Studio Magnolo
Viale Italia, 35/C - 73046 Matino (Le)

LE NUOVE REGOLE PRIVACY

Dopo **due anni** dalla sua entrata in vigore, il **25 maggio 2018** il Regolamento UE n. 2016/679 diventerà pienamente **applicabile**.

A livello **nazionale**, sebbene non sia stato necessario alcun atto di recepimento (essendo il Regolamento, come noto, un atto tipico dell'Unione Europea **direttamente vincolante per i cittadini**), l'articolo 13 L. 163/2017 ha delegato il Governo ad adottare uno o più **decreti legislativi** al fine di adeguare il quadro normativo nazionale alle disposizioni del richiamato Regolamento UE n. 2016/679.

Più precisamente, il Governo, con i previsti decreti delegati avrebbe dovuto **abrogare** espressamente le **disposizioni** del **codice privacy** (D.Lgs. 196/2003) **incompatibili** con il **Regolamento UE**, **coordinando le norme vigenti** e adeguando il **sistema sanzionatorio** penale e amministrativo.

Il **21 marzo** sorso, tuttavia, il Consiglio dei Ministri ha approvato, in esame preliminare, un decreto legislativo che addirittura prevede la totale **abrogazione** del ***codice privacy***: scelta questa, che, se effettivamente operata, sarebbe quantomeno **criticabile**, se non da ritenersi addirittura **incostituzionale** per **eccesso di delega**, e che cancella venti anni della nostra **storia**.

Tutto quanto premesso, analizziamo quindi le disposizioni previste dal nuovo **Regolamento Privacy**, concentrandoci, con questo primo contributo, sugli aspetti generali.

L'**articolo 1** del Regolamento, rubricato "***Oggetto e finalità***" precisa che ad essere protetti sono solo i diritti e le libertà fondamentali delle **persone fisiche**;
il Regolamento **non trova quindi applicazione** quando i dati si riferiscono ad una **persona giuridica**.

Il Regolamento trova inoltre applicazione esclusivamente nell'ambito delle **attività commerciali** e **professionali**; al contrario, non è necessario rispettare le disposizioni che andremo ad analizzare quando il **trattamento dei dati** è effettuato da una **persona fisica** in **ambito personale** o **domestico**, oppure quando il trattamento dei dati è effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (articolo 2 Regolamento 2016/679).
Definiti quindi l'oggetto e l'ambito di applicazione, il Regolamento si occupa, all'**articolo 4**, degli aspetti definitori, chiarendo che **"dato personale"** è "*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*".

Magnolo Dr. Rag. Cosimo Tel. 0833.593605-Fax 0833.593605 P.Iva 02484570755
Commercialista e.mail: studiomagnolo.commercialisti@pec.it C.F. MGNCSM62H03L074J
Revisore Legale studiomagnolo@gmail.com www.studiomagnolo.com

Tutto quanto premesso, quindi, l'articolo 5 Regolamento 2016/679 (rubricato "***Principi applicabili al trattamento di dati personali***") stabilisce che i **dati personali** devono essere:

1. **trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato;
2. **raccolti per finalità determinate**, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
3. **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esatti** e, se necessario, **aggiornati**; devono quindi essere adottate tutte le misure ragionevoli per **cancellare o rettificare tempestivamente** i dati inesatti rispetto alle finalità per le quali sono trattati;
5. **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**;
6. 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**.

Si precisa che, ai sensi del successivo articolo 6 Regolamento 679/2016, il trattamento è **lecito** e rispetta quindi le condizioni di cui al precedente punto *sub a)* - solo se l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità oppure:
1. 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;
2. il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il **titolare del trattamento**;
3. il trattamento è necessario per la salvaguardia degli **interessi vitali dell'interessato** o di un'altra persona fisica;
4. 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;
5. il trattamento è necessario per il perseguimento del **legittimo interesse del titolare** del trattamento o di terzi. A differenza del passato il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare. Trova così espressione il nuovo principio di "**responsabilizzazione**".
Tranne qualche piccola differenza, già segnalata, possiamo ritenere che vi sia una sostanziale continuità tra le **ipotesi di liceità** del trattamento previste dal ***codice privacy*** e quelle richiamate dal **Regolamento**.

