PRIVACY

Tutto quesiti: le principali novità “privacy” per lo studio professionale

Le risposte alle domande dei professionisti

di Armando Urbano | 9 MAGGIO 2018

La *privacy* è il diritto di una persona alla riservatezza dei propri dati e consente di verificare che le proprie informazioni vengano «trattate» o «controllate» da altri solo in caso di necessità.
Infatti, dovranno essere abrogate le disposizioni del codice incompatibili con quelle contenute nel regolamento comunitario, dovrà essere modificato, in alcune parti, il codice in materia dei dati personali, per dare attuazione alle disposizioni, non direttamente applicabili, contenute nel regolamento, e sarà necessario coordinare le disposizioni vigenti in materia di protezione dei dati personali con quelle recate dal regolamento comunitario.
Il Reg. UE 27 aprile 2016, n. 2016/679/UE, si compone di 179 considerando e di 99 articoli, che mirano ad adeguare la protezione dei dati rispetto all’evoluzione tecnologica che ha determinato un aumento dei sistemi informatici e dei flussi.
In questa circolare “Tutto quesiti” si forniscono le risposte alle domande che sono state poste dai lettori in tema di *privacy*.

SOMMARIO:

- QUESITO 1 - TITOLARI, RESPONSABILI DEL TRATTAMENTO E INFORMATIVA NELLE PERSONE GIURIDICHE
- QUESITO 2 - RAPPORTI TRA PROFESSIONISTA E SOCIETÀ PER ELABORAZIONE DATI: ADEMPIMENTI “PRIVACY”
- QUESITO 3 - “PRIVACY” DITTE INDIVIDUALI
- QUESITO 4 - CONSENSO DEI DIPENDENTI
- QUESITO 5 - ADEMPIMENTI “PRIVACY” DEL MEDICO DI BASE
- QUESITO 6 - ADEMPIMENTI PER AZIENDE E PROFESSIONISTI
- QUESITO 7 - CREDENZIALI PERSONALI DEI CLIENTI
- QUESITO 8 - IL TITOLARE DEL TRATTAMENTO E IL DPO IN UNA DITTA INDIVIDUALE
- QUESITO 9 - TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO
- QUESITO 10 - CERTIFICATI MEDICI DEI DIPENDENTI
- QUESITO 11 - SEGNALAZIONE DI “DATA BREACH”
- QUESITO 12 - INFORMATIVA “PRIVACY”
- QUESITO 13 - TRATTAMENTO SU LARGA SCALA
- QUESITO 14 - PROFESSIONISTI E CENTRO ELABORAZIONE DATI

Quesito 1 – Titolari, responsabili del trattamento e informativa nelle persone giuridiche

Domanda

In uno studio di commercialisti istituito nella forma di società a responsabilità limitata:

- il titolare del trattamento è la società o sono i commercialisti?
- Vi può essere la presenza di più responsabili del trattamento sotto un unico titolare del trattamento?
- Per quanto riguarda l'informativa: se i professionisti dello studio hanno clienti separati, bisogna rilasciare informative differenti, in quanto alcuni dei professionisti della società non gestiscono i clienti di altri professionisti?

Risposta

In una **persona giuridica**, come chiarito dal Garante per la protezione di dati personali, in un comunicato stampa dell'11 dicembre 1997, il **titolare del trattamento è la struttura nel suo complesso** e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati. Non devono, quindi, essere considerati come "titolari" le singole persone fisiche che la amministrano o che la rappresentano. Il Garante ha chiarito, peraltro, che, se i "titolari" sono le imprese, per esse **opereranno**, nelle diverse scelte che sia necessario assumere, i **rispettivi amministratori**, secondo le regole che disciplinano ciascuna struttura, di volta in volta:

- l'amministratore unico;
- l'amministratore delegato;
- il consiglio di amministrazione.

Esempio

Le **segnalazioni o le comunicazioni** al Garante dovranno essere **sottoscritte dalla persona fisica che ha il potere di rappresentare la società**.

