Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

Circ. **02/A/180507**

San Fior, lì 07/05/2018

Ai gentili **Clienti**

Loro sedi

OGGETTO: **Nuova disciplina in materia di Protezione dei dati (Privacy - GDPR)**

Introduzione alla nuova privacy ed al relativo regime sanzionatorio

Il 25 maggio 2018 entrerà in vigore la nuova disciplina in materia di Protezione dei dati (Privacy) contenuta nello specifico Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, conosciuto con l'acronimo ***GDPR*** (General Data Protection Regulation).

Per valutare l'impatto che il GDPR avrà su lavoratori autonomi ed imprese è opportuno considerare *in primis* la "***enormità***" delle **sanzioni** previste nei **paragrafi 4, 5 e 6 dell'art. 83**, del GDPR:

- nel par. 4. sono previste sanzioni amministrative pecuniarie **fino a euro 10.000.000** (*non è un errore, sono proprio diecimilioni di euro!*), o per le imprese, **fino al 2 % del fatturato** mondiale totale annuo dell'esercizio precedente, **se superiore**[1], per le violazioni riguardanti:
  a) gli obblighi del titolare del trattamento e del responsabile del trattamento;
  b) gli obblighi dell'organismo di certificazione;
  c) gli obblighi dell'organismo di controllo;
- nel par. 5. sono previste sanzioni amministrative pecuniarie **fino a euro 20.000.000** (*non è un errore, sono proprio ventimilioni di euro!*), o per le imprese, **fino al 4 % del fatturato** mondiale totale annuo dell'esercizio precedente, **se superiore**[2], per le violazioni riguardanti:
  a) i principi di base del trattamento, comprese le condizioni relative al consenso;
  b) i diritti degli interessati;
  c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
  d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
  e) 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 o il negato accesso in violazione dell'articolo 58, paragrafo 1.
- nel par. 6., per l'inosservanza di un ordine da parte dell'autorità di controllo, sono previste sanzioni amministrative pecuniarie **fino a euro 20.000.000**, o per le imprese, **fino al 4 % del fatturato** mondiale totale annuo dell'esercizio precedente, **se superiore**.

[1] Nel prospetto di riepilogo di cui al paragrafo successivo, riportante le disposizioni più importanti, quelle assistite da questa sanzione (euro 10.000.000 / 2%) sono indicate con una faccina triste ☹

[2] Nel prospetto di riepilogo di cui al paragrafo successivo, riportante le disposizioni più importanti, quelle assistite da questa sanzione (euro 20.000.000 / 4%) sono indicate con due faccine tristi ☹☹

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

La disciplina del GDPR è particolarmente corposa e complessa ed è destinata ad entrare in vigore Il 25 maggio 2018 **indipendentemente dall'emanazione di norme nazionali**.

Ad oggi, il Governo ha approvato solo uno ***schema*** di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, che prevede, tra l'altro, a decorrere dall'entrata in vigore dello stesso decreto, l'abrogazione del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Detto decreto non ha certo le caratteristiche di completezza di un "*testo unico*", in quanto contiene continui riferimenti al GDPR; in ogni caso, ai fini della certezza del diritto, sarebbe auspicabile che fosse approvato prima del 25 maggio.

Alcune delle principali disposizioni del GDPR

In questa sede ci si limiterà a sottolineare solo alcune delle principali disposizioni della nuova Privacy.

Nella prima colonna del prospetto che segue, il numero delle ***faccine tristi*** ivi riportate è indicativo della diversa gravità delle sanzioni previste per le violazioni delle singole disposizioni (tenendo presente che anche una sola faccina rappresenta, comunque, il rischio di incorrere in una ***sanzione devastante***!).

A chi non si trovasse nella condizione psicologica ideale per affrontare in questo momento l'*amena* lettura che si propone e si ripromettesse di farlo successivamente, il consiglio spassionato di chi scrive è **quello di leggere subito almeno l'ultima pagina della presente circolare informativa.**

Ambito di applicazione materiale (Articolo 2)	Il regolamento si applica al trattamento interamente o parzialmente automatizzato di **dati personali** e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. Il regolamento non si applica, tra l'altro, ai trattamenti di dati personali: • effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; • effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
Definizioni (Articolo 4)	Ai fini del GDPR s'intende per: - «***dato personale***»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; - «***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; - «***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; - «***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; - «***responsabile del trattamento***»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento; - «***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; - «***rappresentante***»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; - «***impresa***»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica; - «***autorità di controllo***»: l'autorità pubblica indipendente istituita da uno Stato (in Italia, il "*Garante*").
Principi applicabili al trattamento di dati personali	1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