E' tuttavia da precisare che nel caso in cui il trattamento riguardi **dati sensibili**, l'articolo **9 Regolamento** richiede che l'interessato presti il suo **consenso "esplicito"**. Parimenti, l'**articolo 22 Regolamento** precisa che uno dei presupposti legittimanti le decisioni basate unicamente sul trattamento automatizzato, compresa la **profilazione**, è il **consenso "esplicito"** dell'interessato.
Come pare evidente il consenso non deve essere fornito per iscritto, sebbene la **forma scritta** sia l'unica a garantirne l'**inequivocabilità**.

Inoltre, come chiarisce l'articolo 7 Regolamento 679/2016 "*se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda* ***anche altre questioni****, la richiesta di consenso è presentata* ***in***

***modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un **linguaggio semplice e chiaro**".*
Con specifico riferimento agli **intermediari fiscali**, i dati sensibili con i quali questi ultimi più frequentemente si confrontano sono, ad esempio, le **scelte per la destinazione dell'8 del 5 e del 2 per mille**.

Si ricorda, a tal proposito, che il frontespizio della dichiarazione **Redditi PF** riporta l'informativa sul trattamento dei dati personali ai sensi dell'articolo 13 D.Lgs. 196/2003, prevendo che gli intermediari, "*per la sola attività di trasmissione, secondo quanto previsto dal d.lgs. n. 196/2003, assumono la qualifica di "**titolare del trattamento dei dati personali**" quando i dati **entrano nella loro disponibilità** e **sotto il loro diretto controllo**".*

Inoltre, per quanto riguarda i **dati sensibili** "*il **consenso per il trattamento da parte degli intermediari** viene acquisito attraverso la **sottoscrizione della dichiarazione** e con la firma apposta per la scelta dell'otto per mille dell'Irpef, del cinque per mille e del due per mille dell'Irpef*".

Avuto riguardo, invece, alle **altre fattispecie**, giova precisare che il **consenso** raccolto precedentemente al **25 maggio 2018** resta valido se ha tutte le caratteristiche appena richiamate*;*
*"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** (art. 7.2), **per esempio all'interno di modulistica**.*
*Prestare attenzione alla formula utilizzata per chiedere il consenso: **deve essere comprensibile, semplice, chiara** (art. 7.2)*"
(Garante Privacy, Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali).
Come noto, se i dati che lo riguardano sono raccolti presso l'**interessato**, il **titolare del trattamento** deve fornire allo stesso, **nel momento in cui i dati personali sono ottenuti**, specifiche **informazioni** (c.d. "**obbligo di informativa"**).
Più precisamente, l'**articolo 13 Regolamento UE 2016/679** indica le seguenti **informazioni da fornire**:

1. l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo **rappresentante**;
2. i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;
3. le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica del trattamento**. Si precisa che, ogni volta che le **finalità cambiano**, è necessario informarne l'interessato prima di procedere all'ulteriore trattamento;
4. qualora il trattamento sia legittimato dal necessario perseguimento del **legittimo interesse del titolare** del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
5. gli eventuali **destinatari** o le eventuali **categorie di destinatari dei dati personali**;

6. ove applicabile, 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.

Come può notarsi, il **Regolamento** impone **più ampie informazioni** rispetto all'attuale **codice privacy**.

Ed infatti, come anche indicato nella recente guida del **Garante privacy**, il **titolare** deve sempre indicare i dati di contatto del **Responsabile della protezione dei dati** (ovviamente solo se previsto) nonché la **base giuridica del trattamento**.

Il Regolamento, inoltre, prevede alcune **ulteriori informazioni**, da fornire per garantire un **trattamento corretto e trasparente**:

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

Pertanto, è opportuno che "*i **titolari di trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati**, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da **apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento***"

In considerazione del maggior numero di informazioni che dovranno essere fornite, si ritiene pertanto necessario adeguare sempre l'informativa già fornita ai clienti dello studio prima del 25 maggio 2018.

Allo stesso modo, si renderebbe opportuna una modifica, da parte dell'**Agenzia delle entrate**, dell'**informativa privacy** fornita nel modello **Redditi2018**.

Ai sensi dell'**articolo 12 Regolamento UE n. 2016/679**, tutte le richiamate informazioni devono essere fornite in **forma scritta** e in **maniera coincisa**, trasparente, e con un **linguaggio semplice e chiaro**.

Se richiesto dall'interessato, le informazioni possono essere **fornite oralmente**, purché sia comprovata con altri mezzi l'**identità dell'interessato**.