Rispondendo al quesito, il **titolare è la STP** nella persona del suo **legale rappresentante**. Il **responsabile del trattamento** (persona fisica o giuridica), nella previsione del regolamento, è riferibile unicamente al **soggetto esterno** all'organizzazione dello studio che **tratta dati personali per conto del titolare**.

Ricorda

E', per esempio, designabile responsabile del trattamento un **consulente esterno**.

La nomenclatura del D.Lgs. 30 giugno 2003, n. 196, che definiva incaricati, responsabili interni e responsabili esterni, non è più menzionata dal regolamento, che prevede solo la figura del responsabile del trattamento riferibile a soggetto esterno (art. 28).

L'**informativa** dovrà essere **resa dalla STP ai clienti** (soggetti interessati) della stessa.

Per i **clienti non gestiti dalla STP**, i professionisti dovranno **rilasciare l'informativa**, in quanto autonomi titolari. Si precisa che l'autorizzazione di carattere generale 15 dicembre 2016, n. 4/2016 (*G.U.* n. 303 del 29 dicembre 2016), attualmente in vigore, **solleva lo studio del professionista dal richiedere il consenso**, anche se è **preferibile acquisirlo**.

Quesito 2 - Rapporti tra professionista e società per elaborazione dati: adempimenti "privacy"

Domanda

Nel mandato professionale conferito per taluni clienti, si indica il nome della società di elaborazione dati (di cui si avvale lo studio) per porre in essere integralmente i servizi nei loro confronti. Inoltre, viene indicato nel mandato che è direttamente tale società a fatturare i servizi al cliente.

A tale riguardo si richiede: ai fini della *privacy* (relativa informativa da emettere al cliente e gestione connessi), e antiriciclaggio (relativa adeguata verifica, valutazione rischio, e connessa gestione altri adempimenti), tali adempimenti dovranno essere effettuati a nome di tale società che effettua interamente i servizi, ovvero anche da parte dello studio che non effettua i servizi? Seppure si ricorda che è lo studio ad avere posto in essere il mandato professionale, al solo scopo volere coprire l'eventuale rischio di errori a favore del cliente! Con tale società e lo studio sono interconnessi altri servizi in forza di un rapporto professionale (consulenza,

elaborazione, ecc.).

Risposta

Si ritiene, a parere di chi scrive, che i rapporti istituiti tra professionista e società di elaborazione dati debbano essere disciplinati meglio.

Infatti, il **professionista deve scindere gli adempimenti *privacy* da quelli antiriciclaggio** (per questi si rimanda alle risposte ai quesiti 7 e 8 della circolare monografica "Tutto quesiti: i corretti adempimenti antiriciclaggio per i professionisti") **e dalla copertura dei danni cagionati al cliente** mediante la polizza assicurativa.

Quesito 3 - "Privacy" ditte individuali

Domanda

I dati identificativi riferiti a ditte individuali sono dati personali ai fini della normativa *privacy*? Se vengono trattati, deve essere fornita l'informativa *privacy*?

Risposta

L'art. 1 del Reg. UE n. 2016/679/UE, rubricato "*Oggetto e finalità*", al comma 1 precisa che: "*il presente regolamento stabilisce norme relative alla **protezione delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati*".

Il regolamento (GDPR) **non disciplina il trattamento dei dati personali relativi a persone giuridiche**, in particolare alle imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto; in tale caso, le disposizioni del regolamento troveranno **applicazione** con riferimento al **trattamento dei dati personali del rappresentante legale**.

L'art. 4 del GDPR stabilisce che per **dato personale** debba intendersi "*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*".

Pertanto, poiché i **dati delle ditte individuali sono riferiti a persone fisiche**, **si applica la normativa *privacy*** e bisognerà **rendere l'informativa** ai clienti persone fisiche (interessati) e **ottenere** da questi il **consenso** espresso per il trattamento dei dati.

