Sommario

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

LE NUOVE REGOLE PRIVACY

Come noto, la disciplina in materia di Privacy è contenuta nel D.Lgs n. 196/2003. Con il regolamento 24/04/2016, n. 679 (**GDPR**) il Legislatore comunitario ha "uniformato" la disciplina in esame applicabile negli Stati membri **a decorrere dal 25/05/2018**.
A livello nazionale, sebbene non sia stato necessario alcun atto di recepimento, essendo il Regolamento un atto tipico dell'Unione Europea direttamente vincolante per i cittadini, l'articolo 13 della Legge n. 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.
L'armonizzazione dei principi su tutto il territorio comunitario e l'obbligo per i soggetti che tratteranno dati dei cittadini comunitari di adeguarsi ai dettami del Regolamento, si prefigge lo scopo di eliminare le lacune di protezione che incombevano sui dati allorquando questi ultimi circolavano tra i diversi titolari.
In ragione di quanto sopra esposto è importate comprendere le definizioni di quanto la nuova normativa regolamenta.

DEFINIZIONI

Dato personale	**Qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "*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.
Trattamento	**Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali** o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare del trattamento	**La persona fisica o giuridica**, l'Autorità pubblica, il servizio o altro organismo **che**, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	**La persona fisica o giuridica**, l'Autorità pubblica, il servizio o altro organismo **che tratta dati personali per conto del titolare del**

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

	trattamento.
Consenso dell'interessato	**Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato**, con la quale lo stesso **manifesta** il proprio **assenso**, mediante dichiarazione o azione positiva inequivocabile, **che i dati personali che lo riguardano siano oggetto di trattamento**.
Violazione dei dati personali	**La violazione di sicurezza che comporta** accidentalmente o in modo illecito la **distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati**.
Dati genetici	I **dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica** che forniscono informazioni univoche **sulla fisiologia o sulla salute di detta persona fisica**, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici	I **dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica** che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I **dati personali attinenti alla salute fisica o mentale di una persona fisica**, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Archivio	**Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati**, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Pseudonimizzazione	Il **trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico** senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuibili a una persona fisica identificata o identificabile.
Destinatario	La **persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali**, che si tratti o meno di terzi.

AMBITO DI APPLICAZIONE

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: è evidente che in tal caso le disposizioni del GDPR troveranno applicazione con riferimento al trattamento dei dati personali del rappresentante legale.

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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).

Quanto all'ambito di **applicazione territoriale**, il par. 1 dell'art. 3 accoglie come criterio generale il cd. ***principio di stabilimento***. Di conseguenza, **il regolamento si applica ai trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento stabiliti nel territorio dell'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 cui si riferiscono i dati personali trattati**.
Ulteriormente, il par. 2 dell'art. 3 del **GDPR rende vincolanti le sue norme anche al trattamento effettuato da titolari del trattamento e responsabili del trattamento non stabiliti nell'Unione europea**, in due casi:

a) **quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi nell'Unione europea**, indipendentemente dall'obbligatorietà di un pagamento da parte dell'interessato;
b) **quando il trattamento è riferito al monitoraggio (controllo) del comportamento degli interessati** nella misura in cui tale comportamento ha luogo all'interno dell'Unione europea.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

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 SOLO SE L'INTERESSATO HA ESPRESSO IL CONSENSO AL TRATTAMENTO DEI PROPRI DATI PERSONALI PER UNA O PIÙ SPECIFICHE FINALITÀ OPPURE se**:

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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"**.

E' tuttavia da precisare che **nel caso in cui il trattamento riguardi DATI SENSIBILI (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)**, l'articolo 9 Regolamento richiede che l'interessato presti il suo **CONSENSO "ESPLICITO"**.

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***".

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)**.

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:

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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**. **N.B.: 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".

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

FIGURE DEL TRATTAMENTO

Per consentire un'efficace catena di protezione del dato personale durante le attività di trattamento È NECESSARIO PROCEDERE AD **UN TRACCIAMENTO DELLA CATENA DI CUSTODIA E UTILIZZO DELL'INFORMAZIONE ATTRAVERSO LA DEFINIZIONE DI RUOLI E COMPITI ALL'INTERNO DELLA STRUTTURA DEL TITOLARE**.
In quest'ottica, il D.Lgs. n. 196/2003 (vecchia normativa privacy) aveva già introdotto L'OBBLIGO DI INDIVIDUARE L'ORGANIGRAMMA DEI SOGGETTI COINVOLTI NELLE ATTIVITÀ DI TRATTAMENTO DEL DATO.
Principalmente la struttura si fondava sulle figure del Titolare, del Responsabile (interno od esterno) e degli Incaricati.
A differenza di quanto previsto dal D.Lgs. n. 196/2003 che assegnava formalmente un ruolo all'Incaricato, la nuova disciplina del Regolamento UE n. 679/2016 fa riferimento a **"CHIUNQUE AGISCA SOTTO LA RESPONSABILITÀ" DEL TITOLARE O DEL RESPONSABILE o alle "PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI SOTTO L'AUTORITÀ DIRETTA DEL TITOLARE O DEL RESPONSABILE" è tuttavia stato chiarito che IL PERSONALE DIPENDENTE PUÒ ACCEDERE E TRATTARE I DATI SOLO SE HA RICEVUTO UN INQUADRAMENTO FORMALE E SOLO ENTRO I LIMITI DELLE ISTRUZIONI RICEVUTE.**
Per quel che riguarda la figura del **Responsabile del trattamento**, come sopra accennato, l'art. 4, par. 8, Regolamento UE n. 679/2016 lo definisce **"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"**.
La prassi italiana, fino ad ora, ha sempre individuato la figura del responsabile interno e quella del responsabile esterno del trattamento.
Questa impostazione non sembra trovare continuità nel Regolamento UE n. 679/2016 che sostanzialmente divide nettamente i ruoli interni (soggetti autorizzati) da quelli esterni (responsabili) all'organizzazione del Titolare.

