ISSN 2531-8950

Anno IX - 2024 n. 1

NUOVO DIRITTO CIVILE

ALBERTO M. GAMBINO, ELENA MAGGIO, DAVIDE MULA

Il contratto di designazione tra titolare e responsabile del trattamento: le clausole contrattuali tipo

DIKE GIURIDICA

Alberto M. Gambino, Elena Maggio, Davide Mula
(Professore ordinario nell'Università Europea di Roma –
Avvocato, Ph.D., Data Protection Officer e Auditor –
Professore a contratto nell'Università Europea di Roma)

Il contratto di designazione tra titolare e responsabile del trattamento: le clausole contrattuali tipo* **

Sommario: 1. La figura del responsabile del trattamento nel GDPR. - **2.** La forma dell'atto di designazione. - **3.** Le clausole contrattuali tipo adottate dalla Commissione europea*:* 3.1 Analisi delle clausole; 3.2 Analisi degli Allegati.

1. La figura del responsabile del trattamento nel GDPR

L'art. 4, n. 8, del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, di seguito anche "Regolamento" o "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*» riproponendo in maniera pressoché identica la definizione contenuta all'art. 2, lett. *e)*, della direttiva 95/46/CE.

Il responsabile del trattamento è, in estrema sintesi, colui che, con una discrezionalità più o meno ampia nella definizione del *modus*, persegue le finalità di trattamento definite dal titolare. L'elemento caratterizzante la figura del responsabile del trattamento è, dunque, rappresentato dalla strumentalità della sua attività rispetto ai fini del titolare.

---

* Questo scritto, pur se unitariamente concepito, deve essere nelle sue parti così attribuito: A.M. Gambino §1, E. Maggio §4.1 e 4.2, e D. Mula §2, 3 e 4.

** Il contributo è stato sottoposto, in forma anonima, alla valutazione di due *referee*.

Il Regolamento del 2016, direttamente applicabile dal 2018, ha definito le caratteristiche soggettive e le responsabilità del responsabile del trattamento negli stessi termini di cui alla direttiva 1995/46/CE (e, quindi, al D.Lgs. 196/2003 di recepimento nella Legislazione italiana). L'unica differenza che appare dal confronto tra la nuova disciplina e quella che era contenuta nel previgente D.Lgs. 196/2003 è che viene meno la configurabilità dei c.d. responsabili interni, non potendosi attribuire tale qualificazione a soggetti interni all'organizzazione del titolare responsabilità tanto gravose, pari a quelle che possono essere imputate ad un soggetto esterno (1). Al fine di permettere la definizione di organigrammi gerarchici all'interno delle strutture organizzative complesse, il legislatore nazionale ha aggiunto, con il D.Lgs. 101/2018, al predetto D.Lgs. 196/2003 l'art. 2quaterdecies la figura del "designato" al quale il titolare può attribuire specifici compiti e funzioni connessi al trattamento di dati personali.

Come chiarito dall'*European Data Protection Board* (in italiano Comitato europeo per la protezione dei dati, di seguito anche "EDPB" o "Comitato") nelle "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate il 7 luglio 2021 (di sui anche "Linee guida") l'atto di designazione è elemento essenziale ai fini della qualificazione di un soggetto come responsabile del trattamento, ma non può dirsi altresì sufficiente, in quanto non può prescindersi da una valutazione concreta delle attività condotte da tale soggetto.

Infatti, qualora il responsabile, quand'anche designato dal titolare come tale, esorbiti dai compiti assegnatigli e tratti i dati per fini o con mezzi diversi da quelli indicati dal titolare, questo assumerà il ruolo di titolare del trattamento o, a seconda dei casi, di contitolare. Di converso, neanche la qualificazione negoziale di un soggetto come titolare di un trattamento di dati può dirsi elemento sufficiente ad escludere che detto soggetto tratti i dati per conto di un altro soggetto e che, quindi, nella sostanza, operi come suo responsabile.

