ASSIREVI

Documento di Ricerca n. 227

NORMATIVA "PROTEZIONE DEI DATI PERSONALI" PER I CASI DI REVISIONE (LEGALE E VOLONTARIA) E INCARICHI DISCIPLINATI DA LEGGE O REGOLAMENTI

Il presente Documento di Ricerca ha lo scopo di analizzare le diverse problematiche sottese agli adempimenti richiesti dal nuovo Regolamento Europeo 2016/679 ("GDPR") in materia di protezione dei dati personali da parte delle società di revisione contabile al fine di determinare in tale ambito il ruolo del revisore:

i) nello svolgimento degli incarichi di revisione (legale e volontaria), e

ii) nello svolgimento degli incarichi disciplinati da leggi o regolamenti (quali, a titolo esemplificativo e non esaustivo, quelli per il rilascio dei pareri/relazioni di cui agli artt. 2433-*bis* c.c. *(Acconti sui dividendi)*, 2437-*ter* c.c. *(Criteri di determinazione del valore delle azioni)* e ss., 2441 c.c. *(Diritto di opzione)*, art. 2501-*bis*, comma 5, c.c. *(Fusione a seguito di acquisizione con indebitamento)* e altri).

Il presente Documento non si occupa del ruolo del revisore, ai fini della normativa Protezione dei Dati Personali, nello svolgimento di incarichi differenti da quelli sopra indicati.

Per gli incarichi differenti da quelli sopra indicati, il revisore dovrà effettuare una valutazione specifica per poter determinare quale sia il ruolo assunto ai fini della normativa in esame: a tal fine, i criteri riportati nel presente Documento sono comunque di supporto anche per le valutazioni volte a determinare il ruolo che il revisore può assumere nello svolgimento di detti altri incarichi.

Febbraio 2019

Via Vincenzo Monti, 16 - 20123 Milano Tel. 02-436950 Fax. 02-437326 www.assirevi.com

Documento di Ricerca n. 227

Febbraio 2019

NORMATIVA "PROTEZIONE DEI DATI PERSONALI" PER I CASI DI REVISIONE (LEGALE E VOLONTARIA) E INCARICHI DISCIPLINATI DA LEGGE O REGOLAMENTI

1. SCOPO DEL DOCUMENTO

Il presente Documento di Ricerca ha lo scopo di analizzare le diverse problematiche sottese agli adempimenti richiesti dal nuovo Regolamento Europeo 2016/679 ("GDPR") in materia di protezione dei dati personali da parte delle società di revisione contabile al fine di determinare in tale ambito il ruolo del revisore:

i) nello svolgimento degli incarichi di revisione (legale e volontaria), e

ii) nello svolgimento degli incarichi disciplinati da leggi o regolamenti (quali, a titolo esemplificativo e non esaustivo, quelli per il rilascio dei pareri/relazioni di cui agli artt. 2433-*bis* c.c. *(Acconti sui dividendi)*, 2437-*ter* c.c. *(Criteri di determinazione del valore delle azioni)* e ss., 2441 c.c. *(Diritto di opzione)*, art. 2501-*bis*, comma 5, c.c. *(Fusione a seguito di acquisizione con indebitamento)* e altri).

Il presente Documento non si occupa del ruolo del revisore, ai fini della normativa Protezione dei Dati Personali, nello svolgimento di incarichi differenti da quelli sopra indicati.

Per gli incarichi differenti da quelli sopra indicati, il revisore dovrà effettuare una valutazione specifica per poter determinare quale sia il ruolo assunto ai fini della normativa in esame: a tal fine, i criteri riportati nel presente Documento sono comunque di supporto anche per le valutazioni volte a determinare il ruolo che il revisore può assumere nello svolgimento di detti altri incarichi.

2. CONTESTO NORMATIVO

Il Regolamento europeo (UE) 2016/679 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, adottato il 27 aprile 2016, entrato in vigore il 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, ha abrogato la "*Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*".

3. AMBITO MATERIALE E TERRITORIALE

Si definisce «dato personale» ai sensi dell'art. 4, n. 1), GDPR "*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*".

L'art. 4, n. 2), GDPR definisce come «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*"[1].

Il Regolamento si applica a imprese ed enti, ed organizzazioni in generale stabilite nell'Unione Europea.

