IL GDPR E IL PROFESSIONISTA

LINEE GUIDA

CONCETTI GENERALI

Il nuovo **Regolamento Europeo in materia di protezione dei dati personali** ha mutato profondamente il quadro della normativa connessa alle nuove tecnologie, introducendo per la prima volta misure solide e strutturali per fronteggiare le nuove sfide dell'economia digitale.

Il tema tocca da vicino i professionisti tecnici.

A) Il settore della protezione dei dati personali sta attraversando un periodo di particolare fermento a seguito dell'entrata in vigore del Regolamento europeo sulla protezione dei dati personali n. 2016/679, il c.d. GDPR. Quali sono le novità in materia?

1. La nuova figura professionale alquanto complessa come il **Data Protection Officer (DPO)** che dovrà aiutare il titolare del trattamento ed il responsabile del trattamento nello svolgimento delle attività richieste dal GDPR per tutelare la privacy degli interessati.
2. la **valutazione di impatto** sulla protezione dei dati personali (DPIA), attività molto complessa e di primaria rilevanza in presenza di trattamenti molto delicati
3. i **registri delle attività di trattamento** che sebbene non sempre obbligatori considero fondamentali per avere un quadro generale dei trattamenti rilevanti ai fini privacy di una determinata realtà organizzativa.

B) Come si pone il GDPR in merito alla sicurezza informatica?

Nell'ottica del GDPR il concetto di sicurezza informatica ha assunto un significato più attuale alla luce anche dei sempre più numerosi attacchi ed incidenti di natura informatica che lasciano intuire una preoccupante tendenza alla crescita di tale fenomeno. In particolare negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia che possiamo definire "cibernetica" che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:
– Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati.
– Il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.
La combinazione di questi due fattori fa sì che, a prescindere dalle misure minime di sicurezza previste dal nostro codice in materia di protezione dei dati personali, (antivirus, firewall, difesa perimetrale, ecc.) bisogna fare particolare attenzione alle attività degli stessi utenti che devono rimanere sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.

L'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento, difatti tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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 devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In particolare, quindi, assume rilevanza la pseudonimizzazione intesa come un particolare 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.

Inoltre per la prima volta si parla di resilienza dei sistemi informatici intesa come la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.

Notevole rilevanza viene attribuita dal legislatore comunitario anche al disaster recovery, per cui diventa fondamentale predisporre uno specifico piano con il quale si intende fornire servizi volti all'analisi dei rischi di inoperatività del sistema EDP (informatico) e delle misure da adottare per ridurli, nonché la messa a punto del vero e proprio piano di emergenza informatica, che ricomprende, in particolare, procedure per l'impiego provvisorio di un centro di elaborazione dati alternativo o comunque l'utilizzo di macchine di soccorso da utilizzare in attesa della riattivazione.

C) quali sono gli aspetti più interessanti di questa nuova normativa che possono coinvolgere i professionisti tecnici?

indubbiamente i professionisti tecnici (fra cui i geologi) al di là di tutti gli obblighi richiesti al titolare del trattamento in quanto tale, dovranno fare particolare attenzione all'utilizzo di tutti i prodotti o software tecnologicamente avanzati che trattino dati personali, difatti in questi casi potrebbe rivelarsi necessaria una Data Protection Impact Assessment (DPIA) richiesta dall'art. 35 del GDPR quando si è in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Anche l'adozione di procedure tecnologicamente complesse, di processi decisionali automatizzati, di attività sistematiche di monitoraggio potrebbero presentare rilevanti criticità in tema di trattamenti di dati personali.

Anche i professionisti/ studi di professionisti, indipendentemente dalla loro dimensione, dalla struttura e dall'area di attività dovranno adeguarsi.

La divulgazione, anche accidentale dei dati potrebbe ledere i diritti e la libertà delle persone coinvolte.