Si ricorda, infine, che nel caso in cui i dati non siano stati raccolti presso l'interessato, le informazioni da fornire allo stesso sono **diverse** e **più ampie**, così come specificato dall'**articolo 14 Regolamento UE n. 2016/679**.

Il nuovo **Regolamento privacy** prevede, come in passato, le figure del **titolare del trattamento** e del **responsabile del trattamento**, definendone, in maniera ancora più precisa, i compiti.

Una nuova figura, prima non prevista, è invece quella del **Responsabile per la protezione dei dati** (**RPD**, o anche **Data Protection Officer – DPO**): si sottolinea, pertanto, che il **responsabile del trattamento** e l'**RPD-DPO** sono due figure distinte.

Il **responsabile del trattamento** (**articolo 28 Regolamento UE**), infatti, continua ad essere colui che tratta i dati **per conto del titolare**.

A differenza del passato, però, quando l'**unico** soggetto ad essere **obbligato** al rispetto delle norme privacy era il **titolare** (in quanto gli obblighi del **responsabile** erano meramente **contrattuali**, in funzione di quanto contrattualmente stabilito con il titolare), oggi il **responsabile del trattamento** è destinatario di **specifici obblighi**, come, ad esempio, la tenuta del **registro dei trattamenti svolti** ai sensi dell'**articolo 30, par. 2, Regolamento**; l'adozione di idonee **misure**

tecniche e organizzative per garantire la sicurezza dei trattamenti (ai sensi dell'**articolo 32 Regolamento**); la **designazione di un RPD-DPO.**

Il **responsabile del trattamento** deve essere designato con un **contratto** nel quale dovranno essere disciplinate tassativamente le materie indicate nell'**articolo 28**, **par. 3, Regolamento.**

Il **contratto**, pertanto, deve prevedere, tra l'altro, che il **responsabile del trattamento**, tenendo conto della natura del trattamento, assista il **titolare** del trattamento con **misure tecniche e organizzative adeguate** per dare seguito alle richieste per l'esercizio dei diritti dell'interessato ed **assista il titolare del trattamento** nel garantire il **rispetto** degli obblighi di cui agli **articoli da 32 a 36 del Regolamento**.

Tutto quanto premesso, si rende quindi necessario, per i **titolari di trattamento**, **verificare che i contratti o gli altri atti che attualmente disciplinano i rapporti con i responsabili siano conformi a quanto appena richiamato**.

In caso contrario, dovranno essere apportate le necessarie integrazioni o modifiche.

È inoltre opportuno soffermare l'attenzione su quella che è la vera novità del Regolamento *privacy*: il nuovo **principio di "*responsabilizzazione*"** ("***accountability***").

I **titolari** e i **responsabili** devono infatti adottare comportamenti idonei a dimostrare la concreta applicazione del Regolamento, potendo tuttavia decidere in **autonomia** le modalità, le garanzie e i limiti del **trattamento dei dati**, prevedendo fin dall'inizio le **garanzie indispensabili** per la **tutela dei diritti degli interessati** e il **rispetto del Regolamento** (criterio, questo, che viene spesso **sintetizzato** con l'espressione inglese "***data protection by default and by design***" **– articolo 25 Regolamento UE 679/2016**).

Altra importante novità è poi contenuta nell'**articolo 26 Regolamento UE 679/2016** e riguarda la **contitolarità del trattamento**.

Si parla di contitolarità dei dati quando "***due o più titolari*** *del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*".

Si pensi, a mero titolo di **esempio**, al medico specialista che opera all'interno della struttura sanitaria, la quale archivia i dati del paziente: questo è un caso di **contitolarità del trattamento**.

I contitolari devono determinare in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal **Regolamento privacy**, con particolare riguardo all'esercizio dei **diritti dell'interessato**.

Tutto ciò premesso, quindi, è sempre necessario valutare l'**esistenza di situazioni di contitolarità**, **rendendosi in questo caso necessario il richiamato accordo interno**.

Il **principio di "*responsabilizzazione*"** che, come abbiamo detto, ispira la disciplina europea in materia di privacy, trova espressione anche nella previsione della nuova figura del "***responsabile***

della protezione dati" (**RPD**, ovvero **DPO** se si utilizza l'acronimo inglese *Data Protection Officer*).

