SINTESI del REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - GDPR

Il 25 maggio del 2018 sarà pienamente operativo il nuovo **Regolamento generale sulla protezione dei dati** (**GDPR**, Regolamento UE 2016/679) pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno.

La nuova disciplina va a sostituire la Direttiva europea 95/46/CE e – laddove incompatibili – le singole normative nazionali. Per l'Italia la materia della tutela della privacy è stata fino ad oggi regolata dal D.lgs. 196/2003 (Codice in materia di protezione dei dati personali).

Il **Regolatore europeo** nel predisporre la nuova disciplina, ha scelto di non fornire un elenco di norme propriamente prescrittive ma ha preferito piuttosto dettare dei **principi chiave** ai quali i singoli soggetti sono chiamati ad uniformarsi nell'ambito di un generale processo di "(auto)responsabilizzazione" (accountability).

Quanto appena detto è sintetizzabile nell'espressione inglese "*data protection by default and by design*" ossia nella 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 *ex ante*, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'**analisi preventiva da parte dei Titolari** che deve altresì tradursi in una serie di attività specifiche e dimostrabili.

Oltre a questo importante cambio di impostazione, tante sono le **novità introdotte dal GDPR**: innanzitutto il Regolatore europeo ha voluto estendere il più possibile l'ambito di intervento della nuova normativa e difatti il GDPR non si applicherà soltanto ai dati degli "interessati" che sono residenti nell'Unione Europea, ma – a differenza della precedente Direttiva – il **Regolamento si applicherà anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE** che trattano dati personali di residenti nell'Unione Europea. Ciò indipendentemente dal luogo o dai luoghi ove sono collocati i sistemi di archiviazione e di elaborazione.

Dal punto di vista "oggettivo", il Regolamento conferma che ogni trattamento perché sia considerato legittimo deve trovare fondamento in un'idonea base giuridica: i fondamenti di **liceità del trattamento** sono indicati all'**art. 6 dello stesso GDPR** e coincidono, in grande parte, con quelli già elencati dal Codice in materia di protezione dei dati personali.

Tali fondamenti sono il consenso, l'adempimento di obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, gli obblighi di legge cui è soggetto il titolare, l'interesse pubblico o l'esercizio di pubblici poteri, l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il consenso

Relativamente al **consenso**, l'articolo 9 del Regolamento prevede che lo stesso debba essere "**esplicito**" laddove riguardi il **trattamento di dati sensibili**; ciò non significa che debba essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è la modalità più idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito".

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.

In ogni caso il consenso deve essere – così come già previsto anche dal Codice – **libero, specifico, informato e inequivocabile**. A tale fine la formula utilizzata per richiederlo deve essere comprensibile, semplice, chiara.

L'informativa

Tra i principi ispiratori del Regolamento hanno particolare rilievo la **trasparenza e la chiarezza nei confronti dell'interessato**, e proprio al fine di rendere l'interessato maggiormente consapevole e informato in merito al trattamento che viene effettuato sui propri dati, il Regolatore europeo è intervenuto anche sul tema dell'informativa, ampliandone i contenuti (articolo 13, par. 1 e articolo 14, par. 1): al momento della raccolta dei dati (o comunque non oltre un mese dalla raccolta, nel caso in cui i dati non siano raccolti direttamente presso l'interessato) il **Titolare del trattamento deve fornire idonea informativa** ove specifica – tra le altre cose – i **dati di contatto del DPO** (*Data Protection Officer*), laddove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti, il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, il diritto di presentare un reclamo all'autorità di controllo.

Nel rispetto dei summenzionati principi di trasparenza e chiarezza, il **GDPR** specifica inoltre che l'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e deve essere altresì facilmente accessibile.

A cosa deve prestare attenzione un Fondo Pensione nel trattamento dei dati dell'iscritto?

Per verificare d'essere adeguato alla normativa un **Fondo pensione può procedere ad una mappatura puntuale dei dati** che tratta, dal momento in cui li acquisisce a quello in cui li cancella. La mappatura è funzionale alla verifica dello stato di adeguamento della struttura alla nuova normativa ma può essere altresì utile all'identificazione di eventuali trattamenti a rischio elevato che quindi richiedono valutazione dell'impatto sulla protezione dei dati.

Talvolta – soprattutto nel caso in cui riceva richieste di anticipazioni per spese sanitarie – il Fondo pensione si trova a dover **trattare dei dati** c.d. "**sensibili**" (appartenenti a particolari categorie di dati personali, secondo il glossario del GDPR, v. art. 9), in questi casi è necessario che il Fondo acquisisca il **consenso al trattamento** e che lo stesso abbia i requisiti previsti dalla normativa, ovvero sia: libero, specifico, informato e inequivocabile.

Altro aspetto cui il Fondo pensione deve prestare attenzione è l'informativa. L'**informativa deve essere fornita** nel momento in cui si acquisiscono i dati o, nel caso in cui i dati non siano acquisiti direttamente dall'interessato, entro un tempo congruo che il GDPR indica in un mese o comunque non oltre la comunicazione degli stessi all'esterno o la prima comunicazione del Fondo con l'interessato (v. art. 14, par. 3). Ciò significa che nel caso in cui un Fondo pensione riceva un'adesione silente o un'adesione

contrattuale, lo stesso deve fornire all'interessato l'informativa contestualmente all'invio della lettera di benvenuto che deve avvenire non oltre un mese dall'acquisizione dei dati.

È importante che l'informativa sia **chiara, concisa, trasparente, intelligibile**; che sia idonea a fornire informazioni specifiche sul trattamento che viene effettivamente svolto dal Fondo pensione.

Il Fondo Pensione spesso si trova a dover comunicare i dati personali degli iscritti a soggetti esterni alla propria struttura (ad esempio qualora usufruisca di un *service* amministrativo). In questi casi deve nominare tali soggetti quali **Responsabili esterni** attraverso apposito contratto. Della comunicazione dei dati a soggetti diversi dal Titolare deve essere data idonea notizia nell'informativa e, su richiesta dell'interessato, il Fondo pensione deve essere in grado di fornire un elenco completo dei Responsabili esterni del trattamento cui i dati vengono comunicati.

Qualora un soggetto cessi il proprio rapporto con il Fondo pensione (riscatti o trasferisca la propria posizione) ha **diritto di richiedere la cancellazione dei propri dati dagli archivi del Fondo Pensione** e di ottenerla senza ritardo (art. 17, par. 1), il Fondo a sua volta è però tenuto alla conservazione di quei dati che potrebbero essere oggetto di accertamento da parte di autorità giudiziaria o tributaria, per il tempo previsto dalle normative specifiche (art. 17, par. 3, lett.b).

Il periodo di conservazione dei dati personali o, se non è possibile individuarlo, i criteri utilizzati per determinare tale periodo devono essere indicati esplicitamente nell'informativa.