4. PRINCIPALI NOVITÀ INTRODOTTE DAL REGOLAMENTO

Con l'utilizzo dello strumento regolamentare, il legislatore comunitario ha inteso definire un quadro normativo uniforme realizzando una armonizzazione piena della materia all'interno dell'Unione, riducendo quegli spazi di discrezionalità degli Stati membri che avevano portato ad attuare la *Direttiva 95/46/CE* (alla base, in Italia, della L. 31 dicembre 1996, n. 675 e del successivo D.Lgs. 30 giugno 2003, n. 196 "Codice *Privacy*") in maniera non omogenea.

Nel perseguimento dell'obiettivo descritto, il legislatore comunitario ha posto, alla base delle attività di trattamento dei dati personali, tre nuovi principi fondamentali:

(i) il principio di responsabilizzazione ("*accountability*"), che impone a tutti i soggetti che, a vario titolo, pongono in essere attività di trattamento di dati personali (e dunque, ai titolari, contitolari e responsabili del trattamento) di mettere in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR;

(ii) il principio "*privacy by design*", che implica la protezione dei dati fin dalla progettazione, con conseguente riduzione al minimo delle attività di trattamento, anche mediante l'adozione di misure tecniche ed organizzative *ad hoc* (es. pseudonimizzazione dei dati), nonché

(iii) il principio "*privacy by default*", che impone l'implementazione di misure tecniche ed organizzative idonee a garantire il trattamento dei soli dati necessari al perseguimento di una determinata finalità (c.d. "protezione per impostazione predefinita").

[1] Il GDPR individua inoltre particolari categorie di dati quali i dati genetici, biometrici e relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, nonché quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, il cui trattamento viene vietato, salvo che si verifichino dei casi specifici. Si ricorda che il GDPR sottopone a limitazioni anche il trattamento dei dati relativi a condanne penali e reati.

Valorizzando i principi anzidetti, il GDPR, dal punto di vista pratico ed operativo, introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (c.d. *data breach*). Sono previste, in caso di inosservanza, sanzioni pecuniarie aventi un massimo edittale da 10 a 20 milioni di Euro o pari al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore all'importo precedentemente indicato).

L'applicazione del GDPR obbliga le società e le organizzazioni – in qualità di titolari, contitolari e responsabili del trattamento – ad adottare od implementare misure tecniche ed organizzative adeguate al livello di rischio dei trattamenti, nonché a rivedere la documentazione e la contrattualistica in uso, al fine di conformarsi alle nuove disposizioni comunitarie in materia di protezione dei dati personali.

5. TITOLARE E RESPONSABILE DEL TRATTAMENTO

Secondo il GDPR (art. 4, n. 7), si definisce «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*".

Il titolare del trattamento non è, quindi, semplicemente chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali.

Il GDPR definisce il «responsabile del trattamento» come la *"persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"* (art. 4, n. 8). Si tratta quindi di quel soggetto che è preposto e al quale viene affidato, da parte del titolare che gli detta le istruzioni, il trattamento dei dati personali.

Il titolare nomina con contratto o atto giuridicamente valido, il responsabile del trattamento insieme al quale, tramite le istruzioni impartite, definisce le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.

6. I PRINCIPI FONDAMENTALI NELLO SVOLGIMENTO DELL'ATTIVITÀ DI REVISIONE

L'attività di revisione legale, intesa come revisione dei bilanci di esercizio o dei bilanci consolidati effettuata in conformità alle disposizioni del codice civile e del D.Lgs. 27 gennaio 2010, n. 39 ("Decreto") viene svolta nel rispetto dei principi etici internazionali applicabili (Codice etico emanato dallo IESBA[2], organismo dell' IFAC), quali: integrità e obiettività, competenza e diligenza professionale, riservatezza e comportamento professionale.

[2] IESBA – International Ethics Standards Board for Accountants è un organismo indipendente che sviluppa e rilascia, nell'interesse pubblico, standard etici di alta qualità per i revisori in tutto il mondo, contenuti in un Codice etico.

Il revisore e la società di revisione devono rispettare i principi di deontologia e indipendenza stabiliti dagli artt. 9, 10 e 10-*bis* del Decreto integrati dai Principi di indipendenza ed obiettività elaborati da Ordini e Associazioni professionali congiuntamente al MEF e alla CONSOB, in modo da dimostrare di essere indipendenti dalla società sottoposta a revisione e non essere coinvolti in alcun modo nel processo decisionale della predisposizione del bilancio.