(Articolo 5) ☹☹	c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2. Il ***titolare del trattamento*** è competente per il **rispetto** dei principi sopra elencati e in grado di comprovarlo («responsabilizzazione»).
Liceità del trattamento (Articolo 6) ☹☹	1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) 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; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) 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; f) 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.
Condizioni per il consenso (Articolo 7) ☹☹	1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. 2. 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. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante. 3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revocadel consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

	consenso è revocato con la stessa facilità con cui è accordato. 4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (Articolo 8) ☹	1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di **servizi della società dell'informazione** (c.f.r.: qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi) **ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni.** Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
Trattamento di categorie particolari di dati personali (Articolo 9) ☹☹	1. **È vietato trattare dati personali** che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato **ha prestato il proprio consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche; b) il trattamento è necessario 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per 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; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

	giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. 3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.
Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (Articolo 12) ☹☹	1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le **informazioni** … e le comunicazioni … relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. **Le informazioni sono fornite per iscritto** o con altri mezzi, anche, se del caso, con mezzi elettronici. **Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato**. 2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ….
Informazioni da	1. In caso di raccolta **presso l'interessato** di dati che lo riguardano, il titolare del

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

fornire qualora i dati personali siano raccolti presso l'interessato (Articolo 13) ☹☹	trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni: a) **l'identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante; b) **i dati di contatto del responsabile della protezione dei dati**, ove applicabile; c) le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica** del trattamento; d) i legittimi interessi perseguiti dal titolare del trattamento o da terzi (nell'ipotesi di cui all'articolo 6, paragrafo 1, lettera f); e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale …. 2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il **titolare** del trattamento fornisce all'**interessato** le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) 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; c) qualora il trattamento sia basato consenso esplicito (articolo 6, paragrafo 1, lettera a) ed articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di **revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) **l'esistenza del diritto di proporre reclamo** a un'autorità di controllo; e) **l'esistenza del diritto** di sapere se la **comunicazione** di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto e se esista l'**obbligo** di fornire i dati personali **nonché le possibili conseguenze della mancata comunicazione di tali dati**; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione .... 3. 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 di cui al paragrafo 2. 4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.
Informazioni da fornire qualora i dati personali non siano stati ottenuti presso	Anche qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento ha l'obbligo di fornirgli informazioni similari a quelle *ut supra*, tra cui la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico: a) entro un termine ragionevole dall'ottenimento dei dati personali, **ma al più tardi**

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

l'interessato (Articolo 14) ☹☹	**entro un mese** …..; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; c) oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. L'informativa non è necessaria se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento …; d) i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale .., compreso un obbligo di segretezza previsto per legge.
Diritto di accesso dell'interessato (Articolo 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 agli stessi, all'informativa, ecc…
Diritto di rettifica (Articolo 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») (Articolo 17) ☹☹	1. 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 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** … e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, ..; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un **obbligo legale** ..; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
Diritto di limitazione di trattamento (Articolo 18) ☹☹	L'interessato ha il diritto di ottenere dal titolare del trattamento **la limitazione** del trattamento quando ricorre una delle ipotesi previste.

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (Articolo 19) ☹☹	Il titolare del trattamento comunica a ciascuno dei **destinatari** cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.
Diritto alla portabilità dei dati (Articolo 20) ☹☹	1. 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 cui li ha forniti qualora: a) il trattamento si basi sul consenso .. o su un contratto .. e b) il trattamento sia effettuato con mezzi automatizzati.
Diritto di opposizione (Articolo 21) ☹☹	1. 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 ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. 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. 2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
Responsabilità del titolare del trattamento (Articolo 24)	1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di **protezione dei dati** da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
Contitolari del	1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

trattamento (Articolo 26) ☹	i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento.
Responsabile del trattamento (Articolo 28) ☹	Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
Registri delle attività di trattamento (Articolo 30) ☹	1. Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un registro delle **attività di trattamento** svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del **titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del **responsabile della protezione dei dati**; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, …; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, ..; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, ….; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico. 4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo. 5. **Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni**

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

	con meno di 250 dipendenti, a meno che - il trattamento che esse effettuano **possa presentare un rischio** per i diritti e le libertà dell'interessato, - il trattamento **non sia occasionale** o includa il trattamento di: • categorie particolari di dati che rivelino **l'origine razziale o etnica**, le **opinioni politiche**, le convinzioni **religiose** o filosofiche, o l'appartenenza **sindacale**, nonché trattare dati **genetici**, **dati biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla **salute o alla vita sessuale** (articolo 9, paragrafo 1) • o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.
Sicurezza del trattamento (Articolo 32) ☹	1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, la pseudonimizzazione e la cifratura dei dati personali, ecc…. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento.
Notifica di una violazione dei dati personali all'autorità di controllo (Articolo 33) ☹	1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
Comunicazione di una violazione dei dati personali all'interessato	1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

