Camera di Commercio
Gran Sasso d'Italia

Linee guida per i rapporti di contitolarità e per l'attribuzione di responsabilità a soggetti esterni

ai sensi del Regolamento UE 679/2016

ultimo aggiornamento: ottobre 2023

1 - PREMESSA

1.1. - SCOPO E CAMPO DI APPLICAZIONE

Scopo delle presenti linee guida è quello di definire il set di adempimenti, relative responsabilità e strumentazione operativa per la valutazione e la nomina di soggetti esterni in rapporti contrattuali/convenzionali con la Camera di commercio del Gran Sasso d'Italia e la relativa attribuzione delle responsabilità per il trattamento dei dati, in qualità di Contitolari ovvero Responsabili.

In proposito, si specifica che non tutti i contratti con soggetti esterni cui sono affidate attività o servizi di competenza dell'Ente comportano l'attivazione di specifiche cautele a tutela dei dati e degli interessati. Tutte le volte in cui il soggetto che esprime e qualifica il fabbisogno di beni, servizi o lavori per l'Ente camerale ravvisi che un determinato affidamento **non comporta il trattamento di dati personali**, non dovrà essere gestito alcun adempimento di cui al presente documento.

Va inoltre fatto presente che l'individuazione dei ruoli (per esempio quello di Responsabile esterno del trattamento, ovvero di Contitolare, o, ancora, di Titolare autonomo)[1] non è necessariamente una situazione assolutamente predeterminata, potendo variare a seconda delle modalità di organizzazione delle attività che comportano il trattamento dei dati personali. Prevale, al riguardo, una valutazione di tipo sostanziale e non meramente formale[2].

1.2. - RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7, del GDPR);
2. Contitolare del trattamento (art. 4, n. 7 e art. 26 del GDPR);
3. Responsabile del trattamento (art. 4, n. 8 e art. 28 del GDPR);
4. Amministratori di sistema (Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema");
5. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (WP169);

[1] Viene utilizzata l'espressione "Responsabile esterno" – il GDPR parla solo di "Responsabile" – al fine di porre una immediata distinzione con altri soggetti, siano essi interni, ovvero per i quali non è richiesta la nomina ex art. 28.

[2] Cfr. Garante, *Risposta a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del Regolamento (UE) 679/2016*, del 22 gennaio 2019, doc web n. 9080970.

6. Decisione di esecuzione (UE) 2021/915 della Commissione 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 GDPR;
7. EDPB, Linee guida n. 07/2020, vers. 2.0., adottata il 7 luglio 2021, sui concetti di titolare e responsabile nel GDPR.

1.3. - ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation - GDPR)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali"
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati – EDPB - European Data Protection Board)
RPD/DPO	Responsabile della protezione dei dati/*Data Protection Officer* (RPD/DPO)
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera di commercio del Gran Sasso
Responsabile	Responsabile (esterno) del trattamento ex art. 28 GDPR

1.4. - MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione
27/08/2021	Approvato	1^ emissione	Determina del Conservatore in veste di Delegato del Titolare n. 52 del 27.8.2021
16/10/2023	Approvato	2^ emissione	Determina del Delegato del Titolare n. 291 del 16.16.2023

2 - TITOLARITA' E RAPPORTI DI CONTITOLARITÀ

Il Titolare del trattamento è "[…] 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 degli Stati membri" (art. 4 del GDPR).

Non rientrano nella definizione di "Titolare" i casi in cui il trattamento è effettuato al di fuori dell'ambito soggettivo di applicazione del GDPR, come nel caso di una persona fisica che effettua trattamenti per finalità prettamente personali e non commerciali (cfr. il Considerando 18).

