Paesi dell'Unione Europea e verso Paesi terzi che rispettino il GDPR, nell'ambito delle finalità dichiarate con adeguata informativa all'interessato e con il suo consenso (cfr. check list punto 8).

Da ultimo si evidenzia che, al fine di mantenere nel tempo la conformità alle prescrizioni del GDPR, le procedure sopra illustrate devono essere costantemente monitorate e integrate in relazione all'evoluzione delle norme regolamentari e alle modifiche degli assetti organizzativi dei singoli studi.

7. Interpretazioni, esempi e casi di interesse

Si segnalano per la loro rilevanza nell'organizzazione del lavoro quotidiano di studio alcuni esempi e casi di interesse in materia di privacy.

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. Tanto si desume dalle indicazioni fornite dal Garante della privacy, con il parere del 3 giugno 2004 reso al Consiglio Nazionale Forense[23].

Utilizzo di software

Ciascuno studio professionale potrà reperire sul mercato, se lo ritiene opportuno, eventuali *tool software* per monitorare lo stato del trattamento dei dati personali che consentano, inoltre, la redazione di parte della documentazione richiesta, ai fini dell'adempimento degli obblighi derivanti dal GDPR. Nondimeno, è importante che la norma venga compresa, almeno a livello logico, da ciascun *dominus* di studio, in modo che il ricorso a consulenze specialistiche configuri un'opzione residuale.

Periodo di conservazione

[23] In punto si segnala altresì che il considerando 15, relativo all'ambito di applicazione materiale del GDPR stabilisce che: "*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*".

Quanto al periodo di conservazione dei dati, la sua determinazione deve avvenire nel rispetto del principio di *limitazione della conservazione dei dati* (art. 5, par. 1, GDPR).

Pertanto, 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. Il criterio più affidabile per la determinazione del periodo di conservazione consiste nel riferirsi alle norme di settore dell'ordinamento che impongono, direttamente o indirettamente, obblighi di conservazione in capo ai professionisti.

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.

Si ritiene 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.

In linea generale si suggerisce di 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. Così, si potrà provvedere periodicamente alla restituzione dei 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, ed evidenziando altresì al cliente i costi dell'eventuale servizio di conservazione per la durata del mandato professionale, con riferimento sia alla modalità di conservazione cartacea che digitale.

Eventuale nomina del Data Protection Officer nello Studio Professionale

La Comunicazione della Commissione europea – COM (2018) - del 24 gennaio 2018 ricorda che "*il regolamento non ha modificato in modo sostanziale i concetti e i principi fondamentali della legislazione in materia di protezione dei dati introdotta nel 1995. La grande maggioranza dei titolari del trattamento e dei responsabili del trattamento che rispettano già le attuali disposizioni dell'UE non dovrà quindi introdurre importanti modifiche nelle proprie operazioni di trattamento dei dati per conformarsi al regolamento. Il regolamento produce effetti per la maggior parte degli operatori le cui attività principali consistono nel trattamento dei dati e/o nel trattamento di dati sensibili, nonché per gli operatori che si occupano del monitoraggio regolare e sistematico delle persone fisiche su larga scala*".

A tale scopo si ritiene utile ricordare che sono tenuti alla designazione del responsabile della protezione dei dati personali (Data Protection Officer) il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c) del GDPR, ovvero le cui attività principali consistano in trattamenti che richiedono, per loro natura, ambito di applicazione e/o finalità, il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti, su larga scala, di categorie particolari di dati personali[24] o di dati relativi a condanne penali e a reati. Il diritto

[24] Il riferimento è ai dati di cui all'art. 9 del GDPR, ovverosia ai dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o **l'appartenenza sindacale**, i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, i **dati relativi alla salute** o alla vita

dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Varrà evidenziare che il Garante non ritiene obbligatoria la nomina del DPO "*in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale*". Nondimeno, tale nomina "*in ogni caso, resta comunque raccomandata, anche alla luce del principio di <<accountability>> che permea il Regolamento*"[25].

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.

Larga scala

Il GDPR non riporta una definizione di trattamento "su larga scala", ma in questi casi il Garante raccomanda di tenere conto dei fattori di seguito elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- 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.

