FEDERAZIONE CONFSAL-UNSA
COORDINAMENTO NAZIONALE BENI CULTURALI
c/o Ministero dei beni e delle attività culturali e del turismo
Via del Collegio Romano, 27 - 00186 Roma
Tel. 06.67232889 - Tel./Fax 0667232348 – Fax Tiscali 1786070337
info@unsabeniculturali.it – www.unsabeniculturali.it

BOLLETTINO SINDACALE
N. 3 DEL 26 SETTEMBRE 2019

ASPETTI CONTRATTUALI ED ESEMPI PRATICI NEL GDPR DEL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento è una figura che già era presente nel Codice Privacy, ma che viene investita di alcune novità nel regolamento europeo GDPR. Utile approfondire il rapporto con il titolare, i compiti che è chiamato a svolgere e le regole per il suo ingaggio

Una delle figure più rilevanti nell'ambito della protezione dei dati personali è quella del **responsabile del trattamento**, già presente nel Codice Privacy (D.lgs.196/2003) e ripresa con alcune novità dal Regolamento UE 679/2016 (GDPR).

Nello specifico, la novità principale si traduce nel **rapporto tra il responsabile e il titolare del trattamento**: infatti, come previsto dall'articolo 28 del GDPR, è il titolare stesso che designa il responsabile del trattamento, attraverso un contratto o altro atto giuridico vincolate, non più sulla base di una nomina meramente facoltativa, ma obbligatoria.

Pertanto, **la qualificazione giuridica di questo rapporto risulta essere quella di mandato**. L'impatto del GDPR ha portato novità anche per quel che attiene ai profili di responsabilità del responsabile del trattamento, il quale soggiace a specifici obblighi, tra cui ad esempio quello di designare un DPO, ove ne ricorrano i presupposti necessari.

Alla luce di ciò, occorre rivedere i contratti tra titolare e responsabile del trattamento stipulati prima del GDPR e adeguarli al nuovo quadro normativo; nonché stipularne di nuovi sulla base di un'adeguata valutazione del rischio da parte del titolare per il trattamento posto in essere.

Il responsabile del trattamento: contesto normativo

Occorre, innanzitutto, soffermarsi sulla definizione che il GDPR fornisce sia di titolare del trattamento sia di responsabile del trattamento, per poter definire gli **aspetti contrattuali che legano queste due figure**.

Il titolare del trattamento è definito dall'articolo 4, n. 7 del GDPR come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati Membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli Stati membri*".

Il responsabile del trattamento è invece definito **all'articolo 4, n.8 del GDPR** come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare del trattamento"*.

L'articolo 28 del Regolamento prevede anche che il responsabile del trattamento presenti delle "*garanzie sufficienti"* per mettere in atto misure tecniche e organizzative adeguate, nonché garantire la tutela dell'interessato. L'articolo 28, comma 2 del GDPR stabilisce, inoltre, che il responsabile del trattamento non possa ricorrere ad un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare.

Altro elemento previsto dall'articolo 28, comma 3 del GDPR, si rinviene nella designazione: infatti, nello specifico i trattamenti effettuati da parte del responsabile del trattamento **sono disciplinati da un contratto** o da altro atto giuridico a norma del diritto dell'Unione o degli Stati Membri, che vincola il responsabile del trattamento al titolare del trattamento e stabilisce la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e diritti del titolare del trattamento.

Il ruolo del responsabile del trattamento nel Codice Privacy

La figura del responsabile del trattamento era già presente nel quadro normativo delineato dal D.lgs. 196/2003 ("Codice Privacy").

Nello specifico, il Codice Privacy – precedente al D.lgs. 101/2018 – individuava all'articolo 4, comma 1, lett. g, il responsabile come "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*".

Inoltre, ai sensi dell'articolo 29 del Codice Privacy, **il responsabile poteva essere designato dal titolare facoltativamente**, e se designato era individuato tra soggetti che per esperienza, capacità ed affidabilità fornivano **idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento**, compreso il profilo relativo alla sicurezza.

In questo scenario, **il rapporto tra titolare e responsabile si basava su una nomina meramente facoltativa**, con una natura esclusivamente privatistica. La figura in esame era quindi eventuale, ed il titolare stesso poteva decidere se avvalersi o meno di un altro soggetto al fine di ottemperare agli obblighi in materia di trattamento dei dati personali.

