MASSIMO BIANCHI
STUDIO COMMERCIALE

CIRCOLARE MENSILE PER L'IMPRESA

maggio 2018

SUPPLEMENTO

Speciale *privacy*

ICAEW CHARTERED ACCOUNTANT

Via G. Carducci, 51
56010 La Fontina
San Giuliano Terme – Pisa
Tel 050 878668
Fax 050 8755566
email: info@mb-consulenze.com

LE NOVITÀ E LE MISURE ORGANIZZATIVE PER IL TRATTAMENTO DEI DATI PERSONALI ALLA LUCE DEL REGOLAMENTO UE 2016/679

Il Regolamento UE 2016/679 dal prossimo 25 maggio porta seco nuovi adempimenti per professionisti e imprese che dovranno porre misure idonee e adeguate per il corretto trattamento dei dati personali dei propri clienti.

Introduzione

Il Regolamento UE 2016/679 (di seguito GDPR) del 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale UE del 4 maggio 2016, sarà pienamente esecutivo dal 25 maggio 2018, abrogando la Direttiva del '95 sulla protezione dei dati personali che è stata recepita dalla normativa nazionale attuale.

Pur essendo il GDPR direttamente applicabile e vincolante per gli Stati membri, il Legislatore italiano con l'articolo 13, L. 163/2017 (c.d. "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 prevedendo:

- l'espressa abrogazione delle disposizioni del codice incompatibili con quelle contenute nel Regolamento;
- la modifica del codice stesso limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento;
- il coordinamento delle disposizioni vigenti in materia di protezione dei dati personali con quelle recate dal Regolamento (UE) 2016/679.

In tale prospettiva il Consiglio dei Ministri ha approvato, in esame preliminare, un decreto legislativo che introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del citato Regolamento europeo. Ne deriva che a far data dal 25 maggio 2018 il vigente codice in materia di protezione dei dai personali 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*.

In questo contesto il Cndcec, con il recente documento di aprile 2018, ha emanato le *checklist* di base per gli studi professionali atte 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.

Le novità del GDPR

La principale novità del GDPR riguarda il principio di *accountability* del titolare posto alla base della nuova normativa, cioè la responsabilizzazione del titolare rispetto alle misure, organizzative e tecniche, poste in essere per conformarsi al GDPR. In base a questo principio, al titolare è riconosciuto un certo livello di discrezionalità nel processo di adeguamento a fronte del quale è posto, però, l'obbligo di documentare le scelte fatte e le ragioni che le hanno motivate nell'ottica dell'adeguamento alla norma.

Vi sono poi alcune importanti misure che innovano la materia, le più importanti delle quali sono rispettivamente:

- nuovi diritti riconosciuti agli interessati e una particolare attenzione alla tutela dei minori;
- redazione e aggiornamento del Registro dei trattamenti, cioè dell'elenco delle operazioni (trattamenti) effettuate dal titolare che prevedono l'utilizzo di dati personali;
- obbligo di definire a priori i termini di conservazione dei dati personali trattati e di dichiarare tale termine nell'informativa comunicata all'interessato;
- nuovi obblighi posti in capo al titolare, tra cui:
  - obbligo di notifica al Garante delle violazioni di sicurezza relative a dati personali e comunicazione della violazione agli interessati, se necessario;
  - obbligo di tenere conto della *data protection* fin dalla progettazione, in caso di sviluppo di nuovi servizi o per la revisione di quelli esistenti;
  - obbligo di procedere a una analisi approfondita dell'impatto sui diritti e le libertà degli interessati quando l'innovazione comporti rischi particolari anche in virtù delle tecnologie innovative utilizzate;
- riaffermazione della necessità di basare le misure di sicurezza su un'attenta analisi dei rischi;
- ridisegno dei rapporti fra il titolare e i fornitori di servizi che trattano dati personali per conto del titolare stesso, con la previsione, a determinate condizioni, della responsabilità solidale dei 2 soggetti per i danni eventualmente provocati;
- nuova figura del *data protection officer* finalizzata a facilitare la corretta applicazione del GDPR da parte del titolare.