Ad esempio, uno studio legale che tratta dati di una società per svolgere il compito di rappresentante legale deve essere considerato titolare del trattamento in ragione dell'elevato grado di autonomia che gli è riconosciuta nell'assolvere il compito richiesto (cfr. Linee guida, p. 14). Del pari, come chiarito a più riprese dal Garante per la protezione dei dati personali, è titolare autonomo il medico competente nominato ai sensi del D.Lgs. 81/2008 nell'ambito dei compiti di sorveglianza sanitaria che la legge gli attribuisce in via esclusiva, proprio in quan-

(1) Sul punto si veda F. Bravo, *Sulla figura del responsabile "interno" del trattamento di dati personali*, in *Dir. inf.*, 2019, p. 961; L. Conti. *Il ruolo del Responsabile del trattamento ("Data Processor") prima e dopo il Regolamento (UE) n. 2016/679 e il suo rapporto contrattuale con il titolare del trattamento ("Data controller")*, in *Diritto comunitario e degli scambi internazionali*, 2019, pp. 203 e ss.

to le finalità e le operazioni del trattamento che devono essere poste in essere dal medico sono determinate dalla legge (2).

Al contrario, come chiarito sempre dal Garante nel parere del 12 maggio 2020, l'Organismo di Vigilanza, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongono siano interni o esterni, è da considerare "parte dell'ente" e, pertanto, i singoli membri dell'Organo operano quali meri soggetti autorizzati ai sensi dell'art. 29 del GDPR (3).

È da qualificarsi, invece, come responsabile del trattamento il fornitore di servizi di localizzazione geografica (4), il gestore di una pagina di *social network* (5), il fornitore di servizi di posta elettronica (6) e quello di servizi di televigilanza (7).

2. La forma dell'atto di designazione

Ai sensi dell'art. 28, par. 3, del Regolamento, «*i trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del 26 diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, 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*». Inoltre, tale atto deve recare tutti gli impegni indicati al medesimo terzo paragrafo dell'art. 28 del GDPR (cfr. cons. 81 del GDPR). Il contratto o il diverso atto giuridico deve essere «*stipulato in forma scritta, anche in formato elettronico*» (cfr. art. 28, par. 9, del GDPR).

La forma scritta richiesta dalla citata norma non pare configurabile come un requisito *ad substantiam*, quanto, piuttosto, *ad probationem*, essendo la stessa richiesta al fine di provare l'*accountability* sostanziale del titolare. Ciò comporta che integra la forma scritta richiesta anche l'atto di designazione del responsabile sottoscritto mediante spunta apposta ad un'apposita casella in un formulario online predisposto dal nominando responsabile (si pensi ai contratti per adesione dei

(2) Sul punto si vedano GPDP provv. n. 194/2016, doc. web n. 5149198; GPDP provv. n. 273/2021, doc. web n. 9683814.
(3) Sul punto si rinvia a GPDP "*Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, D.Lgs. 8 giugno 2001, n. 231*", doc. web n. 9347842.
(4) GPDP provv. n. 370/2011, doc. web n. 1850581.
(5) Corte di giustizia dell'Unione europea, Grande sezione, 5 giugno 2018, Causa C-210/16, in A. Correra, *Dati personali: la nozione di "responsabile del trattamento" include il gestore di una "fanpage" presente su un "social network"*, in *DPCE online*, 2018, pp. 9 e ss.; M. Castellaneta, *Trattamento dati personali: l'amministratore di una Fanpage può essere responsabile insieme al social network*, in *Guida al Diritto*, 2018, pp. 96-98.
(6) GPDP provv. n. 547/2016, doc. web n. 5958296.
(7) GPDP provv. n. 559/2014, doc. web n. 3671057.

sistemi di gestione di posta elettronica sopra richiamati), in quanto la spunta può essere qualificata come firma elettronica semplice (8).