Nella prassi applicativa italiana si distingueva tra c.d. responsabile interno e c.d. responsabile esterno "*a seconda che l'individuazione avvenisse tra dipendenti e collaboratori del Titolare oppure nei riguardi di un soggetto terzo*".

Il problema dell'inquadramento del responsabile come soggetto interno o esterno era stato affrontato anche dalla *Commission nationale informatique et libertés* (l'autorità per la protezione dei dati francese anche indicata con l'acronimo CNIL), la quale aveva richiamato il parere 1/2010 sui concetti di "*controller*" e "*processor*" del *Working Party Article* 29 (in seguito anche WP29), per interpretare se quel "*trattare i dati per conto del titolare*" potesse includere anche i soggetti interni alla sua struttura.

Occorre precisare che nel richiamare il parere 1/2010 del WP29, si renderà sempre con "titolare" e "responsabile" i termini "controller" e "processor", sostituendo direttamente la differente terminologia utilizzata nelle traduzioni ufficiali.

In particolare, si stabiliva all'interno del parere 1/2010 che l'esistenza di un responsabile del trattamento dipendesse da una decisione presa dal titolare del trattamento.

Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione (c.d. responsabile interno), ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità, oppure di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna (c.d. responsabile esterno), ovverosia ad una *"persona giuridicamente distinta dal Titolare, ma che agisce per conto di quest'ultimo"*.

Il CNIL propendeva per la sola figura del responsabile esterno, inquadrando i rapporti tra titolare e responsabile generalmente in termini di fornitore/cliente.

Nella vigenza del Codice Privacy, la figura del responsabile interno, così come del responsabile esterno del trattamento, non ha mai trovato una definizione a livello normativo. Nonostante ciò, nella prassi la figura del responsabile interno è risultata compatibile con la definizione di responsabile del trattamento presente nella Direttiva 95/46/CE e nel Codice Privacy previgente.

Con il GDPR, in assenza di un'espressa previsione legislativa, spetta all'interprete valutare la compatibilità di dette figure con il mutato quadro normativo: nello specifico, si propende per **un'incompatibilità della figura del responsabile interno con la nuova disciplina, ammettendone la sola esternalizzazione**.

In particolare, alcuni degli obblighi previsti dal GDPR, come ad esempio la nomina di un DPO, oppure la nomina di un rappresentante nel territorio europeo risultano pensati solo per un soggetto esterno alla struttura del titolare; così come molti degli obblighi previsti dall'articolo 28, paragrafo 3, come

assistere il titolare nell'adozione di misure tecniche ed organizzative (art. 28, paragrafo 3, lett. e); oppure l'obbligo di consentire al titolare lo svolgimento di ispezioni e controlli (art.28, par.3. lett.h), sembrano indirizzare l'interprete nel propendere per la sola figura di un responsabile del trattamento esterno.

La figura del responsabile del trattamento nel GDPR

La figura del responsabile del trattamento all'interno del Regolamento (UE) 679/2016 ha una nuova collocazione: è definita dagli articoli 4, n.7) e dell'articolo 28 del GDPR.

L'articolo 28 del GDPR stabilisce i requisiti soggettivi del responsabile del trattamento, che dovrà:

1. fornire le "garanzie sufficienti" per mettere in atto le misure tecniche ed organizzative adeguate;
2. garantire la tutela dei diritti dell'interessato.

Il GDPR, pur non innovando l'essenza della figura del responsabile del trattamento, ne attribuisce "maggiore rilevanza esterna e maggiore responsabilità nella gestione del trattamento dei dati".

Secondo quanto stabilito dall'articolo 28, comma 3 del GDPR, il Responsabile è nominato dal Titolare del trattamento tramite "*contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

In altre parole, "tale accordo previsto dall'articolo 28 del GDPR da concludersi in forma scritta e volto a regolare i rapporti tra data controller e data processor è sovrapponibile a quello che in Italia, fino ad oggi, è noto come *nomina a responsabile esterno del trattamento*."