Quesito 4 - Consenso dei dipendenti

Domanda

Le società, o gli studi professionali con dipendenti, devono acquisire il consenso al trattamento dei dati sensibili di questi (ad esempio, dati riferiti alla salute, certificati medici, ecc.)? O in questi casi si rientra, ex art. 9 del Reg. (UE) n. 2016/679/UE, nei casi in cui il consenso non serve perché i dati sono necessari per assolvere ad obblighi di legge in materia di diritto del lavoro?

Se invece deve essere fornito in via esplicita il consenso, è sufficiente che questo venga fornito in maniera generica nel modulo che si fa sottoscrivere per la *privacy* (con una dicitura generica sul trattamento dei dati sensibili esclusivamente per quanto necessario ai fini della normativa in materia di diritto del lavoro)?

Sempre con riferimento ai dati sulla salute dei dipendenti o dei clienti (ad esempio, dati utilizzati per la dichiarazione dei redditi), in questi casi incombe l'obbligo di tenere il registro del trattamento dei dati personali e deve essere nominato il DPO?

Risposta

Per la corretta gestione del rapporto di lavoro, bisogna **informare il dipendente sui trattamenti che si intendono effettuare e chiedere il consenso**. Il trattamento dei dati nel rapporto di lavoro è regolato dall'autorizzazione 11 dicembre 2014, n. 1/2014 (Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro, in *G.U.* n. 301 del 30 dicembre 2014). Inoltre il regolamento, all'art. 9, comma 2, lett. b), ammette il **trattamento dei dati sensibili anche senza il consenso** dell'interessato, quando 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*".

L'**obbligo di tenuta del registro delle attività di trattamento dati** è previsto per tutte le strutture con **più di 250 dipendenti** o per le strutture che hanno meno di 250 dipendenti, ma che **trattano dati sensibili**.

Attenzione

In deroga all'art. 30, par. 5, la comunicazione WP 29 del 19 aprile 2018 e il considerando 82, in merito alle finalità del registro, ritengono che lo stesso sia **sempre obbligatorio, tranne** nel caso specifico in cui il **trattamento dei dati risulti occasionale**.

La **nomina del *data protection officer*** è **obbligatoria** per tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto le loro finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala** o la cu attività principale consiste nel **trattamento, su larga scala, di dati sensibili**, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Il 26 marzo 2018, il Garante per la protezione dei dati personali, per chiarire alcuni dubbi in merito alla nomina, ai requisiti e alla designazione del responsabile della protezione dei dati (DPO), ha pubblicato sul proprio sito le *FAQ* (*frequently asked questions*) che interessano tale figura in ambito privato e ha precisato che **non ritiene obbligatoria la nomina del DPO** "*in relazione a trattamenti effettuati da **liberi professionisti operanti in forma individuale***"; tale nomina è comunque **raccomandata**, anche se non obbligatoria.

Quesito 5 - Adempimenti "privacy" del medico di base

Domanda

I medici di base devono tenere il registro dei trattamenti? Devono nominare il DPO? Devono criptare le *mail* inviate ai pazienti?

Risposta

I medici di base sono professionisti che operano in forma individuale e pertanto:

1. devono **tenere il registro delle attività di trattamento dati**, in quanto trattano dati sensibili;
2. **non è obbligatoria la nomina del DPO** in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale;
3. è preferibile inviare le ***mail* ai pazienti**, che contengono dati sensibili, o **criptandole** o **utilizzando gli indirizzi PEC** del medico e del paziente (qualora quest'ultimo ne fosse in possesso).

Quesito 6 - Adempimenti per aziende e professionisti

Domanda

Alla luce del nuovo GDPR, cosa va fatto a livello pratico e operativo per essere in regola con la nuova normativa?

Di fatto, una società s.r.l., di dimensioni piccole o medie, prestatrice di servizi, cosa dovrebbe premurarsi di fare per essere regolare?

Stessa domanda per quanto riguarda invece uno studio professionale (commercialisti, consulenti).