Nelle sopra menzionate Linee guida viene chiarito che «*poiché il regolamento stabilisce con chiarezza l'obbligo di stipulare un contratto scritto, qualora non sia in vigore nessun altro atto giuridico pertinente si ha una violazione del* [GDPR], *ovvero dell'art. 28, par. 9, del* [GDPR]». Considerato che «*sia il titolare sia il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento*», l'autorità di controllo compente, il Garante per la protezione dei dati personali per l'Italia, «*potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento*» (cfr. Linee guida, par. 103).

Grava, dunque, tanto sul titolare del trattamento, quanto sul responsabile del trattamento l'obbligo di stipulare il contratto che legittima il trattamento dei dati. Ciononostante, si osserva come in caso di omessa sottoscrizione del contratto di designazione il Garante sia solito sanzionare esclusivamente il titolare del trattamento, in quanto in via preliminare sullo stesso incombe l'obbligo di conformare il trattamento dei dati alle disposizioni del GDPR (9).

3. Le clausole contrattuali tipo adottate dalla Commissione europea

Dopo l'adozione del GDPR la Commissione, nell'ottica di armonizzare anche gli atti attuativi tra i vari Stati membri, ha adottato la Decisione di esecuzione (UE) 2021/915 del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento (di seguito, per brevità, anche "CCT") a norma dell'art. 28, par. 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'art. 29, par. 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio (di seguito anche "Decisione"), previo favorevole parere congiunto dell'*European Data Protection Board* e del Garante Europeo per la Protezione dei Dati, parere n. 1/2021.

---

(8) Cfr. G. Riccio, *Data Protection Officer e altre figure*», in S. Sica, V. D'Antonio, G.M. Riccio, *La nuova disciplina europea della privacy*, Padova, 2016, p. 46; sono d'accordo con l'Autore anche G. Scorza, M.L. Salvati, *commento sub art. 28 GDPR*, in *GDPR e normativa privacy*, E. Belisario, G. Riccio, G. Scorza, Milano, 2018, p. 270, e L. Bolognini, *commento sub art. 28 GDPR*, in *Codice della disciplina privacy*, L. Bolognini, E. Pelino, Milano, 2024, p. 197.

(9) GPDP provv. n. 264/2023, doc. web n. 9909702: «*Il trattamento dei dati personali effettuato dalla Società risulta infatti illecito, nei termini su esposti, con riferimento alla violazione dei principi di correttezza e di trasparenza (artt. 5, par. 1, lett. a), dell'art. 13 del Regolamento, stante la mancata comunicazione di informazioni adeguate in relazione al trattamento, nonché dell'obbligo del titolare in ordine alla designazione dei responsabili del trattamento (art. 28 del Regolamento)*».

Come si legge al considerando 2 della Decisione, infatti, la *ratio* della definizione delle CCT è da rinvenirsi nell'esigenza di «*assicurare un approccio coerente alla protezione dei dati personali in tutta l'Unione e la libera circolazione dei dati personali all'interno dell'Unione*» tenuto anche conto della possibilità di attingere ad un modello negoziale multilingua, che già risolve a monte eventuali problemi linguistici.

Le clausole trovano applicazione nei rapporti tra titolare e responsabile che siano soggetti al Regolamento e che si trovano all'interno dello Spazio Economico Europeo, o in Paesi verso i quali è stata assunta dalla Commissione una decisione di adeguatezza ai sensi dell'art. 45 del GDPR (10). Per regolare il rapporto tra titolare e responsabile del trattamento situato al di fuori dello SEE o in Paese rispetto al quale non è stata assunta una decisione di adeguatezza è possibile, invece, fare riferimento alle "*clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679*", c.d. *Standard Contractual Clauses*, adottate dalla Commissione Europea con Decisione di Esecuzione (UE) 2021/914 del 4 giugno 2021 ai sensi dell'art. 46, par. 2, lett. *c)*, del GDPR (11).

Le CCT si compongono di dieci articoli e di quattro allegati che recano sostanzialmente la trasposizione, arricchita alla luce dei considerati del GDPR, dei sopraindicati obblighi enucleati all'art. 28 del GDPR. Le stesse non sono modificabili nella loro formulazione, per quanto il considerando 6 della Decisione chiarisce che il titolare del trattamento e il responsabile del trattamento sono liberi di includere le CCT in un contratto più ampio e di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo o pregiudichino i diritti o le libertà fondamentali degli interessati.