Tanto premesso va osservato che non svolgere direttamente trattamenti su dati personali – per esempio nel caso in cui questi siano realizzati tramite sistemi telematici - non è condizione sufficiente per escludere la qualifica di Titolare del trattamento. Il Titolare può infatti, legittimamente, demandare tutte le fasi di trattamento – sin dall'inizio – ad un altro soggetto ma resta, comunque, il Titolare che ha effettivamente e in autonomia deciso le finalità (magari demandando ad altri l'individuazione dei mezzi del trattamento). È Titolare, dunque, in questi casi, colui che ricava un beneficio dell'attività di trattamento e mantiene il controllo (e la responsabilità) sul trattamento medesimo. Ad esempio, una società che incarica un'altra di effettuare una ricerca di mercato, definendo i parametri della ricerca e i soggetti a cui rivolgerla, è da ritenersi Titolare del trattamento, anche se la società incaricata si limita a fornire report statistici (e dati personali) derivanti dalle indagini e non l'intera base dati da cui sono ricavate tali analisi (in altre parole, i dati personali ed i mezzi di analisi appartengono a quest'ultima).

Due soggetti possono poi assumere la qualifica di **Contitolari** ai sensi degli artt. 4, n. 7 e art. 26 del GDPR, quando, in relazione ad uno o più trattamenti, determinino **congiuntamente le finalità e i mezzi** dello stesso. A tali fini:

- per "finalità" deve intendersi il "perché" debba essere effettuato un trattamento di dati;
- per "mezzi", devono intendersi non solo gli strumenti tecnici utilizzati per trattare i dati personali (ad es., uno specifico applicativo informatico e le relative misure di sicurezza), ma anche il "come" del trattamento, cioè "quali dati trattare", "chi può avervi accesso", "quanto tempo conservarli ", ecc.
-

In proposito, si specifica che la qualifica di Titolari del trattamento è desumibile:

a) in forza di una Legge o disposizione di fonte secondaria[3] (c.d. "**esplicita competenza giuridica**") che attribuiscano alla Camera di commercio una "funzione istituzionale" (cfr. la

[3] Ad es., decreti ministeriali.

Con riferimento al trattamento di dati personali – come Titolare – sulla base dell'obbligo legale (art. 6, par. 1, lett. c), del GDPR, ovvero per l'esecuzione di un compito di interesse pubblico o connesso con l'esercizio di poteri pubblici (art. 6, par. 1, lett. e), del GDPR), si fa presente che, oltre alle norme di legge o di regolamento, l'art. 2-ter, comma 1, del Codice - come modificato dall'art. 9, comma 1, lett. a) del D.L. n. 139/2021 (convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205) – prevede anche gli atti amministrativi generali.

legge n. 580/1993, nonché le altre disposizioni nazionali o regionali che attribuiscono una competenza istituzionale, come riportato – nel trattamento dei dati personali – nel Registro dei trattamenti);

b) in forza di un **contratto o atto analogo tra le parti** che consentano esplicitamente od implicitamente (ovvero per *facta concludentia*[4]) di *assegnare* ad una od entrambe le parti tale qualifica[5];

c) a prescindere da una specifica competenza o facoltà di controllare dati conferita per legge o per contratto, sulla base di elementi fattuali e circostanze concrete (c.d. "**competenza implicita**") che pongano l'Ente od Organizzazione in una "posizione di dominanza" rispetto ai dati acquisiti, ovvero eserciti "in autonomia" un determinato trattamento.

Si possono ipotizzare, in proposito, alcuni esempi di contitolarità in cui potrebbe trovarsi la Camera di commercio, da valutare sempre caso per caso e nello specifico contesto:

1. L'Ente camerale e un'altra Pubblica Amministrazione si accordano (mediante la stipula di un protocollo, convenzione o atto giuridico analogo) per svolgere una determinata attività o progetto che comporti il trattamento di dati personali (in funzione delle circostanze, i due Enti possono essere entrambi competenti *ratione materiae* in riferimento all'oggetto dell'accordo, ovvero la competenza può essere derivata direttamente dallo strumento contrattuale);
2. L'Ente camerale assume un ruolo di garanzia/controllo su una determinata tematica/attività, posta in essere in attuazione di specifiche Convenzioni/Intese/Protocolli sottoscritti con altri organismi pubblici o privati;
3. L'Ente camerale partecipa in *partnership* con altri Enti, Organismi pubblici o privati, ovvero con Società del Sistema camerale a Programmi regionali, nazionali o comunitari per il finanziamento di specifiche progettualità che comportano l'acquisizione e gestione di dati personali;
4. Nell'ambito delle funzioni attribuite agli Enti del Sistema camerale dalla Legge n. 580/1993, ovvero da altra disposizione normativa, l'Ente camerale realizzi progettualità o servizi gestiti congiuntamente con altre Camere di commercio o con l'Unioncamere, o con altri soggetti appartenenti al sistema camerale.

[4] In relazione ad es., al grado di controllo reale esercitato da una parte, all'immagine, alle informazioni e alle comunicazioni complessive date agli interessati ed al conseguente legittimo affidamento di questi ultimi sul soggetto che – in base alle impressioni e informazioni ricevute – appaia esercitare, anche singolarmente, il controllo sui dati e il ruolo di Titolare.

[5] Quanto detto nel testo va considerato solo in termini illustrativi perché la "qualifica" di titolare, in realtà, non può essere 'attribuita' perché deriva direttamente dal GDPR, ossia *dal fatto* di decidere finalità e mezzi del trattamento. L'EDPB fa presente, a questo riguardo, che occorre proprio un approccio di tipo fattuale e non meramente formale, delineando anche alcuni criteri indicativi quali:

a) il rapporto diretto con i soggetti interessati;
b) la circostanza che la legge imponga, a carico di un soggetto, obblighi specifici che implicano un trattamento di dati personali.

Al primo caso appartengono, ad esempio, le fattispecie in cui tra un soggetto e gli interessati esista un rapporto contrattuale, come nel tipico caso del datore di lavoro nei confronti dei suoi dipendenti.
Rispetto al secondo caso, a parte le rare ipotesi in cui la legge individui espressamente il ruolo di Titolare, se dal dettato normativo sono posti a carico di un determinato soggetto specifici obblighi, che implicano il trattamento di dati personali, significa che la legge ha definito le finalità, per cui ha individuato, indirettamente, come Titolare il soggetto sul quale gravano siffatti obblighi.

La verifica della possibile situazione di contitolarità – prima dell'approvazione del relativo documento da parte dell'organo competente - **deve essere effettuata dal Segretario Generale o dal Dirigente/Responsabile dell'Area organizzativa di riferimento proponente l'atto convenzionale o la specifica progettualità, in collaborazione con la controparte contrattuale;** in questi casi può essere attivato, nella fase istruttoria, il RPD che potrà formalizzare, ove richiesto, uno specifico parere in proposito o collaborare – se del caso – alla fase istruttoria.

In caso di esito positivo, sulla base delle competenze in merito alla procedura, si provvederà ad includere nello stesso atto convenzionale (o in specifico accordo interno stipulato *a latere* dell'atto principale) la definizione delle responsabilità delle parti in merito all'osservanza degli obblighi derivanti dal Regolamento, con specifico (ma non esclusivo) riferimento:

- all'identificazione del soggetto che rilascia l'informativa ed acquisisce gli eventuali consensi al trattamento e che risponde in caso di esercizio dei diritti da parte degli interessati;
- l'eventuale previsione di un unico punto di contatto (es., uno dei due Contitolari cui si aggiunge il relativo Responsabile per la Protezione dei Dati) per gli interessati.