Risposta

In base a quanto previsto dal GDPR, non è possibile fornire una risposta univoca al quesito posto, in quanto non esiste più il Documento programmatico per la sicurezza e **ogni struttura dovrà adeguarsi alla *privacy* in modo differente** a seconda della sua dimensione, dell'organizzazione, del tipo e del quantitativo di dati trattati, della modalità del trattamento e delle vulnerabilità nella sicurezza del trattamento e della conservazione dei dati.

In virtù del **principio di *accountability* (responsabilizzazione)**, ogni azienda/professionista deve adottare criteri e comportamenti tali da dimostrare la corretta adozione di misure finalizzate ad assicurare l'applicazione del regolamento in materia di protezione dei dati personali. Il titolare del trattamento effettua un **processo di valutazione** delle misure tecnico/organizzative che deve adottare per mitigare i rischi connessi al trattamento dei dati personali.

In base a quanto chiarito dalle Linee guida del Garante sull'applicazione del regolamento "*viene **affidato ai titolari il compito di decidere autonomamente** le modalità, le garanzie e i limiti del trattamento dei dati personali -nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.*

*Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le **garanzie indispensabili** "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati -tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso") e richiede, pertanto, un'**analisi preventiva** e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di **attività specifiche e dimostrabili**".*

Per avere un quadro più chiaro su ciò che bisogna "fare", si consiglia di prendere visione del documento elaborato congiuntamente dal Consiglio nazionale dei dottori commercialisti ed esperti contabili e dalla Fondazione nazionale commercialisti, che fornisce una ***check list* di base per gli studi professionali** e presente sul sito www.commercialisti.it (si rimanda alla circolare monografica "Privacy": check list di base per gli studi professionali).

Quesito 7 - Credenziali personali dei clienti

Domanda

Avendo l'autorizzazione dei nostri clienti (contribuenti), si può accedere con le loro credenziali alle aree riservate di INPS, Agenzia delle entrate, INAIL, ecc.?

Se lo si fa, chi e cosa rischiano il cliente che ci ha autorizzato e/o il professionista?

Risposta

A parere di chi scrive, **non è possibile utilizzare le credenziali personali del cliente** e il professionista, per effettuare le consultazioni, deve inviare agli enti preposti le apposite **deleghe rilasciate dai clienti**, al fine di abilitare direttamente i servizi *on line*.

Quesito 8 - Il titolare del trattamento e il DPO in una ditta individuale

Domanda

Il titolare del trattamento può essere la ditta stessa? E' consigliabile che il DPO sia un esterno?

Risposta

Il **titolare del trattamento è il titolare della ditta individuale**.

L'incarico di DPO può essere ricoperto sia da un **dipendente/collaboratore del titolare o del responsabile**, a patto che conosca la realtà operativa in cui avvengono i trattamenti, oppure può essere nominato un **soggetto esterno**, a condizione che garantisca l'effettivo assolvimento dei compiti che il Reg. (UE) n. 2016/679/UE (rego2016042700679) assegna a tale figura.

Il DPO **scelto all'interno** andrà nominato mediante specifico **atto di designazione**, mentre quello **scelto all'esterno** dovrà operare in base a un **contratto di servizi**. Entrambi gli atti, per i quali è obbligatoria la **forma scritta**, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché qualsiasi informazione utile relativa al contesto di riferimento.

Il responsabile della protezione dei dati personali, che sia interno o esterno, dovrà ricevere **adeguato supporto** in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il **titolare o il responsabile del trattamento**, che abbiano designato un responsabile per la protezione dei dati personali, restano comunque **pienamente responsabili** dell'osservanza della normativa in materia di protezione dei dati.

I **dati di contatto** del responsabile della protezione dei dati dovranno essere **pubblicati** dal titolare o dal responsabile del trattamento e **comunicati all'autorità di controllo**.

E' stato precisato che il ruolo di responsabile della protezione dei dati personali è **compatibile con altri incarichi**, a condizione che **non sia in conflitto di interessi** con essi.

Viene comunque consigliato di evitare l'assegnazione di tale ruolo a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione *marketing*, ecc.).