In ogni caso le Linee Guida del Garante escludono che "*il trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato*" possa costituire un trattamento su larga scala. Analogamente, si ritiene, pertanto, che anche il trattamento di dati sensibili effettuato dal singolo commercialista non costituisca un trattamento su larga scala.

Per i restanti casi, si applica il criterio dell'auto-analisi in ottemperanza al criterio di responsabilizzazione previsto dalla normativa comunitaria e si dovrà effettuare una valutazione di impatto nel caso in cui vi siano elevate rischiosità per i diritti e per le libertà degli interessati.

Monitoraggio regolare e sistematico

Il GDPR non riporta una definizione di "Monitoraggio regolare e sistematico", ma il Garante vi fa rientrare tutte le forme di tracciamento e profilazione effettuate tramite *Internet* anche per finalità di pubblicità comportamentale, pur non esclusivamente riferibili all'ambiente *online.*

L'aggettivo "regolare", secondo le indicazioni del Garante, si riferisce alle modalità di effettuazione del trattamento dei dati che assumano almeno uno dei seguenti significati:

sessuale o all'orientamento sessuale della persona, il cui trattamento è in linea di principio vietato dal GDPR, salvo nelle ipotesi espressamente previste dal par. 2 del medesimo art. 9.

[25] Cfr. Garante privacy, *Nuove faq sul responsabile della protezione dei dati in ambito privato*, documento web n. 8036793 del 26 marzo 2018; *Linee Guida sui responsabili della protezione dei dati*, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

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

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[26].

Salvo casi particolari (ad esempio, ove lo Studio utilizzi telecamere a circuito chiuso o effettui tracciamento dell'ubicazione attraverso *app* su dispositivi mobili oppure utilizzi programmi di fidelizzazione o di pubblicità comportamentale), appare rara l'effettuazione, da parte del commercialista, di attività di monitoraggio sistematico e regolare.

Aspetti documentali

Ai fini del corretto adempimento degli obblighi derivanti dal GDPR, ogni misura adottata dovrà essere **documentabile** in ossequio al principio di "responsabilizzazione". Pertanto, nonostante il registro dei trattamenti previsto dal GDPR non sia obbligatorio per gli studi professionali, se ne consiglia l'adozione[27].

[26] Cfr. Garante privacy; Linee Guida sui responsabili della protezione dei dati, cit.

[27] L' articolo 30 del GDPR rubricato *Registri delle attività di trattamento* prevede infatti che:
1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

Riteniamo opportuno richiamare l'attenzione dei colleghi anche su altri aspetti relativi alla conformità documentale richiesta ai fini del principio di responsabilizzazione.

a) *INFORMATIVE*: Le informative sinora utilizzate potrebbero risultare incomplete alla luce di quanto richiesto dal GDPR. È consigliabile verificare la loro conformità al regolamento alla luce di quanto prescritto, in particolare, dagli articoli 13 e 14 del GDPR.

COSA DOVREBBE CONTENERE L'INFORMATIVA	
Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	• Il Commercialista dovrà evidenziare in modo chiaro, trasparente e con linguaggio semplice: • 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 (se nominato); • le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento; • i legittimi interessi perseguiti dal titolare del trattamento o da terzi, se fungono da base giuridica del trattamento; • gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; • l'intenzione del titolare del trattamento di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate od opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili; • 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 o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; • l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso anteriormente

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

COSA DOVREBBE CONTENERE L'INFORMATIVA	
	prestato, nei casi di trattamento basato sul consenso, anche di categorie particolari di dati; • il diritto di proporre reclamo a un'autorità di controllo; • se la comunicazione di dati personali è un obbligo legale o contrattuale o un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati personali, oltre alle possibili conseguenze circa la mancata comunicazione di tali dati; • l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, in tali casi, le informazioni significative sulla logica utilizzata, oltre all'importanza e alle conseguenze previste di tale trattamento per l'interessato.
Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato	Occorre rendere note le informazioni di cui sopra (con esclusione del riferimento alla comunicazione dei dati personali come obbligo legale o contrattuale), con l'aggiunta: • delle categorie di dati personali oggetto di trattamento; • della fonte da cui hanno origine i dati personali e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico.