Qualora dall'istruttoria effettuata vi sia l'ipotesi di:

a) avvio di un nuovo trattamento (non precedentemente effettuato da nessuno dei due o più partner);
b) oppure utilizzo (anche su trattamenti già effettuati) di nuove tecnologie;
c) e tali situazioni è probabile che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, secondo quanto previsto dalle apposite linee guida adottate dall'Ente in materia di DPIA - *Data Protection Impact Assessment*, ("Valutazione d'impatto sulla protezione dei Dati"), l'atto convenzionale (o accordo interno) dovrà inoltre individuare:
    - il soggetto che effettua la DPIA di cui all'art. 35 del GDPR[6] e, in caso di necessità, la consultazione preventiva dell'Autorità di controllo (art. 36 del GDPR);
    - il soggetto che, in relazione alla responsabilità come ripartite nell'atto convenzionale o accordo, dovrà tenere in considerazione le risultanze della DPIA o della consultazione dell'Autorità di controllo ai fini dell'implementazione di adeguate misure a tutela degli interessati[7].

[6] Per l'identificazione delle casistiche in cui è necessario o consigliabile effettuare la DPIA nonché dei parametri da utilizzare per la realizzazione della stessa si faccia riferimento al documento *WP248 - 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*, rev 01, del 4 ottobre 2017, reperibile al seguente link: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

In seguito, il Garante, con il Provv. 11 ottobre 2018, n. 467 (in G.U. n. 269 del 19 novembre 2018), ha stabilito l'"Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679".

Per maggiori informazioni si rinvia al documento della Camera di commercio di ……., "Linee guida per la realizzazione di una valutazione di impatto del trattamento di dati (DPIA)".

[7] Per "Autorità di controllo" si intende, normalmente, il Garante per la protezione dei dati personali, fatti salvi i casi di contitolarità con soggetti di altri paesi europei (V. gli artt. 56 e 60 ss., del GDPR), ovvero che lo Stato membro, ai sensi dell'art. 51 del GDPR, non abbia attribuito competenze, in materia di trattamento di dati personali, ai più autorità di controllo (si pensi, per es., all'AGCOM). Per le questioni inerenti la DPIA, al momento, nel nostro paese, l'Autorità di controllo è unicamente il Garante.

Nel caso in cui dall'accordo istituzionale prenda avvio una specifica progettualità comprendente lo sviluppo di strumenti/applicativi informativi, portali informativi o gestionali o strumenti simili, devono essere definite le responsabilità relative alle fasi di progettazione funzionale e non funzionale (misure di sicurezza) dello stesso, in ossequio ai principi della *privacy by design* e *privacy by default*, nonché la gestione dello stesso.

Va riservata molta attenzione alla differenza che intercorre tra la "gestione" della privacy nell'ambito dell'accordo/contratto/convenzione etc. e quelle che sono poi le attività "operative" dei "prodotti/servizi" oggetto dei citati atti. Il caso tipico è un accordo che prevede la creazione/gestione di un portale web, etc.

Di seguito si riporta una bozza di accordo di contitolarità:

ACCORDO DI CONTITOLARITA', AI SENSI DELL'ART. 26 DEL REGOLAMENTO UE N. 679/2016, RELATIVO A ……

Tra la ***Camera di commercio, industria, artigianato e agricoltura di …..*** *(di seguito "Camera di commercio di …..", con sede legale in …. (indirizzo, pec. etc.)*

in persona del _____ qualifica_____, _____nome_____, che agisce in qualità di soggetto delegato (ovvero, ad acta, se del caso) dal Titolare del trattamento

e il ***CONTRAENTE (CONTITOLARE)*** *_____, in persona del _____ qualifica_____, _____nome_____, che agisce in qualità di soggetto delegato (ovvero, ad acta, se del caso) dal Titolare del trattamento*

PREMESSO CHE:

- *la Camera di commercio di ……. È un ente pubblico che svolge i compiti e le funzioni previste dalla legge. In particolare, l'art. 2, comma 2, lett. …, della legge 29 dicembre 1993, n. 580, prevede …..;*
- *il contraente ……..;*
- *[indicare tutte le altre Premesse ritenute utili alla comprensione dell'accordo],*
- *L'art. 26 del Regolamento UE n. 679/2016 (di seguito indicato come "GDPR") stabilisce che ….*
- *Nel prosieguo la Camera di commercio di ……. e il contraente ……. potranno essere indicati anche, congiuntamente, come "Parti" o "Contitolari" e ciascuna, separatamente, come "Parte" o "Contitolare",*

CONVENGONO E STIPULANO QUANTO SEGUE

Art. 1. Oggetto e legittimazione giuridica.