Nello specifico, il contratto o ogni altro atto giuridico prevede che il responsabile del trattamento:

1. tratti i dati personali soltanto *su istruzione documentata del Titolare*, salvo se lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento: secondo parte della dottrina, tale obbligo di ricevere istruzione documentata da parte del Titolare sembrerebbe imporre in capo al Responsabile la necessità di documentare le istruzioni ricevute, al fine di dimostrare di aver agito conformemente al GDPR; comportando che, anche a fronte di istruzioni ricevute oralmente, in situazioni di urgenza, graverebbe sul responsabile l'onere di documentare dette istruzioni in un momento successivo;
2. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3. adotti tutte le misure di sicurezza del trattamento, previste dall'articolo 32 del GDPR;
4. rispetti le condizioni previste per ricorrere ad un altro responsabile del trattamento (cioè "rispetti i limiti dell'autorizzazione speciale o generale e ingaggi il sub-processor in modo tale che ribalti back to back gli obblighi e le garanzie che cadono sul primo responsabile");

5. tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (previsti al Capo III del GDPR);

1. assista il titolare del trattamento nel garantire il rispetto degli obblighi previsti per la sicurezza dei dati personali, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

2. su scelta del titolare cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

3. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti in capo al responsabile del trattamento, e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Con riguardo a quest'ultimo punto, il responsabile del trattamento informerà direttamente il titolare qualora un'istruzione violi il GDPR o altre disposizioni nazionali o dell'Unione relative alla protezione dei dati.

Inoltre, "in alcuni contratti di *outsourcing*, attività di questo tipo sono espressamente escluse, mentre l'accordo controller – processor, che deriva dalla norma dell'articolo 28 del GDPR, va espressamente in direzione opposta.

A seconda che si tratti di un accordo *client-oriented* o *provider-oriented* è facile aspettarsi conseguenze diverse in caso di mancata informazione da parte del processor al controller in merito a possibili violazioni di legge".

La designazione del sub-responsabile

Una grande novità del GDPR è quella prevista dal comma 2 dell'articolo 28: **il responsabile del trattamento può designare un altro responsabile del trattamento, il cosiddetto "sub-responsabile"**, previa autorizzazione, specifica o generale, scritta del titolare del trattamento.

In tal caso, il responsabile risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, e anche ai fini del risarcimento, di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile, così come previsto dall'art. 28, comma 4, del Regolamento.

Sulla base di ciò, **il rapporto tra responsabile e sub-responsabile risulta un rapporto gerarchico**.

Inoltre, i paragrafi 7 e 8 dell'articolo 28 prevedono la possibilità che la Commissione europea o le autorità di controllo nazionali adottino clausole contrattuali tipo per la designazione del responsabile, che riproducono i contenuti minimi indicati al paragrafo 3 dell'articolo 28.

Come sostenuto dalla dottrina, l'obiettivo è quello di introdurre uno strumento che tuteli non solo le parti dell'accordo, ma anche i terzi la cui sfera giuridica potrebbe essere lesa dagli effetti dell'accorso sul trattamento dei dati concluso tra controller e processor.

In aggiunta, il nuovo quadro legislativo stabilisce che **il responsabile del trattamento condivide in certa misura le responsabilità del titolare del**

trattamento in ordine al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative, a differenza di quanto previsto dal Codice Privacy – previgente alle modifiche operate dal D.lgs. 101/2018 – in cui la sanzione amministrativa era sempre diretta nei confronti del titolare.

Il rapporto giuridico tra titolare e responsabile

Il rapporto tra titolare e responsabile del trattamento **si basa su un contratto o altro atto giuridicamente vincolante**, come previsto dall'articolo 28 del GDPR. Questo significa che il titolare del trattamento è invitato ad effettuare una compiuta valutazione di rischio anche nella nomina del responsabile.

Il GDPR impone, di fatto, di **rivisitare i contratti tra titolare e responsabile del trattamento dati**; oppure, in caso di nuovi rapporti, stipulare nella fase iniziale anche i contratti e gli atti giudici vincolanti necessari.

Infatti, il titolare ha l'obbligo di valutare il rischio dei trattamenti che pone in essere, sia nella fase in cui li progetta che durante il periodo del loro svolgimento. Valutazione, questa, essenziale per consentire al titolare di adottare le misure tecniche e organizzative adeguate ai rischi che i trattamenti possono comportare per le libertà e i diritti delle persone (art. 24 del GDPR).