Le Clausole sono formulate in modo che i redattori finali del contratto di designazione, in *primis* i rappresentanti del titolare che dialogheranno con quelli del responsabile, scelgano tra opzioni predefinite, il cui contenuto, come detto, non può essere modificato affinché sia riconosciuto il valore legale delle CCT. Il vantaggio di ricorrere alla CCT, infatti, risiede nella certa idoneità e correttezza delle stesse, per come enucleate con la Decisione.

Un ulteriore vantaggio è rappresentato dalla disponibilità di un modello di accordo che può essere conosciuto dagli interessati, affinché, in caso di palese violazione, possano agire direttamente nei confronti dei responsabili. Come rilevato da

(10) Sul punto di veda C. Bertoldi, *Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard*, in *federalismi.it*, 2022, pp. 1-26.

(11) Sulle clausole contrattuali tipo per il trasferimento dei dati si veda G.M. Riccio, *"Model contract clauses" e "corporate binding rules": valide alternative al "Safe Harbor Agreement"?*, in *Dir. inf.*, 2015, pp. 865-885.

autorevole dottrina, infatti, la responsabilità nei confronti dei terzi che discende dalla violazione di un obbligo contrattuale presuppone che l'accordo tra titolare e responsabile sia reso pubblico, almeno nei suoi tratti essenziali. Ciò pur non essendo rinvenibile nel Regolamento alcun obbligo di pubblicità dei contratti di designazione, a differenza di quanto previsto per la pubblicità dei contratti contitolari, ai sensi dell'art. 26, par. 2, del GDPR. Conseguentemente può ritenersi che i parr. 6, 7 e 8 dell'art. 82 del GDPR presuppongono l'impiego delle clausole contrattuali tipo, che sono note, almeno negli elementi essenziali, al soggetto interessato (12).

3.1 Analisi delle clausole contrattuali tipo

La **Clausola 1** definisce lo scopo e l'ambito di applicazione dell'accordo, rinvia agli Allegati da I a IV, che costituiscono parte integrante delle CCT, e chiarisce che l'adozione delle stesse lascia impregiudicati tutti gli obblighi ulteriori cui è soggetto il titolare del trattamento ai sensi del Regolamento, nonché che il ricorso alle stesse non garantisce di per sé il rispetto delle norme in materia di trasferimento dei dati. Costituiscono ulteriori obblighi *ex lege* per il responsabile del trattamento quello di tenuta del registro del trattamento, ai sensi dell'art. 30 del GDPR, e l'obbligo di cooperazione con l'autorità competente, ai sensi dell'art. 31 del GDPR. Il perimetro dello specifico contratto di designazione è dettagliato nell'Allegato II (v. *infra*).

La **Clausola 2** reca l'espresso vincolo delle parti a non modificare le CCT, se non per aggiungere o aggiornare le informazioni negli allegati (comma 1) o per aggiungere «*altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati*» (comma 2).

Le **Clausole 3** e **4** prevedono, rispettivamente, che le CCT siano interpretate e attuate in modo conforme al Regolamento e che qualora una clausola o una disposizione di accordi correlati tra le parti si ponga in contraddizione con le CCT prevalgano, in forza del principio gerarchico, queste ultime.

Di particolare interesse risulta essere la **Clausola 5** che reca la possibilità aderire alle clausole da parte di ulteriori soggetti durante tutta la vita del rapporto contrattuale. Ove accettata dalle parti, infatti, un'entità non parte delle clausole può, con l'accordo degli originari sottoscrittori, aderirvi (in qualità di titolare o responsabile) in qualsiasi momento, semplicemente compilando gli allegati e comunicando l'adesione. Questa clausola, l'unica delle CCT che le parti possono decidere di eliminare, risulta utile in caso di trattamenti successivi, potendo la nuova parte del contratto aderire alle clausole senza dover sottoscrivere ulteriori accordi (13).