Il revisore ha l'obbligo di riservatezza e di segreto professionale sulle informazioni che tratta durante i propri incarichi, così come sancito dall'art. 9-*bis* del Decreto che recita espressamente:
"*tutte le informazioni e i documenti ai quali ha accesso il revisore legale e la società di revisione sono coperti dall'obbligo di riservatezza e dal segreto professionale.*
I soggetti abilitati all'esercizio dell'attività di revisione legale rispettano i principi di riservatezza e segreto professionale elaborati da associazioni e ordini professionali congiuntamente al Ministero dell'economia e delle finanze e alla CONSOB e adottati dal Ministero dell'economia e delle finanze, sentita la CONSOB. A tal fine, il Ministero dell'economia e delle finanze sottoscrive una convenzione con gli ordini e le associazioni professionali interessati, finalizzata a definire le modalità di elaborazione dei principi.
Gli obblighi di riservatezza e segreto professionale di cui ai commi 1 e 2 non ostacolano l'applicazione delle disposizioni del presente decreto e, ove applicabile, del regolamento europeo.
Gli obblighi di riservatezza e segreto professionale di cui ai commi 1 e 2 continuano a valere anche successivamente al termine della partecipazione all'incarico di revisione.
Quando un revisore legale o una società di revisione legale è sostituito da un altro revisore legale o da un'altra società di revisione legale, il revisore legale o la società di revisione legale uscente consente al revisore legale o alla società di revisione legale entrante l'accesso a tutte le informazioni concernenti l'ente sottoposto a revisione e l'ultima revisione di tale ente.
Nel caso in cui un revisore legale o una società di revisione legale effettui la revisione legale conti di un'impresa che appartiene a un gruppo la cui società controllante ha sede in un Paese terzo, le regole in materia di riservatezza e segreto professionale di cui ai commi 1 e 2 non pregiudicano il trasferimento al revisore di gruppo situato nel Paese terzo, da parte del revisore legale o della società di revisione legale, della documentazione inerente all'attività di revisione, se la suddetta documentazione è necessaria per eseguire la revisione del bilancio consolidato della società controllante.
Un revisore legale o una società di revisione legale incaricato della revisione legale di una società che ha emesso valori mobiliari in un Paese terzo o appartenente a un gruppo che presenta il bilancio consolidato in un Paese terzo può trasferire all'autorità competente del Paese terzo in questione le carte di lavoro o gli altri documenti che detiene inerenti alla revisione dell'ente in causa soltanto in presenza di accordi di cooperazione di cui all'articolo 36.
Il trasferimento delle informazioni al revisore del gruppo situato in un Paese terzo è effettuato ai sensi del capo IV della direttiva 95/46/CE e delle norme nazionali applicabili alla protezione dei dati di carattere personale".

Il revisore e la società di revisione devono osservare i suddetti principi fondamentali, tenendo conto altresì di quanto puntualizzato nel "*Codice dei principi di deontologia professionale, riservatezza e segreto professionale dei soggetti abilitati all'esercizio dell'attività di revisione legale dei conti*" adottato con determina del Ragioniere generale dello Stato n. 245504 del 20 novembre 2018 ai sensi degli artt. 9, comma 1, e 9-*bis*, comma 2, del D.Lgs. 39/2010.

Si rammenta che il revisore è tenuto al rispetto del segreto professionale anche in forza di una serie di altre norme che integrano quanto indicato dall'art. 9-*bis* del Decreto[3].

7. ILLUSTRAZIONE SINTETICA DELL'ATTIVITÀ CARATTERISTICA DI UNA SOCIETÀ DI REVISIONE

La Fase principale di un incarico di revisione consiste nell'analisi delle voci di bilancio, e nella raccolta e analisi della documentazione probativa a supporto sia degli importi che delle informazioni fornite, nella misura ritenuta necessaria secondo il giudizio professionale del revisore. Tra le altre stabilite dai principi di revisione ISA Italia, le procedure che possono essere rilevanti ai fini della privacy sono:

- Ispezione: il revisore esamina a campione registrazioni e/o documenti, sia interni che esterni, in formato cartaceo, elettronico o in altro formato oppure effettua una verifica fisica di una attività;
- Conferma esterna: il revisore acquisisce risposta diretta in forma scritta da parte di un soggetto terzo in formato cartaceo, elettronico o in altro formato;
- Osservazione: il revisore assiste ad un processo o procedura svolta da altri per l'osservazione della conta fisica delle rimanenze;
- Indagine: il revisore ricerca informazioni di natura finanziaria o di altra natura presso soggetti interni o esterni all'impresa, in possesso delle necessarie conoscenze.