Limiti di applicazione del GDPR

Il presupposto fondamentale per l'applicazione del Regolamento è che l'impresa o il professionista debba trattare **dati personali**. Più precisamente l'articolo 4 del GDPR qualifica come dato personale "*qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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*". Del pari, l'articolo 2 del GDPR stabilisce 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*". Peraltro, lo stesso considerando 14 precisa come sia "*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".

Sul punto giova osservare come **detti obblighi non sussistano** quando:

- il trattamento riguarda dati che non sono personali bensì anonimi (ad esempio, dati aggregati o statistici);
- il trattamento riguarda i dati di enti/persone giuridiche.

Peraltro, è lo stesso considerando 14 a precisare che il Regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare quelli delle imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

Ne deriva che **saranno escluse** dal perimetro di applicazione del GDPR **le persone giuridiche** quali società di capitali, fondazioni o consorzi: in questo contesto i dati dei bilanci, della sede o i dati di contatto non saranno ricompresi negli adempimenti del Regolamento.

Si ricorda che nella vigenza del codice della *privacy* il trattamento dei dati relativi a persone giuridiche, enti e associazioni ha dovuto tener conto della parziale abrogazione, di cui all'articolo 40, comma 2, D.L. 201/2011, convertito con L. 214/2011, di alcune delle disposizioni contenute nella parte prima del D.Lgs. 196/2003. Infatti, a seguito delle richiamate abrogazioni, per dato personale si è dovuto intendere "qualunque informazione relativa a persona fisica" e per interessato esclusivamente "la persona fisica cui si riferiscono i dati personali" (cfr. rispettivamente l'articolo 4, comma 1, lettere b) e i) del codice della *privacy*); in altri termini, la portata applicativa di tutte le disposizioni del codice che riguardano gli interessati ovvero il trattamento di dati personali è stata limitata in via esclusiva alle persone fisiche ed ai trattamenti di informazioni personali che vi si riferiscono, con esclusione di persone giuridiche, enti e associazioni.

Pur tuttavia, le disposizioni del GDPR potrebbero trovare applicazione con riferimento al trattamento dei dati personali del rappresentante legale delle imprese ovvero delle persone che vi lavorano.

Per vero sono da ricomprendersi tra i dati personali le informazioni personali di contatto quali nome, indirizzo di casa, telefono di casa o numero di cellulare, numero di *fax*, indirizzo *email* e *password*; informazioni riguardanti la famiglia, lo stile di vita e le circostanze sociali tra cui età, data di nascita, stato civile; particolarità riguardanti l'occupazione, lo stipendio e altri benefici, prestazione di lavoro, formazione/qualificazione, numeri di identificazione, ID univoco raccolto da dispositivi mobili, vettori di rete o *provider* di dati, indirizzi IP e dati sul comportamento e sugli interessi *online*.

Sul punto giova osservare come per arrivare all'identificabilità di una persona sia opportuno considerare tutti i mezzi di cui si dispone, compresa l'individuazione, di cui il titolare del trattamento o un terzo può avvalersi per identificare detta persona fisica direttamente o indirettamente. "*Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici*."

Peraltro il nuovo Regolamento non trova applicazione anche per i trattamenti di dati personali effettuati:

- da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- da autorità di pubblica sicurezza;
- in casi particolareggiati e specificati nell'articolo 2 del GDPR (ad esempio autorità competenti per fini di prevenzione, indagine, accertamento, esecuzione di sanzioni penali, etc.).

In relazione all'ambito territoriale l'articolo 3 del Regolamento ne stabilisce l'applicazione 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 Europea, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione Europea. In altri termini si guarda se i titolari del trattamento e i responsabili del trattamento siano stabiliti nell'Unione Europea, a prescindere dalla circostanza che il trattamento sia o meno ivi concretamente effettuato e a prescindere dalla nazionalità o dal luogo di residenza dei soggetti.
Peraltro gli adempimenti fissati dal GDPR saranno comunque dovuti nel caso di trattamento dei dati personali di interessati che si trovano nell'Unione Europea, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione Europea, quando le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione Europea, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
- oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione Europea.