(12) In tal senso G.M. Riccio, *commento sub art. 82 GDPR*, in *GDPR e normativa privacy*, a cura di E. Belisario, G. Riccio, G. Scorza, Milano, 2018, p. 599.
(13) L. Bolognini, *commento sub art. 28 GDPR*, cit., p. 200.

La **Clausola 6** si limita a rinviare all'Allegato II (v. *infra*) che deve recare la descrizione dettagliata dei trattamenti, con particolare riferimento alle categorie di dati personali e alle finalità del trattamento demandato al responsabile.

Gli obblighi delle parti sono disciplinati alla **Clausola 7**. Il comma 1, lett. *a)*, prevede che il responsabile tratti i dati solo su istruzione documentata del titolare salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile stesso. Le istruzioni per il trattamento possono essere impartite contestualmente alla sottoscrizione delle CCT o successivamente e possono essere costituite, ad esempio, dalla procedura che il titolare ha adottato per la gestione delle violazioni di dati (c.d. *data breach*) o dalla procedura per la gestione delle istanze degli interessati. Secondo una parte della dottrina, la previsione non reca un obbligo in capo al titolare di impartire per iscritto le istruzioni, quanto piuttosto sembrerebbe imporre al responsabile la necessità di documentare le istruzioni ricevute, al fine di dimostrare di aver agito conformemente al GDPR (14); ciò comporterebbe che, anche a fronte di istruzioni ricevute oralmente, ad esempio in situazioni di urgenza, graverebbe sul responsabile l'onere di documentare dette istruzioni in un momento successivo (15).

Nella prassi si registra, comunque, una propensione degli stessi titolari a disciplinare per iscritto le istruzioni, specie nelle strutture più organizzate, anche nell'ottica di mostrare, in caso di verifiche da parte dell'autorità di controllo, un elevato livello di *accountability*. Come noto, il principio di *accountability*, di cui all'art. 24, par. 1, impone al titolare del trattamento, «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*», di mettere in atto tutte le misure tecniche e organizzative adeguate a garantire, e ad essere in grado di dimostrare, che il trattamento sia stato effettuato conformemente alla normativa di settore. Dette misure devono essere esaminate ed aggiornate qualora "necessario". Il Regolamento non si limita a stabilire questa responsabilità in termini astratti perché specifica la necessità di tenere in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, richiedendo che tali valutazioni si concretizzino sia nella scelta delle misure tecniche e organizzative da adottare nel contesto aziendale sia nell'attuazione di *privacy policy* conformi (16).

---

(14) In particolare, si fa riferimento a P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, Cham 2017, p. 82. Concordano con gli Autori, richiamandoli espressamente, anche G. Scorza, M.L. Salvati, *commento sub art. 28 GDPR*, *op.cit.*, p. 269.

(15) In tal senso depongono anche le FAQ della Commissione Europea pubblicate il 25 maggio 2022 sulle CCT, punto 15 (cfr. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en).

(16) Sul punto A.M. Gambino, A. Stazi, D. Mula, *Diritto dell'informativa e della comunicazione*, Padova, 2019, p. 90.

Peraltro, se il titolare impartisce per iscritto le istruzioni al responsabile sarà anche avvantaggiato in sede giudiziaria nella dimostrazione della violazione da parte del responsabile, cui consegue, oltre all'insorgenza di profili di responsabilità diretta nei confronti degli interessati, l'automatica qualificazione del responsabile quale titolare (17).

Il responsabile del trattamento è tenuto altresì a informare prontamente il titolare qualora una istruzione impartita da quest'ultimo viola il GDPR o una norma nazionale in materia di trattamento.

Di particolare rilievo sono i commi due e tre della Clausola 7 che impongono il rispetto delle finalità e della durata del trattamento, indicata nell'Allegato II (v. *infra*).