Sulla base degli elementi raccolti, il revisore raggiunge le proprie conclusioni e formula il proprio giudizio. In tale fase è previsto uno scambio formale di comunicazioni con i rappresentanti della *governance* del soggetto sottoposto a revisione, in modo particolare qualora si tratti di soggetti EIP, come definiti dall'art. 16 del D.Lgs. 39/2010 (viene infatti predisposta una relazione aggiuntiva rivolta al comitato per il controllo interno e la revisione contabile, che evidenzia i risultati, le difficoltà e gli altri aspetti significativi della revisione svolta).

Nel corso dell'incarico di revisione può rendersi necessario l'intervento di un esperto (es: esperto fiscale, attuariale, IT/Sicurezza, legale, ecc.).

[3] Si vedano art. 5, D.Lgs. 139/2005, art. 622 Codice penale, art. 200 Codice procedura penale, art. 249 Codice di procedura civile.

8. TIPOLOGIA DEI DATI TRATTATI DAL REVISORE

Nell'ambito degli incarichi di revisione, tra gli altri, sono generalmente raccolti:

- dati gestionali e contabili inerenti il personale della società sottoposta a revisione, mediante cedolini, tabulati nominativi TFR, informazioni sui redditi, e altra documentazione da cui possono risultare anche dati sulla salute dei dipendenti, nonché sulla loro appartenenza ad organizzazioni sindacali o politiche;
- dati contabili su rapporti fiduciari, conti correnti, e posizioni fiscali;
- dati inerenti la gestione patrimoniale, ed eventuali carichi pendenti/condanne degli amministratori e soci della società;
- dati relativi a contenziosi, vertenze e denunce in essere con terzi, dipendenti, collaboratori, consulenti ed Autorità;
- dati sensibili relativi a soggetti che sono stati coinvolti ad esempio in attività di studio, ricerca scientifica, opere di ingegno;
- dati personali dei soggetti da identificare ai fini dell'antiriciclaggio.

Su tali dati il revisore svolge analisi di correttezza aritmetica, di verifica di congruità con contratti e norme applicabili, e con i principi contabili utilizzati per la predisposizione del bilancio, e svolge un esame critico delle informazioni raccolte. In taluni casi il revisore richiede a terzi la conferma delle informazioni raccolte presso la società. Le procedure sono finalizzate alla successiva emissione della relazione sul bilancio nel suo complesso. Le funzioni ed i soggetti che trattano tali dati sono, oltre ai professionisti assegnati all'incarico, il personale di segreteria, le funzioni preposte agli adempimenti normativi specifici (quali antiriciclaggio, controllo di qualità, risorse umane ed amministrazione del personale), le Autorità di vigilanza, i soggetti preposti alla gestione dei sistemi informatici, i soggetti preposti all'archiviazione delle carte di lavoro, altri membri della rete che partecipano all'incarico in ragione delle loro specifiche competenze professionali (ad esempio, attuari, esperti fiscali, etc.).

I dati sono sottoposti a rielaborazioni e ricalcoli, sia manuali che mediante l'utilizzo di strumenti informatici, e successivamente archiviati nel rispetto delle norme di conservazione dei documenti fiscali e dei principi di revisione.

Nei casi in cui il *core business* della società sia il trattamento di dati personali, questi potrebbero essere raccolti e rielaborati in parte dal revisore per verificare l'accuratezza e la completezza delle procedure che potrebbero avere impatto sul bilancio.

Per quanto riguarda il trasferimento delle carte di lavoro (e relativi eventuali dati personali che fossero ivi presenti), i revisori fanno riferimento alle specifiche *policies* per i trasferimenti all'interno della propria rete di appartenenza, emanate dalle funzioni interne incaricate oppure dagli stessi *Network* a livello globale (es. sulla base delle clausole tipo della Commissione Europea oppure di *binding corporate rules*), e in linea generale alle normative applicabili nei paesi di riferimento (*Infra UE o Extra UE*).