Al fine di evitare i pericoli della perdita di tali dati, gli avvocati dovranno prestare particolare attenzione a che:

- Le finalità di trattamento dei dati e la loro trasmissione siano chiaramente definite;

Le misure di sicurezza (tanto informatica che fisica) siano precisamente individuate, definite e attuate;
Le persone coinvolte (segreteria, colleghi, collaboratori a qualsiasi titolo) siano adeguatamente informate e coinvolte nel processo di protezione dei dati personali.
Il professionista dovrà anche tenere presente che il progresso tecnologico deve comunque rispettare gli obblighi deontologici e normativi: pertanto, anche nelle ipotesi in cui lo studio/professionista abbia esternalizzato a terzi alcuni servizi (ad esempio l'utilizzo di una segreteria virtuale, la conservazione dei dati su cloud), o utilizzi propri mezzi di comunicazione a terzi (sito web, blog, servizi di consultazione on line, utilizzo di siti terzi), dovrà prestare la massima attenzione a che i dati siano trattati in modo sicuro e nel rispetto delle norme.

La presente guida vuole essere un aiuto ai professionisti per consentire loro di adeguarsi alla normativa in materia di protezione dei dati personali.

D) PRINCIPI DEL GDPR

Il regolamento riafferma principi fondamentali già in vigore con la precedente legislazione e ne aggiunge di nuovi.
Tra i principi relativi al trattamento dei dati che vengono confermati:
finalità del trattamento che ne limita l'utilizzo per i soli fini perseguiti con specifico mandato del professionista (titolare del trattamento);
ad esempio i dati raccolti nelle visure catastali non possono essere utilizzati per conoscere la vita privata dei clienti, e neppure utilizzati a scopi commerciali, di pubblicità politica o elettorale;
necessità e proporzionalità: il trattamento deve essere adeguato, pertinente e necessario allo scopo; i fascicoli delle pratiche e l'archiviazione informatica degli stessi devono essere configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali ed identificativi;
durata limitata: il trattamento non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, ovvero oltre il tempo necessario in funzione dell'incarico e della finalità del trattamento stesso compresi gli obblighi legali di conservazione;
nell'informativa al cliente è essenziale indicare la ragionevole durata del trattamento stesso (considerando che nel concetto di trattamento rientra anche la mera conservazione del fascicolo contenente dati personali, a prescindere dal fatto che si tratti di fascicolo informatico o cartaceo);
sicurezza e riservatezza: il professionista è tenuto, anche per obblighi deontologici e, nel rispetto del segreto professionale, ad approntare un adeguato livello di sicurezza per i dati degli assistiti. Il professionista, pertanto, nella sua qualità di titolare del trattamento deve prevedere tutte le misure necessarie per garantire la confidenzialità, integrità e disponibilità dei dati personali: i dati contenuti nel fascicolo, ad esempio, non possono essere consultati da persone non abilitate ed espressamente istruite e autorizzate ad accedervi in ragione dei loro specifici compiti, sia che si tratti di soggetti interni all'organizzazione dello studio professionale (addetti alla segreteria, colleghi di studio) o esterni allo stesso (consulenti tecnici, commercialisti etc).

rispetto del diritto delle persone.
Sono poi stati introdotti ulteriori principi e doveri cui il professionista deve uniformarsi:
Il principio di accountability, alla quale si è già fatto cenno (o principio di responsabilizzazione);
La minimizzazione dei dati;
Il diritto all'oblio;
il diritto alla portabilità dei dati;

La notificazione dei data breach al Garante e, in talune ipotesi, agli interessati.

D-1) ACCOUNTABILITY (RESPONSABILIZZAZIONE)

Pietra miliare di una visione differente di approccio al dato dell'interessato - ancorché riprenda quanto già previsto dall'art. 6 comma 2 della Direttiva 95/46/CE - il GDPR impone (anche) al professionista un profondo cambiamento culturale nel trattamento delle informazioni di cui viene in possesso o ha accesso in virtù del suo mandato e, pertanto, nella qualità di titolare del trattamento.

Rispetto al Codice Privacy, non sono più previste le c.d. misure minime, ma è posta in capo al titolare del trattamento, la responsabilità (accountability di definire, dopo una attenta analisi dei dati trattati e dei possibili rischi connessi, le misure adeguate al fine di garantire il rispetto delle norme del GDPR.