Il Regolamento si applica infine al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione Europea, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Principi applicabili al trattamento dei dati personali

Il GDPR conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; l'articolo 5, §1 del Regolamento prevede infatti che i dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- 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, § 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- 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");
- 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, § 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");

- 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")".

I fondamenti di liceità del trattamento sono indicati all'articolo 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal codice della *privacy* - D.Lgs. 196/2003 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Sul punto giova rilevare come il trattamento sia **lecito** solo qualora e nella misura in cui ricorra almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il trattamento, oltre che lecito, deve essere corretto e trasparente, laddove il considerando 39 del GDPR precisa che trasparente dovrebbero essere le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Trattamento di dati particolari

Anche il nuovo Regolamento tratta con disposizioni speciali le c.d. "**particolari categorie di dati personali**" che sono concretamente speculari a quelli che nel D.Lgs. 196/2003 sono qualificati come dati sensibili.

In particolare le categorie particolari di dati comprendono specifiche categorie di dati personali che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché dati genetici e/o biometrici intesi a identificare in modo univoco

una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Secondo il GDPR i trattamenti delle categorie particolari di dati personali, necessari per motivi di interesse pubblico rilevante, sono ammessi qualora siano previsti dal diritto dell'Unione Europea ovvero, nell'ordinamento interno, da disposizioni di legge o di Regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante. Tali disposizioni devono, in ogni caso, assicurare:

- che il trattamento sia proporzionato alla finalità perseguita;
- che sia salvaguardata l'essenza del diritto alla protezione dei dati;
- che siano previste misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Per questi dati viene contemplato in via generale un divieto di trattamento fatto salvo che l'interessato abbia prestato il proprio consenso esplicito per finalità specifiche o sia necessario trattarli per:

- assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- accertare, esercitare o difendere un diritto in sede giudiziaria.

Sul punto l'emandando decreto provvederà che in ogni caso si dovranno considerare compiuti per motivi di interesse pubblico rilevante i trattamenti effettuati in ambiti identificati o in altri espressamente individuati dalla legge, tra cui:

- attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- rapporti tra i soggetti pubblici e gli enti del Terzo settore;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- trattamento dati idonei a rivelare lo stato di salute da parte di esercenti professioni sanitarie e organismi sanitari;
- compiti del Ssn e degli altri organismi sanitari, nonché igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- trattamenti effettuati per scopi storici, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di rilevante interesse storico, per scopi scientifici, nonché da soggetti che fanno parte del sistema statistico nazionale (Sistan);
- instaurazione, gestione ed estinzione di rapporti di lavoro e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità.

Giova precisa che per il trattamento di dati relativi a condanne penali e reati o a connesse misure di sicurezza ai sensi dell'articolo 6, § 1, del GDPR, che non avviene sotto il controllo dell'autorità pubblica sarà consentito solo se autorizzato da disposizioni di legge o di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.
In questo ambito tali trattamenti saranno consentiti se autorizzati da disposizioni di legge o di Regolamento riguardanti, in particolare:

- l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro;
- l'adempimento degli obblighi previsti da disposizioni di legge e Regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
- la verifica o accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi e dai regolamenti;
- l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché per la prevenzione, accertamento e contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi e dai regolamenti in materia;
- l'accertamento, esercizio o difesa di un diritto in sede giudiziaria;
- l'esercizio del diritto di accesso ai dati e ai documenti amministrativi;
- l'esecuzione di investigazioni o ricerche o per la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del Testo unico delle leggi di pubblica sicurezza;
- l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e certificazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale, nei casi previsti da leggi o dai regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
- l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
- l'attuazione della disciplina in materia di attribuzione del *rating* di legalità delle imprese ai sensi dell'articolo 5-*ter*, D.L. 1/2012;
- l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Consenso e informativa

Ai sensi dell'articolo 4 del nuovo Regolamento il **consenso** viene definito come una "*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*".
In questo ambito appare sussistere la possibilità che la dichiarazione di consenso non risulti necessariamente da una documentazione resa per iscritto, purché tale dichiarazione sia stata prestata in maniera inequivocabile.