È chiaro che, per poter fare tale valutazione di rischio, e nei casi previsti dall'art.35, anche la valutazione di impatto, il titolare deve tenere conto anche della parte dei trattamenti che intende affidare ad esempio in *outsourcing* a soggetti esterni, che assumono la posizione di responsabili.

In questo quadro, egli deve tener conto anche del contenuto dei contratti o degli atti giuridici vincolanti che intende stipulare con essi, al fine di verificare quali siano i singoli impegni da questi assunti, e quali le modalità con cui, sia pure sotto il suo controllo e seguendo le sue istruzioni, tratteranno i dati.

Non a caso tra gli obblighi del responsabile dei trattamenti previsti dall'articolo 28, paragrafo 3, lettera c), vi è anche quello di adottare tutte le misure richieste per garantire la sicurezza dei trattamenti di cui all'art. 32.

È previsto inoltre l'obbligo per il responsabile di assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui dagli articoli da 32 a 36 e dunque:

1. misure di sicurezza;
2. ***data breach*** e segnalazione ad Autorità di controllo e agli interessati;
3. **valutazione di impatto**;
4. consultazione preventiva dell'Autorità di controllo nei casi stabiliti dall'art. 36.

Il responsabile del trattamento diventa così un ruolo il cui svolgimento concorre in modo determinante a definire le caratteristiche delle modalità di trattamento dei dati, al fine di valutare il rischio che il trattamento comporta e adottare le misure adeguate.

Tuttavia, una volta chiarito che il responsabile può essere solo una figura esterna, distinta e separata dall'organizzazione del titolare, come del resto fin dal 2010 aveva ben chiarito il *Working Party29* nella sua *Opinion*, si precisa che l'espressione "intervenire *per conto di*" significa servire gli interessi di un altro soggetto, evocando cosi il concetto giuridico di mandato.

La designazione a responsabile del trattamento appare dunque riconducibile all'istituto del mandato, (artt. 1703 e ss. c.c.), che si presume a titolo oneroso (art. 1709 c.c.).

L'art. 1708 del c.c. prevede che il mandato comprende non solo gli atti per cui è stato conferito, ma anche quelli che sono necessari al loro compimento.

È un atto di autonomia privata, avente natura negoziale in ambito privato, con cui si attua una distribuzione di compiti e una ripartizione di competenze (e quindi anche di responsabilità). La designazione a responsabile del trattamento potrà quindi ritenersi a tutti gli effetti valida a condizione che essa:

1. risulti da atto scritto recante data certa;
2. il responsabile possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni attribuite;
3. conferisca al responsabile tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni attribuite.

Interessante è l'inquadramento della nomina di responsabile come elemento accessorio di un contratto di appalto, ad esempio quando la nomina di responsabile avviene nell'ambito di un contratto che prevede l'incarico per lo sviluppo e la manutenzione di un sistema informatico integrato.

In questo caso, laddove il trattamento dei dati sia inscindibilmente connesso all'oggetto della prestazione dell'appaltatore, le norme del mandato lasciano probabilmente strada a quelle dell'appalto.

Si pensi, ad esempio, alle norme che regolano la revisione del corrispettivo per le variazioni necessarie al progetto (art. 1660 c.c.) che prevedono l'intervento del giudice in assenza di accordo tra le parti, o qualora l'importo superi 1/6 del corrispettivo complessivo, legittimano l'appaltatore a recedere ed a richiedere una equa indennità, o il committente a recedere e corrispondere un equo indennizzo.

O ancora si pensi alla garanzia prevista dall'art. 1668 c.c. per difetti dell'opera, intendendosi per difetti ad esempio un sistema informatico non *compliant* con il GDPR.

La responsabilità del responsabile del trattamento

Il responsabile del trattamento, ai sensi dell'articolo 82, "*risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*".

Per chiarezza, occorre premettere che **il GDPR pone dei nuovi obblighi gravanti direttamente sul responsabile del trattamento dei dati**, che non discendono dalla delega di un'attività operata dal titolare e da cui derivano specifiche sanzioni se non rispettati.