9. CRITERI PER INDIVIDUARE IL RUOLO DELLA SOCIETÀ DI REVISIONE COME TITOLARE O RESPONSABILE DEL TRATTAMENTO DEI DATI

Diversi *regulators* europei hanno emanato delle linee guida per individuare quando revisori, dottori commercialisti, consulenti agiscono come titolari o responsabili del trattamento. In particolare, il Gruppo di lavoro "articolo 29" (o *Working party 29*), sostituito ora dal Comitato europeo per la protezione dei dati, ha affermato che[4] il ruolo tradizionale e l'esperienza professionale del fornitore di servizi svolgono un ruolo predominante, che può comportare la sua qualifica di titolare del trattamento dei dati.

La capacità di "determinare gli scopi e i mezzi ..." può derivare da diverse circostanze legali e/o fattuali: una competenza legale esplicita (quando la legge nomina il titolare del trattamento o conferisce un compito o dovere di raccogliere ed elaborare determinati dati); disposizioni legali comuni o ruoli tradizionali esistenti che normalmente implicano una certa responsabilità all'interno di determinate organizzazioni (...); circostanze di fatto e altri elementi (come i rapporti contrattuali, il controllo effettivo di una parte, la visibilità verso gli interessati, ecc.).
Il *Working Party 29* ha fatto inoltre riferimento a criteri che possono aiutare a determinare il ruolo delle parti nell'ambito della legislazione sulla privacy.

L'autorità francese[5] per la protezione dei dati ha fornito ulteriori spiegazioni che possono essere riassunte come segue:

1) Livello di istruzioni preliminari: il grado di autonomia della società di revisione dipende dal livello delle istruzioni fornite dal cliente. Se i servizi sono forniti sulla base di istruzioni molto generali la società di revisione può essere titolare del trattamento, se i servizi sono forniti sulla base di istruzioni molto dettagliate agisce come responsabile del trattamento dati.
2) Livello di monitoraggio: il monitoraggio da parte del cliente sui servizi e i dati possono rivelare se la società di revisione agisce come titolare del trattamento o come responsabile. Se la società di revisione non è monitorata dal cliente sul modo in cui utilizza i dati può essere considerata titolare del trattamento, se invece il cliente può eseguire controlli e richiedere alla società di revisione di riferire regolarmente sul suo lavoro e su come sono stati utilizzati i dati potrebbe essere considerata responsabile del trattamento.
3) Trasparenza: la prestazione dei servizi da parte della società di revisione è visibile o meno agli interessati, ed è permesso alla stessa di utilizzare i dati per l'incarico ricevuto, incluse le procedure ausiliari ad esso relative (*conflict check, quality review, document retention*, ecc.). Se la società di revisione agisce in nome proprio e non per conto del cliente e può utilizzare i dati per lo svolgimento del proprio incarico, nonché per l'adempimento delle altre procedure ausiliarie può essere considerata titolare del trattamento, se invece opera per conto del cliente (nel suo nome) e non può utilizzare i dati per lo svolgimento del proprio incarico, nonché per l'adempimento delle altre procedure ausiliarie potrebbe essere responsabile del trattamento.

---

[4] *Opinion* 1/2010 del *Working Party 29*
[5] CNIL – *Les questions posées pour la protection des données personnelles par l'externalization hors de l'Union Europeenne de traitements informtiques del 9 settembre 2010.*

4) Livello di competenza: se i servizi forniti dalla società di revisione richiedono un livello elevato di esperienza, il cliente potrebbe non essere in grado di determinare le modalità del trattamento. Se la società di revisione decide autonomamente come elaborare i dati ed il cliente non può modificarli in quanto non ha le competenze appropriate può essere considerata titolare del trattamento.