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".*

Il Regolamento, all'articolo 12, prevede che il titolare del trattamento adotti misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento.

Più precisamente il Regolamento stabilisce che le informazioni contenute all'interno dell'informativa vengano fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro; le stesse sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato e il fatto di aver dato le informazioni.

Secondo la nuova disciplina il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è la modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Invero, il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Per i **dati "particolari"** (quelli sensibili *ex* articolo 9, Regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22).

Giova precisare come il consenso raccolto precedentemente al 25 maggio 2018 resti valido se ha tutte le caratteristiche individuate dal Regolamento. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il Regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica e prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara.

In tale prospettiva si osserva come i **contenuti dell'informativa** siano elencati in modo tassativo negli articoli 13, § 1, e 14, § 1, Regolamento e in parte siano più ampi rispetto al codice vigente. In particolare, il titolare deve sempre specificare:

- l'identità e i dati di contatto del titolare del trattamento e del RPD-DPO (Responsabile della protezione dei dati - *data protection officer*), ove esistente;

- le finalità del trattamento e la base giuridica;
- le categorie di dati personali che tratta;
- gli eventuali destinatari o categorie di destinatari dei dati;
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, etc.).

Peraltro, il Regolamento prevede anche ulteriori informazioni da fornire **in aggiunta** nel momento in cui i dati personali sono ottenuti, in quanto necessarie per garantire un trattamento corretto, tra cui:

- periodo di conservazione dei dati personali o criteri per determinarlo;
- diritti dell'interessato (accesso, rettifica, portabilità dei dati, etc.);
- laddove previsto, l'esistenza del diritto di revocare il consenso in qualsiasi momento;
- diritto di proporre reclamo a un'autorità di controllo;
- se obbligo legale o contrattuale oppure requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze;
- esistenza di un processo decisionale automatizzato, compresa la profilazione.

Sono, inoltre, parzialmente diversi i requisiti che il Regolamento fissa per l'esonero dall'informativa (si veda articolo 13, § 4 e articolo 14, § 5 del Regolamento, oltre a quanto previsto dall'articolo 23, § 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda articolo 14, § 5, lettera b) – a differenza di quanto prevede il codice della *privacy*.

È utile precisare che l'informativa deve essere fornita all'interessato **prima di effettuare** la raccolta dei dati (se raccolti direttamente presso l'interessato – articolo 13 del Regolamento).

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, **prima** di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Invero, se i dati non sono raccolti direttamente presso l'interessato (articolo 14 del Regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento ed essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato). In tali casi, per come specificato nella norma *ex* articolo 14, comma 2, GDPR, il titolare dovrebbe fornire all'interessato ulteriori informazioni al fine di garantire un trattamento corretto e trasparente quali:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- qualora il trattamento si basi sull'articolo 6, § 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

- qualora il trattamento sia basato sull'articolo 6, § 1, lettera a), oppure sull'articolo 9, § 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, § 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Appare utile ricordare che quanto previsto nell'articolo 14, GDPR non si applica se:

- l'interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione applicabile;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale.

Va, infine, rilevato come, qualora il professionista effettui il trattamento dei dati personali sulla base di un contratto con il cliente, il consenso non sia necessario. Del pari non è obbligatorio ottenere il consenso anche nei casi in cui il trattamento si renda necessario per adempiere a un obbligo normativo o per legittimo interesse ovvero per l'adempimento di un obbligo di legge (in questo ambito potrebbero essere ricompresi i dati trattati ai fini della normativa antiriciclaggio). Si rende, invece, certamente obbligatorio il consenso specifico in caso di trattamento di particolari categorie di dati (ad esempio dati giudiziari o particolari categorie di dati, come quelli desumibili dalla documentazione attestante il sostenimento di spese mediche consegnate dal cliente al professionista ai fini della relativa detrazione fiscale).