In particolare, il responsabile del trattamento è tenuto a:

1. adottare misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, e precisamente le misure richieste dall'articolo 32 del GDPR;
2. istituire un **registro dei trattamenti** per conto di ciascun titolare (art. 30, par.2 del GDPR);

3. designare un responsabile per la protezione dei dati personali, ove ne ricorrano i presupposti (art.37 e ss. del GDPR);
4. nominare un rappresentante, qualora non sia stabilito nel territorio europeo (art. 27, par.1 del GDPR);

1. cooperare con le autorità di controllo (art. 31 del GDPR).

Tra le obbligazioni condivise con il titolare, rientrano quella di adottare idonee misure di sicurezza, cooperare con il titolare per le valutazione d'impatto (DPIA) e/o in caso di *data breach*.

In caso di violazione dei predetti obblighi, il responsabile è passibile di una sanzione amministrativa pecuniaria di ammontare fino a euro 10.000.000,00 o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art.83, par.4 GDPR).

Pertanto, in merito al regime di responsabilità del responsabile del trattamento, quest'ultimo ne risponderà nel caso di violazione di un obbligo previsto dal GDPR, ovvero per violazione di un obbligo contrattuale.

A titolo di esempio, l'adozione di misure di sicurezza adeguate è un obbligo posto sia in capo al titolare sia al responsabile: pertanto, ai fini della responsabilità, è fondamentale regolare nel dettaglio all'interno del contratto gli obblighi del titolare e del responsabile in relazione alle misure di sicurezza.

Ove tuttavia tale previsione non vi sia, né nel contratto, né nella lettera di nomina di responsabile, la valutazione della responsabilità di tale violazione deve seguire ragionevolmente i comuni principi relativi alla imputabilità (colpa o dolo) e della conseguente responsabilità.

Infatti, l'obbligo di adottare appropriate misure di sicurezza è ritenuto una obbligazione di mezzi per la quale pertanto si applicano i criteri generali sulla imputabilità e sulla responsabilità.

Le clausole contrattuali

È fondamentale avere nei contratti di durata **una clausola che preveda la «successione nel tempo» delle leggi** in modo da garantire la *compliance* del responsabile agli obblighi in base alla previsioni legislative che si succedono nel tempo.

Si pensi, ad esempio, ai contratti di durata pluriennale, sottoscritti prima del GDPR, quando il responsabile aveva un diverso e minore compito da svolgere rispetto a quelli imposti dal GDPR, ma che continuano quindi ad operare dopo il GDPR, quando invece il responsabile è più onerato.

Una clausola ben strutturata può consentire di regolare in modo adeguato questi nuovi impegni del responsabile, limitarne l'impatto, prevederne il corrispettivo.

Da un diverso punto di vista, per altro si potrebbe anche sostenere che in alcuni casi il contratto di nomina del responsabile, sottoscritto prima del GDPR, possa essere eventualmente risolto per eccessiva onerosità laddove l'adempimento degli obblighi previsti dal GDPR sia eccessivamente oneroso per il soggetto responsabile, o egli non abbia una adeguata struttura o competenza per far fronte agli impegni previsti dal GDPR.

Aspetti contrattuali di rilievo: casi concreti

Nel rapporto tra titolare e responsabile del trattamento problemi possono sorgere proprio in relazione ai profili di responsabilità, legati ad esempio alla

validità di clausole contrattuali preesistenti all'entrata in vigore del GDPR, oppure legate alla ripartizione di responsabilità laddove non espressamente previsto nel contratto. Un esempio concreto potrebbe essere il seguente:

La società Beta effettua – sui sistemi informatici del cliente Alpha e nell'ambito di un contratto in essere con quest'ultimo – operazioni di trattamento di dati personali di titolarità del cliente Alpha stesso. La società Beta è stata nominata responsabile del trattamento da parte del cliente Alpha, titolare del trattamento. Prima della definitiva entrata in vigore del GDPR, la società Beta segnala al cliente la necessità di mettere in atto, sui sistemi del cliente Alpha utilizzati per il trattamento da parte della società Beta, nuove o più robuste misure tecniche e organizzative al fine di garantire, una volta entrato in vigore il GDPR, un livello di sicurezza adeguato al rischio esistente (art. 32 GDPR).