Al comma 4 della Clausola in parola sono riportati, arricchendoli, gli obblighi in materia di sicurezza del trattamento secondo quanto dettagliato nell'Allegato III cui rinvia (lett. *a)*, v. *infra*), e in materia di autorizzazione al trattamento dei soggetti che opereranno per conto del responsabile che, come detto, devono essere vincolati contrattualmente alla riservatezza.

Ai sensi del quinto comma il responsabile è tenuto ad applicare "limitazioni specifiche e/o garanzie supplementari" in caso di trattamento di dati sensibili, per tali intendendosi i dati idonei a rivelare l'origine raggiale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici, nonché dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali.

Il sesto comma della Clausola 7 prevede, poi, che entrambe le parti siano in grado di dimostrare l'adempimento delle CCT e, in particolare, che il responsabile sia in grado di "rispondere prontamente e adeguatamente" alle richieste di informazioni del titolare (lett. *b)*), mettendo a disposizione dello stesso tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al Regolamento e alle CCT (lett. *c)*, primo periodo) e rendendosi disponibile all'attività di revisione e riesame (lett. *c)*, secondo periodo). Tali attività di riesame e revisione possono essere svolte direttamente dal titolare o da un soggetto terzo delegato (lett. *d)*). In caso di adozione delle CCT le parti devono essere in grado di mettere

(17) In tal senso si veda Cass., sez. I, 23 luglio 2021, n. 21234: «*può far valere la qualità di "responsabile del trattamento" solo il soggetto che sia stato preposto al trattamento dal "titolare" e che si sia attenuto alle istruzioni da questi impartitegli in esplicazione del suo potere decisionale; ne consegue che ove ciò non avvenga, il "responsabile" potrà essere riconosciuto come "titolare" in concreto del trattamento, in ragione dell'autonomia decisionale e gestionale manifestata anche disattendendo le disposizioni del "titolare"*». Nella specie, la Suprema Corte, respingendo il ricorso, ha ritenuto che non potesse essere qualificato come mero "responsabile" del trattamento il preposto che aveva indebitamente attivato contratti, schede e servizi telefonici non richiesti dagli interessati. Per un commento all'ordinanza si veda R. Settimio, *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto*, in *GiustiziaCivile.com*, 2022.

a disposizione dell'autorità di controllo tutte le informazioni, compresi gli esiti delle eventuali attività di revisione.

L'ottavo comma della Clausola in parola disciplina il ricorso a sub-responsabili del trattamento da parte del responsabile, prevedendo la possibilità di una autorizzazione preliminare specifica, che deve essere richiesta entro un termine che il titolare può liberamente determinare, o, in alternativa, il titolare può accettare di rendere una "autorizzazione generale" a ricorrere a sub-responsabili scelti da un elenco concordato. In questa seconda ipotesi il responsabile è tenuto a informare preventivamente per iscritto il titolare del trattamento di eventuali modifiche che prevede di apportare a tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento entro un termine liberamente determinabile dal titolare, affinché quest'ultimo abbia il tempo sufficiente per poter opporsi a modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento deve fornire al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

Come chiarito dal Garante per la protezione dei dati personali, allorquando un responsabile non rispetta l'obbligo di richiedere l'autorizzazione alla nomina di un sub-responsabile o di mera comunicazione dell'intendimento di nominare un sub-responsabile configura un'autonoma violazione dell'art. 28, par. 2, del GDPR, di cui risponde in via diretta ed esclusiva (18).

Il responsabile in caso di ricorso a sub-responsabili è obbligato a sottoscrivere un contratto di designazione (lett. *b)*), che deve essere dato in copia al titolare, con l'accortezza che, qualora il contratto rechi segreti aziendali o altre informazioni riservate, queste possono essere oscurate (lett. *c)*). Naturalmente il responsabile resta pienamente responsabile nei confronti del titolare in caso di inadempimento da parte di un sub-responsabile (lett. *d)*). Il responsabile si obbliga altresì a inserire nel contratto di designazione del sub-responsabile una clausola che imponga a quest'ultimo, nel caso di cessazione dell'attività del responsabile o divenga insolvente, di riconoscere al titolare del trattamento il diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

Viene, infine, previsto che in caso di trasferimento di dati al di fuori dello Spazio Economico Europeo sia garantito il rispetto delle disposizioni del Cap.