Responsabilizzazione significa, sostanzialmente, che le misure dovranno essere adeguate alla struttura del singolo titolare ed elaborate, caso per caso, ricorrendo ad una preventiva mappatura dei dati trattati, della mole degli stessi, dei rischi di trattamento dei dati gestiti.

Accountability, inoltre, significa qualcosa di più: significa anche essere in grado di "rendere conto" delle attività poste in essere e del fatto di aver rispettato i principi del GDPR (e ciò in base a quanto previsto dal secondo comma dell'art. 5 del GDPR).

Il Professionista, pertanto, deve garantire la conformità (compliance, in inglese) al Regolamento dei trattamenti eseguiti (sia dal titolare che dai
soggetti da lui eventualmente nominati come responsabili).

Ciò significa, ad esempio, che anche l'adozione di criteri e procedure di trattamento certe e di una formazione adeguata allo studio, potrà precostituire una prova della conformità del trattamento al fine di evitare pesanti sanzioni.

D-2)MINIMIZZAZIONE DEI DATI

E' il principio secondo il quale i dati personali da trattare per ogni singola attività debbano essere soltanto quelli necessari per il raggiungimento dello scopo.

Consiste, ad esempio:

nell'interrogarsi sulla necessità di trattare dati personali per raggiungere le finalità richieste dal trattamento;

nel limitare al minimo il ricorso al trattamento dei dati personali, ove sia necessario, per quanto attiene: le categorie di dati trattati, il volume e la quantità di dati e il sapere se sono o meno necessari al trattamento.

Al fine di conformarsi al principio di minimizzazione, il professionista dovrà trattare, per quanto possibile, solo i dati essenziali, necessari e pertinenti per compiere la prestazione richiesta dal cliente.

Ad esempio i dati raccolti nell'assolvimento di un incarico non possono essere utilizzati per conoscere la vita privata delle persone, e neppure utilizzati a scopi commerciali di pubblicità politica o elettorale;

D-3) DIRITTO ALLA CANCELLAZIONE - DIRITTO ALL'OBLIO

L'art. 17 del GDPR (C65, C66) prevede il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano ed il correlativo obbligo di adempiere senza ingiustificato ritardo da parte del titolare stesso.

L'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o sia venuto meno il motivo per cui sono stati forniti.

Per il professionista il diritto all'oblio non potrà essere esercitato sino quando non sia maturato il termine di prescrizione dell'azione per la responsabilità professionale.
E' importante rilevare, inoltre, che l'esercizio del diritto in parola cede il passo di fronte all'adempimento di alcuni obblighi di archiviazione dei dati per periodi specifici e risulta pertanto non utilmente esercitabile ove comprometta l'adempimento ad obblighi fiscali o si ponga in contrasto con necessità archivistiche di pubblico interesse.

D-4) LA VALUTAZIONE DI IMPATTO

L'art. 35 del GDPR (C84, C89-C93, C95) prescrive
-quando sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche, ivi compreso il trattamento su larga scala di dati particolari:
- che il titolare del trattamento debba effettuare una preliminare valutazione d'impatto (DPIA).
Per facilitare l'esecuzione della valutazione di impatto, il Garante per la protezione dei dati personali ha messo a disposizione un software, scaricabile al seguente link:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268