b) *CONSENSO*: Come detto, il trattamento dei dati può non basarsi sul consenso. Qualora il commercialista effettui il trattamento dei dati personali sulla base di un contratto con il cliente il consenso non è necessario. Parimenti, si ricorda che non è obbligatorio ottenere il consenso anche nei casi in cui il trattamento si renda necessario per adempiere ad un obbligo normativo o per legittimo interesse. Si rende, invece, certamente obbligatorio il consenso specifico in caso di trattamento di particolari categorie di dati (es. dati giudiziari o particolari categorie di dati, come quelli desumibili dalla documentazione attestante il sostenimento di spese mediche consegnate dal Cliente al Commercialista ai fini della relativa detrazione).

c) *DELEGHE AUTORIZZATIVE*: il titolare del trattamento (*dominus* di Studio o Associazione o Società Professionale) dovrà autorizzare i propri collaboratori e tirocinanti ad effettuare il trattamento dei dati personali degli interessati.

d) *ORGANIZZAZIONE DI STUDIO*: il titolare del trattamento (*dominus* di Studio o Associazione o Società Professionale) dovrà impostare tutte le proprie attività e l'organizzazione di studio rispettando i principi della "*privacy by design*" e "*privacy by default*"[28],adottando

[28] Si tratta dei principi desumibili dall'art. 25 del GDPR rubricato *protezione dei dati fin dalla progettazione (privacy by design) e protezione per impostazione predefinita (privacy by default)* in base al quale: "*1. 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*

conseguentemente, adeguate misure tecniche ed organizzative, prima che il trattamento dei dati personali abbia inizio, idonee a consentire il rispetto dei principi di minimizzazione dei dati, limitazione della conservazione e ad evitare la comunicazione dei dati a persone non autorizzate. Qualora lo studio effettui, inoltre, profilazioni, trattamenti automatizzati, trattamenti trasfrontalieri di dati personali, videosorveglianza, monitoraggio sistematico o trattamenti su larga scala, dovrà prevedere informative, consensi e misure adeguate al maggiore livello di rischiosità concretizzato per la protezione dei dati personali. Inoltre, si consiglia di prevedere, sempre, una procedura per i c.d. "*data breaches*" (violazione dei dati personali) nonché appositi meccanismi per consentire l'esercizio dei diritti dell'interessato secondo le modalità descritte dal GDPR[29] (es. diritto di accesso).

Trattamento per finalità diverse da quelle per cui i dati sono stati raccolti

Qualora il Commercialista, in qualità di titolare del trattamento, intenda trattare ulteriormente i dati personali per finalità diverse da quella per cui gli stessi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato una nuova informativa relativa a tale diversa finalità e ogni ulteriore informazione pertinente. Tale informativa potrà costituire appendice al contratto già stipulato con il Cliente[30].

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.

2. 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.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo".

[29] In punto, si veda il Capo III, *diritti dell'interessato*, artt. 12-23 del GDPR.

[30] Cfr. art. 13 co. 3 GDPR.

Glossario GDPR

Glossario

Si riportano a seguire le definizioni adottate dall'art. 4 del GDPR:

1) «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 o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «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 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 o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «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;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «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; 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;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il

trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «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;

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;

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;

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;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

20) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

Allegato

Checklist di base per

GLI STUDI PROFESSIONALI

Categorie di dati personali ed interessati coinvolti 1°	Specificare tutti gli elementi inclusi nel trattamento per ciascuna categoria 2°	Fonte dei dati personali 3°	Scopo del trattamento dati personali 4°	Base giuridica per ciascun scopo (categorie non speciali di dati personali) 5°	Categorie speciali di dati personali 6°	Base giuridica per il trattamento di categorie speciali di dati personali 7°	Periodo di conservazione 8°	Azioni richieste per la conformità al GDPR 9°
Elencare le categorie di interessati e dati personali raccolti e conservati, ad es. dati relativi al personale attivo di ufficio ed in congedo; dati relativi alla clientela (es. informazioni sui servizi dallo studio, ecc.)	*Elencare ciascun tipo di dati personali inclusi all'interno di ciascuna categoria di dati personali, ad es. nome, indirizzo, eventuali dettagli bancari, cronologia dei servizi acquistati, cronologia di navigazione online, immagini di spese sostenute, atti inerenti la persona, ecc.).* *È importante tracciare anche il flusso dei dati personali trattati.*	*Elencare la (e) fonte (i) dei dati personali e se sono raccolti direttamente o da terze parti*	*All'interno di ciascuna categoria di dati personali, indicare gli scopi per i quali dati vengono raccolti e conservati, ad es. esecuzione del contratto, marketing, miglioramento del servizio, ecc)*	*Per ogni scopo per il quale vengono trattati i dati personali, elencarne la base giuridica su cui si basa* *ad es. consenso, contratto, basi legali (articolo 6 GDPR).*	*Se vengono raccolte e trattati speciali categorie di dati personali,* *specificarne i dettagli sulla natura dei dati, ad es. dati sanitari, genetici, biometrici.*	*Elencare la base giuridica per la quale sono trattati categorie speciali di dati personali, ad es. consenso esplicito, liceità art. 9 GDPR.*	*Per ogni categoria di dati personali, elencare il periodo per il quale i dati saranno conservati.* *Come regola generale, i dati devono essere conservati per un periodo non superiore a quello necessario per lo scopo per il quale sono stati raccolti originariamente*	*Identificare le azioni necessarie per garantire che tutte le operazioni di trattamento dei dati personali siano conformi a GDPR, ad es. cancellazione dei dati laddove non vi siano ragioni in linea con lo scopo originario per conservarle.*

a) Dati Personali trattati

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trattamenti basati sul consenso (Art. 7, 8, 9)	Si sono esaminati i meccanismi di Studio per la raccolta del consenso per garantire che la richiesta di consenso venga presentata in modo chiaramente distinguibile dalle altre materie (es. in una pagina distinta ed a parte del contratto di consulenza), in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro?			
	Se i dati personali che attualmente si trattano in base al consenso non soddisfano quanto richiesto ai sensi del GDPR, lo studio ha proceduto a richiedere nuovamente il consenso dell'interessato per garantire la conformità al GDPR?			
	Esistono procedure di Studio per dimostrare che una persona ha acconsentito al trattamento dei propri dati personali?			
	Esistono procedure per consentire ad una persona di revocare il proprio consenso al trattamento dei propri dati personali?			
Dati personali dei minori (Art. 8)	Qualora vengano forniti servizi online ad un minore, esistono procedure per verificare l'età e ottenere il consenso di un genitore / tutore legale, ove richiesto?			
Trattamenti basati sul legittimo interesse	Se l'interesse legittimo è una base giuridica su cui vengono trattati i dati personali, è stata effettuata un'analisi appropriata per garantire che l'uso di questa base giuridica sia appropriata? Tale analisi deve dimostrare che 1) esiste un valido interesse legittimo, 2) il trattamento dei dati sia strettamente necessario per perseguire l'interesse legittimo, e 3) il trattamento non sia pregiudizievole ovvero non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento.			