---

(18) Cfr. GPDP provv. n. 44/2022, doc. web n. 9754332, «*si ritiene che il ricorso da parte della Società [responsabile] ai servizi offerti da [xxx], senza previa autorizzazione scritta dal [titolare], sia avvenuto in violazione dell'art. 28, par. 2, del Regolamento.* […] *In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria, nella misura di euro 10.000 (diecimila) per la violazione degli artt. 28, par. 2, e 32 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva*».

V del GDPR, utilizzando le specifiche clausole contrattuali tipo adottate dalla Commissione europea ai sensi dell'art. 46, par. 2, lett. *c)*, del GDPR (v. *supra*).

La **Clausola 8** disciplina gli obblighi di assistenza al titolare del trattamento nel fornire riscontro alle istanze degli interessati, secondo le istruzioni impartite dal titolare (lett. *a)* e *b)*), nella procedura di valutazione d'impatto sulla protezione dei dati, ivi inclusa l'eventuale fase di consultazione dell'autorità di controllo (lett. *c)*).

Sebbene sia un obbligo che grava sul titolare del trattamento quello di svolgere la valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR, ove il trattamento preveda l'impiego di un prodotto tecnologico, ad esempio un dispositivo *hardware* o un *software*, il titolare potrà richiedere al fornitore del prodotto di mettere a disposizione un *set* di informazioni utili senza compromettere i segreti né generare rischi per la sicurezza, divulgando vulnerabilità (19).

Alla **Clausola 9** viene disciplinata la notifica delle eventuali violazioni di dati personali trattati dal titolare (par. 1) o dal responsabile (par. 2) del trattamento. Se risultano sufficienti le informazioni prescritte che il responsabile del trattamento deve fornire al titolare ai fini della successiva notifica all'autorità di controllo della violazione verificatasi, pare invece, doversi integrare la previsione in esame, dettagliando il tempo entro il quale il responsabile del trattamento deve notificare l'evento al titolare, affinché quest'ultimo possa a sua volta notificare la violazione all'autorità di controllo. Ai sensi dell'art. 33 del Regolamento, infatti, il titolare del trattamento deve notificare la violazione entro 72 ore, nel caso in cui la violazione avvenga a dati trattati dal responsabile del trattamento diviene dirimente comprendere da quando il titolare possa dirsi "effettivamente a conoscenza".

Al riguardo si osserva che nelle Linee guida 9/2022 in materia di notifica delle violazioni di dati personali (*data breach*) dell'EDPB viene chiarito che sebbene l'EDPB ritenga che un titolare del trattamento dovrebbe essere considerato a conoscenza quando ha un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali, ciononostante lo stesso Comitato afferma che è onere del titolare del trattamento attuare tutte le misure tecniche di protezione e organizzative adeguate per stabilire immediatamente se sia avvenuta una violazione e per informare tempestivamente l'autorità di controllo e gli interessati (20).

---

(19) Sul punto si rinvia alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" (WP248.rev01), nella versione adottata il 4 ottobre 2017, dal Gruppo di lavoro Art. 29, pp. 8 e ss.

(20) EDPB, *Guidelines 9/2022 on personal data breach notification under GDPR* (version 2.0, adopted 28 March 2023: «*31. As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. The EDPB considers that a controller should be regarded as having become*

Un termine più specifico ben potrebbe, dunque, essere integrato nelle CCT (21).

Alla **Clausola 10** vengono, infine, disciplinate le ipotesi di risoluzione e di inosservanza delle CCT espressamente prevedendo che nel caso in cui il responsabile del trattamento violi queste ultime il titolare può dargli istruzioni affinché sospenda il trattamento, fino all' esatto adempimento o, in subordine, cessi ogni operazione di trattamento. Qualora dopo la sospensione il responsabile non ottemperi, il titolare ha il diritto di risolvere il contratto. È riconosciuto il diritto di risolvere il contratto di designazione al responsabile qualora il titolare non modifichi una istruzione che il responsabile ha segnalato essere in contrasto con il GDPR o altra norma nazionale in materia di trattamento.