D-5) LA PORTABILITÀ DEI DATI

Il diritto alla portabilità attribuisce agli interessati la facoltà di esigere dal titolare del trattamento la trasmissione dei loro dati ad un altro titolare, senza che il primo si possa opporre.
L'art. 20 del GDPR attribuisce all'interessato 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.
Ciò significa che il professionista che tratti i dati dei clienti con mezzi automatizzati (per esempio, adottando un gestionale informatico o anche solo tenendo uno schedario sotto forma di foglio di calcolo) è tenuto a comunicare i dati del suo cliente al collega alle seguenti condizioni:
-il cliente ha espresso il suo consenso al trattamento dei suoi dati personali o il trattamento è necessario per l'esecuzione di un contratto a cui il il cliente è parte o l'esecuzione delle misure precontrattuali adottate a richiesta del cliente;
- e il trattamento è stato effettuato con mezzi automatizzati.
Pertanto, se il suo cliente richiede la trasmissione dei suoi dati ad un collega, il professionista dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.
Peraltro, il diritto alla portabilità non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
il diritto alla portabilità non è esteso ai fascicoli cartacei, che sembrano dunque esclusi dal diritto alla portabilità.
Deve però essere ricordato che, secondo l'art. 2235 c.c., il professionista non ha diritto a trattenere i dati se non il tempo necessario alla tutela dei propri diritti.
I titolari del trattamento devono essere in grado di seguire e identificare i destinatari dei dati personali che elaborano, e nei casi previsti debbono tenere un registro dei trattamenti.

D-6) L'INFORMATIVA SUL TRATTAMENTO DEI DATI

L'art. 13, paragrafo 1, del GDPR impone al professionista che acquisisce i dati degli assistiti di fornire le seguenti informazioni:

1.l'identità e i dati di contatto del titolare dello studio e, ove applicabile, del suo rappresentante all'estero;
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;
4.le categorie di dati personali in questione;
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 destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta a tali informazioni, una volta che i dati personali siano stati acquisiti, il titolare del trattamento dovrà fornire all'interessato ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente, vale a dire:

7.il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
8.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;
9. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'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;
10.il diritto di proporre reclamo a un'autorità di controllo;
11.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;
12.l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

I professionisti che agiscono quali titolari dei dati sono liberi di determinare i mezzi occorrenti per assicurare l'informativa alle persone.
In altri termini, e volendo semplificare ai minimi termini, il professionista è tenuto a rendere le informazioni sul trattamento dei dati esclusivamente ai propri clienti, oltre che a tutti gli altri soggetti i cui dati vengano trattati per ragioni contrattuali (fornitori, collaboratori, consulenti, con esclusione dei dati che il titolare detenga ai fini dell'adempimento di un obbligo di legge
Gli interessati al trattamento da parte di uno studio professionale dovranno essere informati su:
• L'identità e i dettagli di contatto del titolare del trattamento (studio o l'associazione professionale);
• i dettagli di contatto del responsabile o dei responsabili della protezione dei dati, qualora nominati;
• Le finalità del trattamento
• La base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta del cliente);
• interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f;

• destinatari di dati (subappaltatori, ufficiali giudiziari, ecc.);
• flussi transfrontalieri;
• la durata di conservazione;
• i diritti che gli interessati possono esercitare;
• le condizioni e le modalità per l'esercizio dei diritti degli interessati;
• il diritto di revocare il consenso, se questo è la base giuridica del trattamento;
• il diritto di presentare un reclamo all'autorità di controllo;
• le informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Come va resa l'informativa.

L'informativa dev'essere scritta in un linguaggio chiaro e semplice ma può essere resa anche in formato elettronico (ad esempio, se destinate al pubblico, attraverso un sito web) o comunicata via e -mail

(ad esempio, in occasione della trasmissione di una nota di onorario in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati).

L'informativa può essere data anche nel corpo dell'accordo professionale.

Sono ammesse icone per la sua composizione, purché queste siano accompagnate da una informativa estesa (queste icone dovranno essere uguali in tutta Europa e saranno definite dalla Commissione Europea).

Il testo dell'informativa può anche essere inserito nel sito web del professionista, a condizione che poi lo stesso possa dimostrare che l'informativa è stata letta, ad esempio inserendo nel testo dell'incarico professionale che il cliente ha preso visione dell'informativa pubblicata sul sito, e di averla ben compresa.

D-7) CONSERVAZIONE DEI DATI

Il professionista titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio.

I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta.

In generale, i dati dei clienti possono essere tenuti per la durata dell'incarico professionale tra il professionista e il suo cliente.