L'**RPD assiste** il titolare del trattamento e il responsabile, **garantendo** che il trattamento dei dati sia effettuato conformemente alle previsioni del **Regolamento**; nello specifico, i compiti dell'**RDP** sono dettagliati nell'**articolo 39 Regolamento** e vanno dall'**attività di informazione** e **consulenza**, alla **vigilanza** e alla **cooperazione** con le Autorità di controllo.

L'**RPD** deve essere **obbligatoriamente nominato** solo al ricorrere delle specifiche **cause** previste dall'**articolo 37 del Regolamento**, ovvero **quando:**

1. il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccetto le autorità giurisdizionali quando esercitano le loro **funzioni giurisdizionali**;
2. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli **interessati** su larga scala; oppure
3. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali** o di dati relativi a **condanne penali** e a **reati**.

Per la protezione dei dati" **sono quindi tenuti alla nomina di un RDP,** 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; società che erogano servizi televisivi a pagamento.

La designazione del responsabile del trattamento **non è** invece **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.

Anche ove il Regolamento **non imponga** in modo specifico la **designazione** di un RPD, può tuttavia risultare utile procedere a tale designazione su base **volontaria**;

Il ruolo di **responsabile della protezione dei dati personali** può 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 e che, soprattutto, possieda un'**approfondita conoscenza** della normativa e delle prassi in materia di **privacy**.

Alternativamente, l'incarico può essere anche affidato a **soggetti esterni**, a condizione che garantiscano l'effettivo assolvimento dei compiti assegnati a tale figura dal Regolamento.

A tal proposito giova inoltre precisare che uno **stesso RPD** può svolgere le sue funzioni per conto di **più titolari**.

Il **responsabile della protezione dei dati**, in tutti i casi, dovrà operare sulla base di un atto in **forma scritta,** nel quale dovranno essere dettagliati i **compiti attribuiti** e le **risorse assegnate**. Più precisamente, il **responsabile della protezione dei dati**:

- dovrà essere nominato mediante **specifico atto di designazione** se è stato scelto all'interno (si segnala, a tal proposito, che è già disponibile sul sito del Garante uno **schema di atto di designazione**),
- dovrà operare in base a un **contratto di servizi** se è stato individuato in un soggetto esterno.

I **dati di contatto** del responsabile designato dovranno essere inoltre **pubblicati** dal titolare o responsabile del trattamento; **non è invece necessario** (sebbene sia comunque consigliato) pubblicare il **nominativo** del responsabile della protezione dei dati.

"***I RPD non rispondono personalmente in caso di inosservanza del RGPD***. *Quest'ultimo chiarisce che spetta al* ***titolare del trattamento*** *o al* ***responsabile del trattamento*** *garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1).*

L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento".

Il **Regolamento europeo**, introducendo il nuovo **principio di "responsabilizzazione"** (o "***accountability***"), richiede la concreta adozione, da parte del titolare e dei responsabili, di **misure di sicurezza** appropriate per il rispetto del regolamento stesso.

I **titolari**, pertanto, devono svolgere una serie di specifiche **attività preventive (dimostrabili)**, tenendo conto del **rischio inerente al trattamento** (ovvero il **rischio di impatti negativi** sulle libertà e i diritti degli interessati).

Il **rischio inerente al trattamento** deve quindi essere preventivamente **valutato**, individuando le misure tecniche e organizzative idonee a **mitigare tali rischi**: più precisamente, l'**articolo 35 Regolamento UE 2016/679** impone una "**valutazione dell'impatto dei trattamenti**" (o "***Data Protection Impact Assessment***" – **DPIA**), la quale **non** è tuttavia **obbligatoria** in ogni caso.

Le Linee guida "***Data Protection Impact Assessment***" propongono pertanto alcuni criteri utili per l'individuazione delle attività soggette alla **DPIA**.

In generale "*fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione,* ***è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato"***".

Sul punto giova tra l'altro precisare che l'**articolo 35 del Regolamento** fornisce alcuni **esempi** di casi nei quali un trattamento "***possa presentare rischi elevati***":

"a) una ***valutazione sistematica e globale di aspetti personali*** *relativi a persone fisiche, basata su un* ***trattamento automatizzato****, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) il ***trattamento****, su larga scala, di* ***categorie particolari di dati personali*** *di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*

c) la ***sorveglianza sistematica su larga scala di una zona accessibile al pubblico***".