b) Diritti degli interessati

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Diritto di accesso ai dati personali (Art. 15)	Esiste una politica / procedura documentata per la gestione delle richieste di accesso ai propri dati personali da parte dell'interessato?			
	Lo Studio è organizzato a rispondere entro un mese?			
Portabilità dei dati (Art. 20)	Esistono procedure per fornire agli interessati i loro dati personali in un formato strutturato, comunemente usato e leggibile da un dispositivo?			
Diritto di rettifica e di cancellazione (Art. 16 e 17)	Esistono controlli e procedure per consentire la cancellazione (oblio) o la rettifica dei dati personali (ove applicabile)?			
Diritto alla limitazione di trattamento (Art. 18)	Esistono controlli e procedure per cessare il trattamento dei dati personali laddove un interessato abbia, per motivi validi, richiesto la limitazione del trattamento?			
Diritto di opposizione (Art. 21)	Gli interessati al trattamento sono informati del loro diritto di opporsi all'effettuazione di determinati tipi di trattamento (come per il marketing diretto)?			
	Esistono controlli e procedure per cessare il trattamento dei dati personali quando l'interessato si è opposto al trattamento?			
Profilazione e processi automatizzati (Art. 22)	Se lo studio utilizza un processo decisionale automatizzato, che ha un impatto legale o significativo per l'interessato, il trattamento è basato sul consenso, ed è stato raccolto con un consenso esplicito?			
	Quando viene presa una decisione automatizzata che è necessaria per stipulare o eseguire un contratto, o in base al consenso esplicito di un dell'interessato, esistono procedure per facilitare il diritto dell'interessato ad ottenere l'intervento umano e di poter contestare la decisione?			

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Limitazioni (Art. 23)	Sono stati chiariti all'interessato le ipotesi di limitazioni ai propri diritti e libertà fondamentali previste dall'art. 23 GDPR (es. prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica)?			

c) Accuratezza e conservazione

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Scopo limitato	I dati personali vengono utilizzati solo per gli scopi per i quali sono stati originariamente raccolti?			
Minimizzazione del dato	I dati personali raccolti sono limitati a quanto necessario per gli scopi per cui sono trattati?			
Accuratezza	Sono in atto procedure per garantire che i dati personali siano aggiornati e precisi e dove è necessaria una correzione, le modifiche necessarie sono apportate senza ritardi?			
Conservazione	Sono in atto politiche e procedure di conservazione per garantire che i dati personali siano conservati per un periodo non superiore a quello necessario per gli scopi per cui sono stati raccolti?			
	Lo studio è soggetto ad altre regole che richiedono un periodo minimo di conservazione (ad esempio documenti fiscali da mantenere per i dieci anni civilisticamente previsti: quantificare con il cliente anche i relativi costi di conservazione e la reale necessità di mantenerli in archivio di studio o se possibile di restituirli al cliente ed in che modalità)?			
	Sono attuate procedure per garantire che i dati personali vengano distrutti in modo sicuro, in conformità con le politiche di conservazione?			
Duplicazione delle informazioni	Esistono procedure per garantire che non vi siano duplicazioni inutili o non regolamentate dei dati personali raccolti e trattati?			

d) Requisiti di trasparenza

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trasparenza verso clienti e dipendenti (Art. 12, 13 e 14)	I dipendenti ed i collaboratori di studio ed i clienti sono pienamente informati sul come si utilizzino i propri dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile utilizzando un linguaggio chiaro e trasparente?			
	Esistono policy di studio chiare sull'utilizzo degli strumenti informatici utilizzati?			
	Laddove i dati personali siano raccolti direttamente presso l'interessato, sono in atto procedure per fornire le informazioni elencate all'art. 13 del GDPR (il personale di studio è all'uopo istruito)?			
	Se i dati personali non sono raccolti direttamente dall'interessato ma da una terza parte (ad esempio da un altro Professionista) sono in atto procedure per fornire le informazioni elencate all'Art. 14 del GDPR?			
	Quando si interagisce con gli interessati, ad esempio quando si fornisce un servizio personalizzato derivante da profilazione o si utilizza un Sistema di videosorveglianza, esistono procedure per informare proattivamente gli interessati dei loro diritti conformemente al GDPR?			
	L'interessato ha avuto ed ha disponibilità di capire come poter esercitare i propri diritti GDPR nei confronti dello studio con informativa in un formato facilmente accessibile e leggibile?			