Possono ovviamente essere conservati anche dopo la cessazione del
rapporto professionale, al fine di tutelare i diritti dello stesso nei confronti del cliente, sia quanto al diritto a conseguire i compensi, sia per resistere ad eventuali azioni di responsabilità: per tale ragione, si ritiene che la conservazione dei dati possa prolungarsi per tutto il tempo di prescrizione ordinaria, prima della loro cancellazione definitiva.

È inoltre importante ricordare che i dati acquisiti in sede di identificazione e adeguata verificata ai sensi del decreto legislativo n. 231 del 2007 in materia di antiriciclaggio devono essere conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale (art. 31, comma 3, d. lgs. 231 del 2007).

D-8) IL CONSENSO

Il consenso è definito dall'art. 4, par. 1 n. 11, del GDPR come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'inte ressato, 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".

L'art. 6, par. 1, del GDPR indica le condizioni di liceità del trattamento, individuando 5 condizioni di cui almeno una deve ricorrere affinché il trattamento possa essere considerato lecito.

Delle condizioni indicate, si evidenziano le seguenti:

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.

Quantunque non sia richiesto un consenso scritto, e sebbene l'attività professionale possa rientrare nella lettera b), è preferibile precostituirsi la prova di avere ottenuto il consenso (art. 7, par. 1, del GDPR): il professionista, quindi, dovrà sottoporre al cliente per la firma una dichiarazione di consenso in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive (C42). È facoltà dell'interessato revocare il proprio consenso in qualsiasi momento (art. 7, par. 2, del GDPR), ma "la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca ".

D-9) IL DIRITTO DI ACCESSO AI DATI

Qualsiasi persona fisica che giustifichi la sua identità ha diritto di interrogare il titolare
-per sapere se sta trattando i suoi dati;
-per ottenere la comunicazione dei dati in forma comprensibile e tutte le informazioni disponibili per quanto attiene l'origine del trattamento;
-per ottenere informazioni sulla finalità del trattamento i dati raccolti e i destinatari
Sinteticamente:
Tempo di risposta a una richiesta: il tempo di risposta è ora un mese dal ricevimento della richiesta (articolo 12.3). Viene tuttavia offerta l'opportunità di prorogare questo termine di due mesi" data la complessità e il numero di applicazioni ", a condizione che l'interessato riceva comunque un'informazione al riguardo entro un mese dal ricevimento della richiesta (articolo 12.3).
Commissioni di riproduzione: il regolamento prevede un principio di gratuità copie fornite come parte di una richiesta di accesso (Articolo 12.5). questo solo quando la domanda è manifestamente infondata o eccessiva che il responsabile del trattamento può richiedere il pagamento di "costi ragionevoli" che tengono conto dei costi amministrativi sostenuti per la fornitura delle informazioni. La medesima regola si applica quando viene richiesta una copia aggiuntiva dei dati.
Le modalità di comunicazione dei dati: il regolamento prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta
È comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente (art. 12,3).
Prevede inoltre che il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso (articolo 28 e). Ad esempio: un datore di lavoro potrebbe chiedere al proprio responsabile del trattamento di fornirgli supporto per fornire ai dipendenti che lo richiedono geolocalizzazioni "in forma accessibile";

D-10) PRIVACY BY DEFAULT E PRIVACY BY DESIGN

L'art. 25 del GDPR
prevede l'obbligo Integrare di default il concetto di dati personali nella progettazione di nuovi prodotti e servizi. Quando il professionista cambia i suoi software, pertanto, si deve interrogare sin dall'inizio in merito all'impatto dell'evoluzione sui dati che tratta. Ciò implica in particolare l'integrazione di tecniche di protezione e misure organizzative per limitare i rischi di violazione dei diritti e delle libertà delle persone.

****

APPLICAZIONE PRATICA PER GLI STUDI PROFESSIONALI/PROFESSIONISTI

TITOLARE:
Il professionista sarà il titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dai clienti in virtù o in correlazione all'incarico ricevuto.
In caso di incarico a più professionisti questi saranno co-titolari. In questo caso sarà necessario un accordo interno per definire le relative responsabilità e compiti.
Qualora più professionisti ricevano incarico dallo stesso soggetto per finalità ed attività differenti, ciascun professionista sarà un autonomo titolare del trattamento.