In caso di assenza di una pattuizione contrattuale espressa che ponga a carico di una delle parti i costi di adeguamento, la valutazione dovrà essere necessariamente effettuata sulla base del caso concreto e dunque sulla tipologia di misure proposte e sulla loro stretta necessità rispetto ai compiti delegati alla società Beta nel contratto.

Laddove si dovesse ritenere che le misure che la società Beta intende implementare non sono strettamente necessarie all'esecuzione del mandato medesimo o comunque eccessive rispetto ad una valutazione di adeguatezza ai sensi dell'art. 32 del GDPR, esse possano essere economicamente imputabili alla società Beta.

Diversamente, qualora ricadano in misure che debbono essere poste in essere per adempiere al mandato e siano strettamente necessarie per garantire la *compliance* all'art. 32 del GDPR, queste possano essere ragionevolmente poste a carico della società Alpha.

Un ulteriore esempio concreto potrebbe essere il caso in cui alla società Beta sia richiesto di "adottare tutte le necessarie misure di sicurezza".

In tal caso, ai sensi dell'art. 32 del GDPR che prevede che le misure di sicurezza adeguate siano adottate dal titolare e dal responsabile, la società Beta potrebbe essere tenuta a adottare tali misure proprio per adempiere al mandato e poiché il mandato, ai sensi del contratto stipulato dalle parti in tal caso, si intende a titolo oneroso, avrebbe titolo per richiedere il relativo compenso alla società Alpha.

Tuttavia, occorrerà verificare se nella lettera di nomina di responsabile non sia comunque precisato che tale nomina avviene a titolo gratuito. In tal caso, sarà più difficile sostenere che l'adeguamento preveda un impegno economico aggiuntivo da parte della società Alpha.

Del pari sarà più difficile richiedere il pagamento alla società Alpha dell'upgrade di sicurezza, laddove nella lettera di nomina a responsabile o nel contratto il perimetro delle misure di sicurezza sia già esattamente delineato, e con esso l'ambito del mandato. In tal caso, infatti, si potrebbe applicare l'art. 1711 c.c. con la conseguenza che, eccedendo il mandato, tali attività siano imputabili al mandatario e dunque i relativi costi rientrino nel portafoglio del mandatario.

L'art. 1712 c.c. prevede comunque che il mandatario debba comunque senza ritardo comunicare al mandante l'esecuzione del mandato e il ritardo del mandante a rispondere dopo aver ricevuto tale comunicazione per un tempo superiore rispetto a quello richiesto dalla natura dell'affare o dagli usi importa approvazione anche se il mandatario si è discostato dalle istruzioni o ha ecceduto i limiti del mandato.

Pertanto, laddove la società Beta abbia adottato tali misure, per essere in *compliance* con l'art. 32 del GDPR e evitare qualsiasi rischio di sanzioni, sarebbe comunque consigliabile che la società Beta desse tempestiva comunicazione alla società Alpha di tale condotta così che, nell'ipotesi in cui la società Alpha non dovesse rispondere alcunché in un tempo ragionevole, la società Beta potrebbe invocare a suo favore la previsione dell'art. 1712 c.c. e dunque pretendere che i relativi oneri siano a carico di Alpha.

Ancora, sempre in termini di ripartizione delle responsabilità tra titolare e responsabile, potrebbe verificarsi la seguente fattispecie: qualora la società Beta abbia segnalato al cliente Alpha che le misure di sicurezza che ha adottato non risultano conformi a quanto previsto dal GDPR, il grado di responsabilità di Alpha potrebbe assurgere a livello di dolo o della colpa grave e limitare se non escludere di conseguenza la responsabilità di Beta.

Inoltre, la società Beta potrà liberarsi avendo dimostrato di aver agito con la massima diligenza e fatto quanto era nelle sue possibilità per attivare tali misure e dunque andare esente da dolo, ma anche da colpa, laddove materialmente impossibilitata ad eseguire l'upgrade di sicurezza che suggerire al cliente Alpha di svolgere.

Dall'analisi di queste fattispecie, risulta necessario che il titolare sia chiamato a rivisitate i contratti posti in essere prima del GDPR, ed i successivi basarli su un'attenta valutazione del rischio che può generare il trattamento dei dati.

A cura dell'Avv. UE Teodoro CALVO