e) Altri obblighi del titolare

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Accordi con i fornitori (Art. 27 a 29)	Sono stati esaminati accordi con fornitori e altre terze parti che trattano dati personali per conto dello Studio al fine di garantire che siano inseriti tutti i requisiti di protezione dei dati in modo adeguato?			
Data Protection Officer (DPO) – Responsabile della protezione dei dati personali (Art. 37 a 39)	Si è valutato se si è obbligati o meno come Studio a nominare un DPO (ex Art. 37 GDPR)? Il trattamento di dati personali non dovrebbe essere considerato un trattamento 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) qualora riguardi dati personali di clienti da parte di un singolo professionista.			
	Se si decide che un DPO non è obbligatorio per lo studio, si è proceduto ad archiviarne i motivi?			
	Se si decide che un DPO vada nominato, è prevista una procedura per il reporting al dominus di Studio? Queste procedure sono documentate?			
	Sono stati resi noti i dettagli di contatto del DPO di Studio affinché clienti, dipendenti e collaborator, possano prendere agevolmente contatto con lui?			
Data Protection Impact Assessment (DPIA) (Art. 35) o valutazione di impatto	Se il trattamento dei dati personali è considerato ad alto rischio, esiste in studio un processo per identificare la necessità di effettuare una valutazione di impatto? Queste procedure sono documentate?			

f) Sicurezza del trattamento

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Adeguate misure di sicurezza tecniche ed organizzative (Art. 32) 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	Lo studio ha valutato i rischi associati al trattamento dei dati personali effettuati e messo in atto misure adeguate per mitigarli? Ne ha messo anche da parte la relative documentazione?			
	Esiste un programma di sicurezza documentato che specifichi le misure tecniche, organizzative e logiche per un trattamento dei dati personali conforme al GDPR?			
	Dipendenti e collaboratori di studio sono stati adeguatamente formati sui rischi generali e specifici dei trattamenti di dati, sulle misure organizzative, tecniche ed informatiche adottate in studio, nonché sulle responsabilità e sulle sanzioni?			
	Esiste un processo documentato per la risoluzione di reclami e di problemi relativi alla sicurezza?			
	Esiste una persona di Studio che sia designata quale responsabile della prevenzione e delle indagini sulle violazioni della sicurezza (c.d data breach)? È stata valutato questo ruolo?			
	Sono utilizzate per trasferire, archiviare e ricevere informazioni personali riservate degli interessati tecnologie crittografiche?			
	Quando non è più necessaria la conservazione dei dati personali trattati, gli stessi, vengono distrutti, cancellate o anonimizzati? Gli interessati ne sono consapevoli?			
	L'accesso ai dati personali può essere ripristinato tempestivamente in caso di incidente fisico o tecnico?			

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
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.				

g) Data breaches (violazione dei dati personali)

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Obblighi di risposta alla violazione dei dati personali (Art. 33 e 34)	Lo studio ha un piano di risposta agli incidenti sulla sicurezza e sulla privacy che sia documentabile?			
	Questi piani e relative procedure vengono riesaminate in modo periodico?			
	Esistono procedure per notificare al Garante Privacy una violazione dei dati?			
	Esistono procedure per notificare agli interessati (qualora ne ricorrano i presupposti) una violazione dei dati?			
	Esiste piena documentazione di tutte le violazioni subite?			
	Esistono procedure di cooperazione tra i titolari del trattamento dei dati in ufficio, i fornitori ed altri partner per far fronte alle violazioni dei dati?			

h) Trasferimento dati personali (Extra europeo) – qualora applicabile

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trasferimenti internazionali di dati personali (Art. 44 a 50)	I dati personali sono trasferiti al di fuori dell'Europa, ad es. negli Stati Uniti o in altri paesi?			
	Il trasferimento include percaso anche particolari categorie di dati (es. dati sensibili)?			
	A che scopo viene effettuato il trasferimento?			
	A quale soggetto sono trasferiti tali dati personali?			
	Esiste un elenco complete di tutti i trasferimenti eventualmente effettuati? comprese le risposte ai quesiti precedenti (ad esempio, la natura dei dati, lo scopo del trattamento, da quale Paese i dati vengono esportati e quale Paese riceve i dati e chi è il destinatario del trasferimento?)			
Trasferimenti internazionali leciti	Esiste una base legale per il trasferimento? (ad es. Decisione sull'adeguatezza della Commissione europea; clausole contrattuali standard). Queste basi sono documentate?			
Trasparenza	Gli interessati sono pienamente informati di eventuali trasferimenti internazionali previsti dei loro dati personali?			