IL RESPONSABILE DEL TRATTAMENTO DEI DATI

È designato dal Titolare del trattamento, tramite contratto nel quale dovranno essere specificate tassativamente almeno le materie di cui all'art. 28, par. 3, Regolamento UE n. 679/2016. Allo stesso sono imputabili specifici obblighi distinti da quelli di pertinenza del Titolare.
In particolare deve:

- tenere il Registro dei trattamenti svolti (**N.B.:** non richiesto per i soggetti con meno di 250 dipendenti che non effettuano "trattamenti a rischio" ex art. 30, par. 5, Regolamento UE n. 679/2016) contenente un quadro aggiornato dei trattamenti in essere all'interno dell'azienda "*indispensabile per ogni valutazione e analisi del rischio*";
- adottare misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
- designare, nel caso in cui sia necessario, il Responsabile per la protezione dei dati (RPD / Data Protection Officer – DPO).

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

Rappresenta una nuova figura non prevista dalla previgente disciplina, finalizzata a facilitare l'attuazione della disciplina in materia di Privacy da parte del Titolare / Responsabile.

Il RPD assolve funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento UE n. 679/2016.

È una figura obbligatoria per i soggetti le cui attività consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o un trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

Come desumibile dalle specifiche FAQ disponibili sul sito Internet del Garante della Privacy (www.garanteprivacy.it), sono tenuti alla normativa, ad esempio: istituti di credito, imprese assicurative, società finanziarie, società di revisione controllo, CAF e patronati, società operanti nel settore della cura della salute, della prevenzione / diagnostica / diagnostico sanitaria.

Lo stesso Garante specifica che nei casi diversi da quelli sopra richiamati, la designazione del RPD non è obbligatoria (ciò si riscontra, ad esempio, in relazione ai trattamenti effettuati da liberi professionisti operanti in forma individuale, agenti / rappresentanti / mediatori operanti non su larga scala, imprese individuali / familiari / piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti).

Il ruolo di RPD può essere ricoperto da un dipendente del Titolare o del Responsabile (non in conflitto di interessi) che conosce la realtà operativa in cui avvengono i trattamenti; **L'incarico può essere affidato anche a soggetti esterni**, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento UE n. 679/2016 assegna a tale figura.

DIRITTI DEGLI INTERESSATI

Diritto di accesso dell'interessato (art. 15)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

Diritto di rettifica (art. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione (diritto all'oblio) (art. 17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento;
d) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
e) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Diritto di limitazione di trattamento (art. 18)

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto alla portabilità dei dati (art. 20)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento.

Diritto di opposizione (art. 21)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

APPROCCIO BASATO SUL RISCHIO E PRINCIPIO DI ACCONTABILITY

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.

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

I titolari, pertanto, **devono svolgere una serie di specifiche attività preventive (privacy by design) dimostrabili, tenendo conto del rischio inerente al trattamento** (ovvero il rischio di impatti negativi sulle libertà e i diritti degli interessati).
Devono inoltre essere messe in atto **MISURE ADEGUATE affinché i dati personali necessari per ogni specifica finalità del trattamento siano trattati, per impostazione predefinita (protezione di defalut), solo i dati personali necessari per ogni specifica finalità del trattamento**.
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, (*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 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.

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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**.

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 **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.

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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 dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
4. 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, nelle sue recenti linee guida ha inoltre 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***".

Il D.Lgs. 196/2003 prevedeva e pretendeva "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

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

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".