Nel caso in cui sia obbligatoria una **valutazione d'impatto sulla protezione dei dati**, quest'ultima, ai sensi dell'**articolo 36, dovrà contenere almeno**:

1. una **descrizione** sistematica dei **trattamenti** previsti e delle **finalità del trattamento**, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
2. una valutazione della **necessità** e **proporzionalità** dei **trattamenti** in relazione alle **finalità**;
3. una **valutazione dei rischi** per i diritti e le libertà degli interessati;
4. le **misure** previste per **affrontare i rischi**, includendo le **garanzie**, le **misure di sicurezza** e i **meccanismi** per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Solo se le **misure** adottate sono idonee a **mitigare il rischio** potrà avvenire il **trattamento dei dati**; alternativamente sarà necessario consultare l'**autorità di controllo** competente per ottenere indicazioni su **come gestire il rischio residuale**.

L'Autorità, pur **non** avendo il potere di "**autorizzare**" il trattamento, potrà indicare le **misure ulteriori** che il titolare può implementare.

Come può desumersi, pertanto, il nuovo **principio di responsabilizzazione** prevede un intervento dell'**Autorità** solo ***ex-post***; non è invece prevista come in passato, la notifica preventiva dei trattamenti all'autorità di controllo.

I registri delle attività di trattamento

Un ulteriore adempimento imposto dalla nuova disciplina privacy è rappresentato dall'obbligo di **tenuta dei registri delle attività di trattamento**, di cui all'**articolo 30 Regolamento.**

È in primo luogo necessario premettere che i **Registri dei trattamenti** non devono essere tenuti dagli **organismi con meno di 250 dipendenti**, **a meno che il trattamento da effettuare**:

- presenti un **rischio per i diritti e le libertà dell'interessato**,
- **non sia occasionale**,

oppure

- includa il trattamento di **categorie particolari di dati** di cui all'**articolo 9** (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) o i **dati personali relativi a condanne penali e a reati** di cui all'**articolo 10**.

Il primo registro (**registro delle attività di trattamento**) deve essere tenuto da ogni **titolare** o dal suo **rappresentante** e deve contenere tutte le seguenti **informazioni**:

1. 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;
2. le **finalità del trattamento**;
3. una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
4. le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. 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;
6. ove possibile, i **termini** ultimi **previsti** per la **cancellazione** delle diverse categorie di dati;
7. ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'**articolo 32**, paragrafo 1.

Come detto, la compilazione dell'appena richiamato registro è demandata al titolare del trattamento; il Regolamento prevede poi un **ulteriore registro** la cui **compilazione** è richiesta al **responsabile del trattamento**, il quale, appunto, deve tenere un **registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento**, contenente:

1. 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**;
2. le **categorie dei trattamenti effettuati** per conto di ogni titolare del trattamento;
3. ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'**organizzazione internazionale**, compresa l'identificazione del paese terzo o

4. dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
5. ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative** di cui all'**articolo 32 Regolamento**.

Entrambi i registri devono essere **tenuti in forma scritta**, anche in formato elettronico, e devono essere **esibiti su richiesta al Garante**.

Il Garante, ha precisato che il **registro dei trattamenti** non costituisce un mero adempimento formale, ma "***parte integrante di un sistema di corretta gestione dei dati personali***. *Per tale motivo, si invitano* ***tutti i titolari di trattamento e i responsabili****, 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 – ove già non condotta*".

Le misure di sicurezza

Il **D.Lgs. 196/2003** prevedeva "**misure minime**" e "**misure idonee**" al fine di garantire la **sicurezza** dei dati personali.

Il nuovo **Regolamento privacy** abbandona questa previsione, soprattutto in considerazione della circostanza che la rapida evoluzione delle tecnologie **non** consente di individuare **preventivamente** le misure necessarie per garantire la **protezione dei dati**.

Ecco il motivo per il quale, in ossequio al più generale **principio di responsabilizzazione**, non sono state previste **misure minime di sicurezza**, preferendo invece attribuire ai **titolari** e ai **responsabili** del trattamento l'onere di individuare le **misure di sicurezza più idonee**.

L'**articolo 32**, pertanto, propone un semplice **elenco** di **misure di sicurezza adottabili**, lasciando tuttavia spazio anche a **soluzioni alternative** più adeguate in considerazione del **rischio nel trattamento dei dati**.

Tra gli esempi proposti di "**misure tecniche e organizzative adeguate**" assume particolare rilevanza la c.d. "**pseudonimizzazione**", ovvero 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***".

LÌ, 27 APRILE 2018