(Articolo 34) ☹	con un linguaggio semplice e chiaro la natura della violazione dei dati personali …. 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la **cifratura**; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
Valutazione d'impatto sulla protezione dei dati (Articolo 35) ☹	1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti** sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
Designazione del responsabile della protezione dei dati (Articolo 37) ☹	1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un **responsabile della protezione dei dati** ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) 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; c) oppure, le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. 5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39. 6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
Posizione del responsabile	1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

della protezione dei dati (Articolo 38) ☹	in tutte le questioni riguardanti la protezione dei dati personali.
Compiti del responsabile della protezione dei dati (Articolo 39) ☹	1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
Diritto di proporre reclamo all'autorità di controllo (Articolo 77)	1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. 2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.
Diritto al risarcimento e responsabilità (Articolo 82)	1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presenteregolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Prof. Dott. Giandomenico Andreetta
Dottore Commercialista e Revisore Contabile

Dr.ssa Alessandra Gava
Dottore Commercialista

Dr.ssa Cristina Vecellio Segate
Dottore Commercialista

Dr.ssa Paola Brunetta
Dottore in Economia e Commercio

STUDIO
ANDREETTA & ASSOCIATI
Dottori commercialisti e Revisori contabili

Il decalogo da rispettare per evitare le mostruose sanzioni previste dal GDPR

Fermo restando che non è possibile in questa sede fornire una ricetta valevole in tutti i casi, per evitare di trovarsi impreparati alla data del 25 maggio p.v., il **buon senso** suggerisce il rispetto del seguente decalogo:

1. effettuare la ricognizione dei dati trattati nello Studio o nell'Azienda riferibili alle ***persone fisiche***, classificandoli in categorie a seconda del grado di riservatezza necessaria (ad es.: dati personali non sensibili; dati personali sensibili: a) che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; b) dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale);
2. individuare i **fondamenti legali del trattamento** (per esempio, consenso, trattamento in vista dell'esecuzione di un contratto, obbligo legale, ecc…) di ciascuna categoria di dati;
3. predisporre un'adeguata ***informativa***, stabilendo le modalità per porla a conoscenza dei soggetti interessati e per provare di averlo fatto;
4. predisporre le procedure che permettono di raccogliere e di provare l'assenso;
5. predisporre procedure e modalità per assicurare l'esercizio dei diritti dell'interessato (cancellazione, rettifica, accesso, portabilità …)
6. effettuare un'adeguata formazione del personale (interno ed esterno) che dovrà trattare i dati;
7. verificare la necessità di istituire i *Registri delle attività di trattamento*, tenendo conto che le dimensioni dell'impresa o organizzazione (più o meno di 250 dipendenti) non costituiscono l'unico elemento presupposto;
8. individuare le criticità dell'archiviazione e dell'utilizzo dei dati con particolare riguardo alla sicurezza, riservatezza, conservazione al fine di valutare se le misure adottate sono adeguate ai rischi;
9. definire le procedure per evitare (o minimizzare) qualsiasi violazione accidentale o da fatto illecito della sicurezza che possa comportare distruzione, perdita, divulgazione o accesso non autorizzati ai dati personali;
10. definire le procedure per individuare i rimedi o per ridurre gli effetti negativi in capo all'interessato delle violazioni della sicurezza.

Inutile precisare che il decalogo dovrà trovare pratica applicazione!

Ma per l'eventuale verificatore, probabilmente, **il buon senso non sarà sufficiente**; cosa fare allora per dimostrare di avere fatto tutto il possibile ed evitare, così, il rischio di sanzioni sproporzionate?

Quasi tutte le principali case di software stanno sviluppando soluzioni informatiche aventi lo scopo di aiutare studi professionali ed aziende a gestire gli adempimenti previsti dal GDPR che, partendo dalla "*autovalutazione dei rischi*", propongono procedure guidate atte a gestire la valutazione di impatto sulla protezione dei dati, la redazione dell'informativa e la documentazione delle scelte di "***compliance Privacy***".

Esperienza vissuta consiglia di evitare software nati solo per sfruttare l'occasione di business, che trasformino gli utenti in "***cartifici***"; per questo, lo Studio Andreetta & Associati sta "testando" alcune procedure informatiche che non mancherà eventualmente di suggerire agli interessati qualora le stesse si dimostrino idonee allo scopo, rappresentando un ragionevole compromesso tra le esigenze di completezza e rigore scientifico, da un lato e dall'altro, semplicità d'uso ed economicità.

Cordialità.

GiAn