10. RUOLO DELLA SOCIETÀ DI REVISIONE NELL'AMBITO DELLA NORMATIVA SULLA PROTEZIONE DEI DATI PERSONALI

Tenuto conto del quadro normativo e regolamentare in cui opera la società di revisione e dei criteri sopra citati risulta che il revisore o la società di revisione **nell'ambito dell'incarico di revisione** (legale o volontaria) e degli incarichi disciplinati da Leggi o Regolamenti:

- ottiene i dati che lui stesso ritiene necessari per poter svolgere l'incarico di revisione;
- effettua una scelta autonoma del trattamento dei dati in base alle necessità di completamento dell'incarico nel rispetto delle finalità stabilite dalla normativa in materia, in applicazione dei principi di revisione di riferimento;
- è tenuto all'obbligo di segreto professionale;
- deve documentare il proprio lavoro con apposite carte di lavoro che contengono i dati raccolti e che restano di proprietà del revisore che è tenuto a conservarle;
- deve poter rendere disponibili le proprie carte di lavoro, contenenti i dati, alle Autorità e ad altri soggetti, in applicazione di norme di legge che prevedono trattamenti specifici (es. trasferimenti ad altri revisori);

pertanto ricopre, ai fini della nuova normativa Protezione dei Dati Personali, il ruolo di **Titolare Autonomo** secondo la definizione riportata all'art. 4 n. 7 del GDPR.

La società di revisione esprime il proprio giudizio professionale in modo indipendente, ha un alto livello di competenza e deve essere autonoma nello svolgimento delle proprie attività, agendo in conformità alle disposizioni legislative e regolamentari e agli obblighi professionali. Per eseguire il lavoro per il quale è stato incaricato, il revisore determina:

- se i dati personali devono essere elaborati;
- quali elementi di dati personali saranno necessari (il contenuto dei dati);
- la finalità e la modalità con cui saranno elaborati (ovvero come il *team* di revisione utilizzerà i dati);
- per quanto tempo dovranno essere conservati (i dati personali contenuti nei documenti di lavoro saranno conservati per la durata del periodo di prescrizione legale, in conformità con le regole professionali applicabili alla società di revisione).

Inoltre, la Società di revisione risponde del contenuto del lavoro svolto per il cliente.

Nell'ambito dei servizi oggetto di analisi del presente Documento, il revisore non può quindi mai essere qualificato come responsabile del trattamento come definito ai sensi dell'art. 4 n. 8 del GDPR, ovvero come la "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

L'inquadramento della società di revisione come responsabile del trattamento comporterebbe infatti il venir meno dei requisiti di autonomia ed indipendenza che caratterizzano l'attività stessa del revisore e che costituiscono principi fondamentali cui il revisore deve attenersi nello svolgimento dell'incarico.

Inoltre, in relazione alla sua qualifica di titolare del trattamento, la società di revisione:

- non è tenuta a fornire un'informativa agli interessati i cui dati sono oggetto di trattamento in relazione all'incarico, ai sensi dell'art. 14, paragrafo 5, lett. a), c) e d) del GDPR;
- non deve richiedere il consenso degli interessati per l'utilizzo dei dati stessi, ai sensi dell'art. 6, paragrafo 1.

In conclusione, alla luce delle considerazioni sopra svolte e dei criteri enunciati, la società di revisione nello svolgimento dell'incarico di revisione (legale e volontaria), nonché ai fini dell'adempimento delle altre procedure ausiliarie e degli altri incarichi disciplinati da leggi o regolamenti, si configura quale titolare autonomo del trattamento.

In questo senso si è espressa anche Accountancy Europe che afferma "*Accountancy Europe believes that in principle, auditors qualify as data controllers in their own right*" e che così conclude: "*Statutory auditors decide how they process data obtained from their audit clients and are therefore considered data controllers in their own right under GDPR*"[6].

Febbraio 2019

[6] Accountancy Europe, Position Paper "GDPR: Implications for auditors", December 2018.
In particolare, *"Accountancy Europe believes that in principle, auditors qualify as data controllers in their own right.*
Statutory audit legislation obliges auditors to be independent [of their audit clients] and for this reason, auditors are the ones that decide what data they need to perform the audit and how the data is used, stored, etc. Additionally, the auditor and client do not jointly determine the purposes and means of the processing, the purposes being determined by law and regulations. Therefore, auditors in the framework of statutory audit should be considered data controllers.
As a consequence, auditors should not enter into a data processing agreement with their audit clients, but are obliged to set up a privacy policy and notify their clients by including a data protection clause in the engagement letter. This privacy policy should clarify their role and responsibilities as data controllers in their own right."