Nel caso di Studio professionale associato il titolare sarà il soggetto giuridico in nome del LRPT

Se il professionista incarica altri soggetti per l'adempimento di una o più attività questi saranno Responsabili del trattamento.

REGISTRO DEI TRATTAMENTO DATI:
non vi è l'obbligo per soggetti con meno di 250 dipendenti a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, non occasionale o se si riferisce in particolare a dati sensibili o dati relativi a condanne e reati.

Un professionista tratta:

- i dati relativi al proprio personale dipendente ed ai collaboratori;
  è vietato raccogliere dati relativi alla famiglia e i dati su opinioni politiche o appartenenza sindacale del candidato/dipendente/collaboratore;
  il professionista deve far sottoscrivere l'informativa privacy al proprio personale dipendente ed ai collaboratori;

- i dati relativi ai clienti;
  il professionista deve far sottoscrivere l'informativa privacy ai propri clienti indicando le finalità e limitando al minimo la raccolta dati; tale informativa può essere contenuta del conferimento di incarico professionale;

  Il professionista deve avere un sistema informatico che garantisca la sicurezza dei dati del cliente;

- i dati raccolti attraverso il sito internet (se li raccoglie);

RESPONSABILE DEL TRATTAMENTO:
E' colui che "tratta" i dati per conto del Titolare del trattamento.
Nel caso di studi professionale/professionisti il responsabile del trattamento è esterno ed è colui a cui sono comunicati i dati personali trattati (commercialista – consulente – fornitore-gestori informatici). Con questi soggetti è necessario stipulare un accordo/contratto in cui sia compresa l'informativa privacy.

IL SITO WEB DELLO STUDIO/PROFESSIONISTA:
Sul sito web deve essere pubblicata l'informativa privacy.

Qualora il sito web prevede anche una raccolta dati il professionista dovrà prevedere un programma per avere la conferma che il soggetto che inserisce i dati ha accettato l'informativa privacy e comunque deve inserire tale attività nel registro trattamento dati.

SICUREZZA INFORMATICA:

Lo studio/professionista dovrà adottare le norme sulla sicurezza informatica, inserendo accessi con identificativo ed utilizzare programmi sicuri.

DPO (DATA PROTECTION OFFICER)/ RPD (RESPONSABILE PROTEZIONE DATI):

L'ART. 37 del GDPR prevede la nomina del DPO ogni qualvolta:

- il trattamento sia effettuato da un'autorità, un organismo ovvero un ente pubblico;
- le attività principali del titolare del trattamento e del responsabile del trattamento richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le loro principali attività le portano a trattare su larga scala categorie specifiche di dati sensibili;

in tutti gli altri casi il professionista7studio non ha l'obbligo di nominare il DPO ma può farlo se lo ritiene utile;

DPIA (DOCUMENTO DI VALUTAZIONE DI IMPATTO PER LA PROTEZIONE DATI):

quando sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche, ivi compreso il trattamento su larga scala di dati particolari:
Per facilitare l'esecuzione della valutazione di impatto, il Garante per la protezione dei dati personali ha messo a disposizione un software, scaricabile al seguente link:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268

DATA BREACH:

un professionista/studio professionale deve notificare al garante tutte le violazioni dei dati personali e comunicare tale violazione alle persone interessate.
Il modulo per la notifica è on line sul sito del Garante.
Se la violazione crea un rischio per i diritti e le libertà degli interessati la comunicazione andrà fatta anche a loro.

SANZIONI:

L'autorità garante può erogare sanzioni al titolare ed al responsabile del trattamento qualora non vengano rispettate le direttive del GDPR.
Le sanzioni variano a seconda della irregolarità e dell'importo del fatturato.
Con il D. Lgs. 101/18 nei primi 8 mesi verranno emanate sanzioni meno importanti.

Avv. Cristiana Fabbrizi