Il titolare, i responsabili esterni e gli incaricati

Il titolare viene qualificato nel Regolamento come: "*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*".

Tale definizione introduce anche la nuova disciplina della **contitolarità** del trattamento (articolo 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente. Ne deriva che nel contratto intercorrente tra contitolari dev'essere configurata una chiara ripartizione delle responsabilità ai sensi del GDPR, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

Il titolare e/o i contitolari sono tenuti a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività che compiono sui dati con il GDPR, compresa l'efficacia delle misure di sicurezza che adottano. Tali misure dovrebbero tener conto della natura,

dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Il GDPR prevede poi anche la figura del **responsabile** ossia "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*.

Al riguardo il Regolamento fissa più dettagliatamente (rispetto al codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto e deve disciplinare tassativamente almeno le materie riportate al § 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento.

In realtà saranno sussistenti obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari (tenuta del registro dei trattamenti svolti, adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti, designazione di un DPO). Peraltro è consentita la nomina di *sub*-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; ne deriva che quest'ultimo risponderà dinanzi al titolare dell'inadempimento dell'eventuale *sub* responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

In merito, va rilevato che, come indicato anche dal Cndcec, i rapporti di approvvigionamento (responsabile trattamento dati, responsabile protezione dei dati, servizi *cloud*, etc.) dovranno essere regolati tramite un contratto firmato *intuitu personae*. All'uopo sarà sicuramente utile:

- richiedere al fornitore di inoltrare la sua politica di sicurezza dei sistemi informativi insieme a tutti i documenti di supporto delle sue certificazioni di sicurezza delle informazioni e allegare tali documenti al contratto e verificare che le misure siano conformi alla propria politica di sicurezza e alle raccomandazioni dell'autorità Garante;
- determinare e fissare in modo dettagliato, su base contrattuale, le operazioni che il responsabile del trattamento potrà eseguire sui dati personali, tra cui:
  - i dati a cui avrà accesso o che gli saranno trasmessi;
  - le operazioni che deve eseguire sui dati;
  - la durata per la quale può memorizzare i dati;
  - tutti i destinatari a cui il responsabile del trattamento potrà trasmettere i dati;
  - le operazioni da eseguire al termine del servizio (cancellazione permanente dei dati o restituzione dei dati nel contesto della reversibilità quindi distruzione di dati);
  - gli obiettivi di sicurezza stabiliti dal titolare del trattamento;
- determinare, su base contrattuale, la ripartizione delle responsabilità in merito ai processi legali volti a consentire agli interessati di esercitare i propri diritti;
- vietare o regolare l'utilizzo di fornitori di secondo livello;
- chiarire nel contratto che il rispetto degli obblighi di protezione dei dati è un requisito vincolante del contratto e prevedere specifiche clausole di responsabilità.

Il Regolamento non prevede espressamente la figura dell'**incaricato**, richiamando invece le c.d. "persone autorizzate al trattamento" sotto l'autorità diretta del titolare o del responsabile.
Sul tema l'emanando decreto attuativo indicherà espressamente che il titolare o il responsabile del trattamento possano disciplinare nell'ambito del proprio assetto organizzativo che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate che operano sotto la loro autorità. In concreto, il titolare o il responsabile del trattamento hanno la possibilità di individuare, con le modalità più opportune, le persone che operano sotto la propria autorità diretta per autorizzarle al trattamento dei dati personali.