3.2 Disamina degli Allegati

Come detto completano le CCT quattro Allegati che costituiscono parte integrante del contratto di designazione.

L'**Allegato I** reca i nomi delle parti, qualifica e contatto del sottoscrittore, data e firma.

L'**Allegato II** reca, invece, la descrizione del trattamento e, più specificatamente: a) le categorie di interessati coinvolti nel trattamento delegato al responsabile; b) le categorie di dati personali trattati; c) in caso di trattamento di dati sensibili le misure di limitazione del trattamento e le garanzie ulteriori applicate; d) natura del trattamento; e) finalità del trattamento e, infine, f) la durata del trattamento.

Come accennato nei precedenti paragrafi questo documento è uno tra i più importanti e deve essere compilato con grande attenzione, al fine di ben perime-

---

"aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. 32. However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject24. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action. 33. When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required».

(21) In tal senso depongono anche le FAQ della Commissione Europea pubblicate il 25 maggio 2022 sulle CCT, punto 8 (cfr. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en).

trare le attività delegate e circoscrivere le responsabilità e le attività demandate al responsabile e la natura del trattamento delegato, ovvero sia la base giuridica in forza del quale il trattamento è svolto da parte del titolare.

A sostegno di quanto appena affermato si consideri che il Garante ha sanzionato una pubblica amministrazione proprio perché «*L'atto, infatti, non indica in modo analitico i compiti attribuiti* […] *e, di conseguenza, non comprende specifiche istruzioni, in relazione alla molteplicità dei trattamenti effettuati dal* [responsabile] *per conto del* [titolare]» (22). Come anticipato, inoltre, particolare attenzione deve essere data alla durata del trattamento, che deve chiaramente ricomprendere anche l'eventuale fase di cancellazione o restituzione dei dati al titolare.

All'**Allegato III** devono essere puntualmente indicate le misure tecniche e organizzative per garantire la sicurezza dei dati, indicando in modo quanto più puntuale possibile le misure per prevenire gli specifici rischi nelle attività di trattamento delegate e nella gestione interna delle stesse. Nel presente Allegato devono essere anche descritte le misure tecniche e organizzative specifiche che il responsabile del trattamento si impegna ad adottare per essere in grado di fornire assistenza al titolare del trattamento. In tale Allegato possono, dunque, essere inserite anche le "istruzioni documentate" definite sin dalla fase di sottoscrizione delle CCT. Al contenuto dello stesso dovrà farsi riferimento per verificare l'esatto adempimento da parte del responsabile e procedure, in caso di inadempimento, alla sospensione o alla risoluzione del relativo contratto.

Nell'ambito delle misure di "identificazione e autorizzazione dell'utente" si ritiene debba essere data particolare attenzione alle modalità di nomina degli amministratori di sistema, ancora soggette al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (23).

Nell'**Allegato IV**, infine, devono essere riportati tutti i sub-responsabili del trattamento, dettagliando, in analogia a quanto operato nell'Allegato II, il perimetro del trattamento oggetto di sub-delega.

Il saggio, dopo una breve disamina sulla figura del responsabile del trattamento, si prefigge di analizzare le clausole contrattuali tipo tra titolari e responsabili del trattamento adottate dalla Commissione Europea con Decisione di Esecuzione (UE) 2021/915 del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'art. 28, par. 7, del regolamen-

(22) Così GPDP provv. 278/2020, doc. web n. 9529527.

(23) GPDP provv. del 17 novembre 2008, doc. web n. 1577499: "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".

to (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'art. 29, par. 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio.

The essay, after a brief examination of the figure of the data controller, aims to analyze the standard contractual clauses between data controllers and data processors adopted by Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.