E' stato infine chiarito che il responsabile della protezione dei dati personali deve sempre essere individuato in una **persona fisica**, quando viene nominato un "dipendente" del titolare o del responsabile del trattamento.

Qualora il responsabile della protezione dei dati personali sia individuato in un **soggetto esterno**, quest'ultimo potrà essere **anche una persona giuridica**.

E' preferibile che il ruolo di responsabile della protezione dei dati personali (DPO) sia affidato a soggetto esterno in grado di conservare un **livello adeguato di autonomia** rispetto al titolare del trattamento.

Quesito 9 - Titolare del trattamento e responsabile del trattamento

Domanda

Il titolare del trattamento può essere contemporaneamente anche responsabile del trattamento?

Risposta

Nell'attuale quadro normativo, il **responsabile del trattamento** è riferibile **soltanto a figure esterne** che trattano dati per conto del titolare (art. 28 del Reg. UE n. 2016/679/UE).

In una **ditta individuale**, ci sarà il titolare del trattamento (la persona fisica titolare della ditta) e potranno esserci uno o più responsabili di trattamento esterni, in base alle necessità.

In una **società**, il titolare del trattamento dei dati sarà la società stessa e, anche in questa fattispecie, potranno esserci uno o più responsabili di trattamento esterni, in base alle necessità.

Quesito 10 - Certificati medici dei dipendenti

Domanda

Una società di elaborazione paghe chiede se il certificato medico di malattia e infortunio senza indicazione di diagnosi rientra nei dati sensibili.

Risposta

Di per sé il **certificato medico** deve essere generico e **non deve fornire indicazioni** circa:

- lo stato di salute del paziente;
- la struttura sanitaria;
- la specializzazione del reparto;
- la specializzazione del medico;
- la tipologia di esame diagnostico effettuato e la tipologia di visita effettuata.

Il **medico** inoltre è **obbligato a non divulgare a terzi le condizioni di salute dei propri pazienti** e, nei certificati medici, **non deve essere riportata la diagnosi**. Ciò detto, Il Considerando 35 ha precisato che:

"*Nei **dati personali relativi alla salute** dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro*".

La definizione data dal Considerando 35 è piuttosto ampia e bisogna, in via preventiva, verificare se si rientra in una delle fattispecie ivi indicate.

Pertanto, a parere di chi scrive, **se sul certificato non sono presenti la diagnosi o altri elementi che possano ricondurre allo stato di salute** del soggetto, quest'ultimo **non è considerato un dato sensibile**.

Quesito 11 - Segnalazione di "data breach"

Domanda

In caso di *ransomware* che cripta un *server*, che poi viene ripristinato mediante *restore* di un *backup*, è comunque obbligatorio segnalare al garante? In sostanza, è considerato l'evento *data breach*?

Risposta

Il ***ransomware***, la cui traduzione letterale dall'inglese è "virus del riscatto", **è un *malware*** che può provenire dall'apertura di un allegato infettato presente in una *e-mail*, da un clic su un *pop-up* ingannevole o semplicemente dalla visita di un sito *web* compromesso.

Si manifesta in una delle seguenti modalità:

- bloccando lo schermo di un utente (*ransomware lock-screen)* o
- crittografando i *file*.

Nel primo caso, provoca il **blocco di un singolo PC** e viene visualizzato sul *monitor* un messaggio con la richiesta di riscatto, rendendo il *computer* inutilizzabile fino a quando il *malware* non viene rimosso.

La **crittografia *ransomware* blocca permanentemente gli utenti dai propri *file* e dati**, non solo sui singoli PC, ma sull'intera **rete aziendale**.

Viene utilizzata la crittografia (*cryptolocker*) per scombinare i dati, con una tecnologia molto difficile da decriptare, fino al pagamento di un riscatto.

Poiché i dati sono stati attaccati e non è possibile avere la certezza se vi sia stato anche un furto degli stessi, nonostante si effettui il *restore* di un *backup*, è opportuno **effettuare tempestivamente al Garante la segnalazione di *data breach*, entro il termine perentorio di 72 ore** da quando il titolare è venuto a conoscenza della violazione.