L'accountability, il rischio e le misure di sicurezza

Tra le novità introdotte dal Regolamento vi è il principio di "**responsabilizzazione**" (c.d. ***accountability***), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali. In altri termini, titolari e responsabili dovranno adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, decidendo in via autonoma le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.
Come evidenziato dal Garante uno dei criteri è sintetizzato dall'espressione inglese "***data protection by default and by design***", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili. Si tratta in altri termini di valutare il rischio inerente al trattamento e di adottare le misure idonee a mitigare sufficientemente il rischio.
Fra le varie attività fondamentali vi sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. Al riguardo è l'articolo 35 del Regolamento a introdurre il concetto di valutazione d'impatto sulla protezione dei dati; in concreto la valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
In tale prospettiva si osserva come non sia obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, § 1). Il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei

dati non siano soddisfatte non diminuisce tuttavia l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento *"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

In questo ambito, le **misure di sicurezza** devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento; peraltro, la lista di cui al § 1 dell'articolo 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (*ex* articolo 33, codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento.

Sul punto si dovrà comprovare di aver posto in essere le misure idonee a tal fine: in concreto all'entrata in vigore del Regolamento, il titolare/responsabile del trattamento dovrà aver 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 richiamano, quali misure di sicurezza, i dispositivi anti intrusione, gli allarmi , le porte blindate, gli 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, il cambiamento periodico delle credenziali di accesso alla rete, il monitoraggio degli accessi, i salvataggi periodici e programmati dei dati trattati elettronicamente, la 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.

Le principali prescrizioni del GDPR

La nuova disciplina impone ai destinatari un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Con riguardo ai singoli adempimenti si sintetizzano alcune indicazioni metodologiche utili per la valutazione sulle misure organizzative necessarie per adeguarsi alle prescrizioni del GDPR.

In primo luogo andrà valutata la designazione di un "responsabile della protezione dati" (***Data protection officer* - DPO**) per l'attività esercitata. Il Regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali *ex* articoli 38 e 39). Il DPO coopera con l'Autorità (e proprio per questo, il suo nominativo va

comunicato al Garante e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Il Garante ha precisato che il DPO, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di *privacy*, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve inoltre poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Del pari deve agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, etc.) necessarie per l'espletamento dei propri compiti.

Il ruolo di DPO può poi essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (UE) 2016/679 assegna a tale figura. Il DPO scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei propri compiti, il DPO (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (articolo 5, § 2 del Regolamento).

I dati di contatto del responsabile designato dovranno poi essere pubblicati dal titolare o responsabile del trattamento. Per il Garante non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo.

Secondo le indicazioni del Regolamento, la **nomina del DPO è obbligatoria**:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Sul punto il Garante, nelle *faq* recentemente pubblicate sul sito istituzionale, ha chiarito che, ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito, imprese assicurative, sistemi di informazione creditizia, società finanziarie, società di informazioni commerciali, società di revisione contabile, società di recupero crediti, istituti di vigilanza, partiti e movimenti politici, sindacati, caf e patronati, società operanti nel settore delle "*utilities*" (telecomunicazioni, distribuzione di energia elettrica o gas), imprese di somministrazione di lavoro e ricerca del personale, società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione, società di *call center*, società che forniscono servizi informatici e società che erogano servizi televisivi a pagamento.
Sempre il Garante ha precisato che nei casi diversi da quelli previsti dall'articolo 37, § 1, lettera b) e c), del Regolamento (UE) 2016/679, la designazione del DPO **non è obbligatoria** (ad esempio, in relazione a trattamenti effettuati da **liberi professionisti** operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: si veda anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").
In quest'ottica resta comunque raccomandata, anche alla luce del principio di "*accountability*" che permea il Regolamento, la designazione di tale figura i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati. Al riguardo il Cndcec consiglia 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.

Sotto un ulteriore profilo tutti i titolari, a partire dal 25 maggio 2018, dovranno **notificare** all'autorità di controllo **le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovranno informare delle violazione anche gli interessati, sempre senza ingiustificato ritardo. Sarà necessario predisporre protocolli organizzativi che consentano di intervenire tempestivamente e procedere senza ritardo alla comunicazione al Garante.
Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all’autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Il registro dei trattamenti e le relative modalità di tenuta

Ulteriore obbligo del nuovo Regolamento è l’adozione di un **registro dei trattamenti**. In particolare i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda articolo 30, § 5), devono tenere un “*registro delle operazioni di trattamento”* i cui contenuti sono indicati all’articolo 30. Si tratta di uno strumento

fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Ogni titolare del trattamento dovrà tenere un registro delle attività di trattamento svolte che contenga le seguenti informazioni:

- 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;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- 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;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, § 1.