IL REGIME SANZIONATORIO

L'art. 83, par. 3 e 4, Regolamento UE n. 679/2016 prevede **2 distinte categorie di sanzioni amministrative pecuniarie a seconda della natura della violazione**. In particolare, sono previste le seguenti sanzioni:

- **fino al 2% del fatturato dell'esercizio precedente per le sanzioni relative agli obblighi**:
  - del Titolare / Responsabile del trattamento;
  - dell'Organismo di certificazione;
  - dell'Organismo di controllo;
- **fino al 4% del fatturato dell'esercizio precedente per le violazioni relative**:
  - ai principi base del Trattamento, comprese le condizioni di consenso;
  - ai diritti degli Interessati;
  - ai trasferimenti dei dati personali a un destinatario di uno Stato terzo o un'organizzazione internazionale;
  - a qualsiasi obbligo ai sensi della legislazione nazionale adottata a norma del Capo IX;
  - all'inosservanza di un ordine, di una limitazione provvisoria / definitiva di trattamento o di un ordine di sospensione dei flussi di dati all'Autorità di controllo o il negato accesso.

IN SINTESI UN CONFRONTO TRA VECCHIA A NUOVA NORMATIVA

PRIMA (D.Lgs 196/2003)	DOPO (GDPR)
La normativa era applicabile nel luogo in cui aveva sede il Titolare del trattamento dei dati.	La legge applicabile è quella del soggetto i cui dati vengono raccolti.
Erano previste le figure del Titolare del Trattamento dei Dati e del Responsabile.	Con il nuovo regolamento viene abolita la figura del Titolare del Trattamento Dati e rimane solo la figura di Responsabile.
La documentazione (anche formale) era importante.	Ora viene introdotto il principio dell'**accountability** (**responsabilità verificabile**), secondo cui tutti i soggetti che partecipano al trattamento dati devono essere consci e responsabili e devono tenere documentazione di tutti i trattamenti effettuati. Chi non documenta, è soggetto a possibili sanzioni a prescindere dall'utilizzo che si fa dei dati, è sufficiente non avere i documenti per essere perseguibili.
L'informativa era spesso lunga, formale,	L'informativa deve essere leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com

incomprensibile e con richiami normativi complessi.	normativi. Deve essere fornita per iscritto (oralmente va bene SOLO se l'interessato è d'accordo e la sua identità deve comunque essere comprovata con altri mezzi).
PRIMA (D.Lgs 196/2003)	DOPO (GDPR)
Il consenso doveva essere libero, specifico e informato. Ci doveva essere un atto formale per accettare il trattamento dei dati.	Il consenso deve essere libero, specifico, informato e inequivocabile. Il consenso è valido se la volontà è espressa in modo NON equivoco, anche con un'azione positiva: basta un testo in cui si informa che proseguendo si accetta il trattamento dati con link all'informativa.
Si preparava il DPS.	Si effettua una valutazione degli impatti privacy analizzando i rischi, definendo i gap rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando annualmente gli effetti degli interventi per ridurre i rischi. Il nuovo documento sarà denominato **PIA: Privacy Impact Assessment**.
Si doveva informare il Garante che un soggetto sta trattando dati per una particolare finalità. (ex art. 37 D.lgs. 196/2003)	Non si dovrà più notificare il Garante, ma ogni anno l'azienda dovrà redigere il Privacy Impact Assessment, con il quale si considera effettuata la notifica.
Il **Data Protection Officier** (DPO) non era una figura contemplata.	Occorre istituire (per tutti gli enti pubblici e per aziende il cui core business coinvolge trattamenti di natura rischiosa) la figura ed la funzione del **Responsabile per la Protezione dei Dati (DPO).** Il DPO sarà una figura manageriale con rinnovo periodico, sarà referente del Garante e dovrà avere requisiti e competenze elevate. Il DPO potrà essere sia un dipendente che un collaboratore con regolare contratto.
La Privacy era un elemento conclusivo e finale.	La Privacy deve essere vista come un elemento iniziale: occorre affrontare l'argomento appena si decide di raccogliere i dati e predisporre adeguati livelli di privacy nel trattamento dati.
Non era necessario comunicare violazioni nel trattamento dati.	Nel caso di violazione del trattamento dati bisogna effettuare una segnalazione al Garante entro 72 ore dall'evento e, nel più breve tempo possibile, bisogna informare anche i diretti interessati. **Il mancato rispetto di quest'obbligo comporta sanzioni penali**. È possibile prevedere delle assicurazioni per coprire il costo di comunicare la violazione a tutti gli interessati (Data Breach).
Pochi diritti tutelavano l'interessato in merito alla gestione dei suoi dati.	Vengono introdotti nuovi tra i quali il **diritto alla portabilità dei dati** (ora si può pretendere che il soggetto a cui si è concesso l'uso di dati personali li "restituisca" su un supporto elettronico strutturato così che si possa farne ulteriore uso, anche presso un altro soggetto); diritto a essere totalmente dimenticato da chi ha raccolto i miei dati (**Diritto all'Oblio**).

A disposizione per eventuali chiarimenti.

Studio Negri e Associati - Sede Legale Via Balicco, 63 - 23900 LECCO - ITALIA C.F. e P. IVA 02922330135 - tel +39 0341 226911 - fax +39 0341 360544
e-mail studio@negriassociati.com - www.negriassociati.com