Quesito 12 - Informativa "privacy"

Domanda

Le informative *privacy* raccolte degli anni precedenti rimangono valide e pertanto devono essere aggiornate con quelle nuove dall'entrata in vigore della nuova norma?

Risposta

> ⚠ Attenzione
>
> Le **informative *privacy*** raccolte sono **valide sino al 24 maggio 2018**.

Dal 25 maggio 2018 bisognerà raccogliere le nuove informative e i relativi consensi espressi degli interessati.

Così come consigliato dalle Linee guida del Garante sull'applicazione del regolamento *"è opportuno che i titolari di trattamento **verifichino la rispondenza** delle informative attualmente utilizzate a tutti i criteri delineati dal Regolamento, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da **apportare le modifiche o le integrazioni** eventualmente necessarie prima del 25 maggio 2018*".

Quesito 13 - Trattamento su larga scala

Domanda

Un sito di *e-commerce* utilizza le informazioni fornite da *adword* sulla profilazione, volte ad individuare le tipologie di clientela potenzialmente interessate alla vendita dei prodotti.

Queste informazioni sono comunque anonime (genere, attività lavorativa, area geografica, età di riferimento, ecc.).

In questo caso, si può ritenere che non si tratta di trattamento "su larga scala", secondo quanto previsto dal GDPR?

Risposta

Secondo le linee guide emanate il 13 dicembre 2016, successivamente emendate e adottate il 5 aprile 2017, dal Gruppo di lavoro Art. 29, al fine di **stabilire se un trattamento sia effettuato su larga scala**, si raccomanda di tenere conto, in particolare, dei **seguenti fattori**:

1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
3. la durata, ovvero la persistenza, dell'attività di trattamento;
4. la portata geografica dell'attività di trattamento.

Alcuni **esempi di trattamento su larga scala** sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni **esempi di trattamento non su larga scala** sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

In base a quanto esposto, bisognerà **valutare, nel caso specifico**, se il trattamento è effettuato su larga scala; in mancanza di ulteriori informazioni, si ritiene che la tipologia di trattamento sia effettuata dal sito di *e-commerce* su larga scala.

Quesito 14 - Professionisti e centro elaborazione dati

Domanda

Quali adempimenti devono porre in essere un commercialista e un consulente del lavoro che assistono un Centro elaborazione dati s.r.l. sia per quanto riguarda l'invio delle dichiarazioni dei redditi (che contengono i dati delle spese mediche ed altri dati sensibili) ovvero che conservano il LUL (all'interno del quale vi possono essere dati quali trattenute del quinto, pignoramenti, assegni familiari, legge 5 febbraio 1992, n. 104, ecc.)?

Devono nominare anche il DPO? Devono acquisire il consenso di tutti i contribuenti e quello dei lavoratori per cui elaborano le buste paga?

Risposta

Il **Centro elaborazione dati deve nominare i due professionisti quali responsabili del trattamento** (art. 28 del Reg. UE n. 2016/679/UE).

I singoli **professionisti**, a loro volta, dovranno **consegnare al Centro elaborazione dati un'attestazione** nella quale comunicano di essere in regola con la normativa in materia di protezione dei dati personali. Il **titolare del dato potrà richiedere ai professionisti l'esibizione del registro del trattamento** specifico per il titolare in questione.

Il **Centro elaborazioni dati** s.r.l. dovrà **nominare il DPO**, in quanto non è intervenuta un'esplicita esclusione, come per i professionisti che operano in forma individuale.

Riferimenti normativi:

- Reg. (UE) 27 aprile 2016, n. 2016/679/UE (rego2016042700679);
- D.Lgs. 30 giugno 2003, n. 196, art. 13.

Argomenti trattati

PRIVACY | TRATTAMENTO DEI DATI PERSONALI | TITOLARE DEL TRATTAMENTO DEI DATI | RESPONSABILE DEL TRATTAMENTO DEI DATI | RESPONSABILE DELLA PROTEZIONE DEI DATI