Ogni responsabile del trattamento dovrà tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- 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;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- 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;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, § 1.

Come osservato dal Garante la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali e quindi vengono invitati tutti i destinatari, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Lo stesso Cndcec osserva come 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, il Cndcec ne consiglia l'adozione.

Responsabilità e sanzioni

Il Regolamento, all'articolo 82, prevede il diritto per l'interessato che sia oggetto di un danno (materiale o immateriale) di ricevere un risarcimento per il danno, in base al soggetto che ha commesso la violazione, ovvero il titolare e/o il responsabile.

Più precisamente il titolare risponde per il danno cagionato dal suo trattamento che violi le norme del Regolamento, mentre il responsabile risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare. Di contro il titolare e/o il responsabile sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi, titolare e il responsabile, siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Il Regolamento aggrava poi le **sanzioni amministrative pecuniarie** fissando limiti massimi più elevati di quelli fino ad oggi previsti.

Ebbene, la violazione delle seguenti disposizioni/obblighi del titolare e del responsabile, in particolare degli articoli 25 *privacy by design*/*by default* e 32 sicurezza) è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
- gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
- gli obblighi dell'organismo di controllo a norma dell'articolo 41, § 4;

La violazione delle seguenti disposizioni (tra cui i principi fondamentali in materia di protezione) è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- i diritti degli interessati a norma degli articoli da 12 a 22;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, § 2, o il negato accesso in violazione dell'articolo 58, § 1.

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa, in ogni singolo caso si tiene debito conto dei seguenti elementi:

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, § 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Deve osservarsi altresì come il mancato adeguamento al Regolamento potrebbe comportare anche l'applicazione di **sanzioni penali**, che il GDPR ha lasciato a una regolamentazione autonoma di ogni singolo Stato. Infatti, il considerando 149 del testo GDPR, recita "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente Regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente Regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente Regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di Giustizia".*

Al riguardo, nella bozza del decreto di adeguamento della normativa nazionale alle disposizioni contenute nel GDPR, sono presenti le **sanzioni già esistenti e afferenti al trattamento illecito dei dati personali** (pena della reclusione da 6 a 18 mesi) e alla **falsità nelle dichiarazioni e notificazioni al Garante** (pena della reclusione da 6 mesi a 3 anni).

Accanto a tali sanzioni vengono previste nuove fattispecie incriminatrici e più precisamente:

- la comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone sanzionata con la reclusione da 1 a 6 anni;
- l'acquisizione fraudolenta di dati personali sanzionata con la reclusione da 1 a 4 anni.

Le *check list* del Cndcec

Il Cndcec, con il documento di aprile 2018, ha fornito alcune indicazioni di formazione e di informazione che possano costituire una efficace forma di auto-valutazione preventiva degli studi

alla luce della disciplina introdotta dal GDPR e ha ritenuto utile proporre delle "*check list di base per gli studi professionali*" da utilizzare al fine di valutare il livello di adeguamento alle nuove disposizioni del GDPR.

Secondo il Cndcec nell'**informativa** il professionista 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 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.

Secondo il Cndcec il titolare del trattamento (*dominus* di studio o associazione o società professionale) dovrà autorizzare i propri collaboratori e tirocinanti a effettuare il trattamento dei dati personali degli interessati definendo specifiche **deleghe** per i soggetti incaricati. Il titolare del trattamento dovrà poi impostare tutte le proprie attività e l'organizzazione di studio rispettando i principi della "*privacy by design*" e "*privacy by default*", adottando conseguentemente, **adeguate misure tecniche e 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 a evitare la comunicazione dei dati a persone non autorizzate.

Per l'organo di autoregolamentazione, 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.
A fattor comune comunque viene consigliato 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.