L'oggetto del presente accordo è l'instaurazione di un rapporto di contitolarità tra le Parti per i trattamenti dei dati personali necessari ai fini della realizzazione _____ descrivere l'oggetto e la finalità delle attività previste dall'accordo, nonché la base legale su cui l'attività è posta in essere _____.

L'oggetto del presente accordo è l'instaurazione di un rapporto di contitolarità tra le Parti per il trattamento dei dati acquisiti, gestiti e trattati ai fini della realizzazione _____

descrivere l'oggetto e la finalità delle attività previste dall'accordo, nonché la base legale su cui l'attività è posta in essere _____.

La legittimità giuridica del trattamento, deriva oltre che dalle disposizioni di cui all'art. 2, comma 2, lett. …, della Legge n. 580/1993 e dal D.M. 7 marzo 2019, n. 277 (che ha ridefinito i servizi che il sistema delle Camere di commercio è tenuto a fornire sull'intero territorio nazionale in relazione alle funzioni amministrative ed economiche di cui all'art. 2 della citata legge n. 580/1993), dall'esecuzione di un compito di interesse pubblico di cui all'art. 6, par. 1, lett. e) del GDPR e dal consenso libero e informato dell'interessato di cui all'art. 6, par. 1, lett. a) del GDPR [si tratta di una esemplificazione]

Art. 2. Dati trattati e ripartizione delle responsabilità

L'attività di cui trattasi comporterà il trattamento di dati _____ *qualificare i dati personali acquisiti* _____, relativi a _____ *qualificare tipologia di interessati* _____

La "contitolarità" è riferita alla acquisizione congiunta e/o disgiunta e/o al conseguente trattamento dei dati acquisiti dalle Parti per le finalità sopra riportate, intendendosi per "trattamento" qualunque operazione o complesso di operazioni effettuate con o senza l'ausilio di strumenti elettronici e concernenti la raccolta, la registrazione, l'organizzazione, l'archiviazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, l'utilizzo, la diffusione, la cancellazione e la distruzione di dati acquisiti ed, in definitiva, tutti i processi di gestione dei dati cui il presente accordo è riferito.

Le Parti, con il presente accordo, stante le medesime finalità e modalità del trattamento definite in sede progettuale, intendono trattare i dati acquisiti e gestiti in regime di contitolarità, come di seguito indicato:

CAMERA DI COMMERCIO DI ……	CONTITOLARE

Descrivere in tabella le tipologie di trattamento posto in essere singolarmente o congiuntamente dalle parti, comprese le finalità, scomponendo in processi, sotto-processi e fasi di trattamento ove opportuno al fine di circoscrivere le responsabilità a quanto effettivamente realizzato

La suddetta tabella scompone le attività in sotto-attività, definendo di conseguenza i trattamenti dei dati personali svolti congiuntamente e/o disgiuntamente dai Contitolari, al fine di circoscrivere le responsabilità di ciascuna Parte a quanto effettivamente realizzato.

Ogni Parte/Contitolare risponde in solido nei confronti degli interessati per i danni derivanti dal trattamento, fermo restando, nei rapporti interni, la responsabilità di ciascuna Parte per i trattamenti alla stessa direttamente imputabili in base al presente accordo.

Rimane fermo che le Parti sono vincolate all'utilizzo dei dati secondo le finalità definite in ambito progettuale e qui richiamate nonché esposte nelle informative rilasciate agli interessati, che dovranno comunque prevedere il contenuto essenziale del presente accordo.

Art. 3. Obblighi ed attività derivanti dalla contitolarità

Nello specifico i Contitolari assumono, vicendevolmente, le seguenti responsabilità:

CAMERA DI COMMERCIO DI ……..	CONTITOLARE

Art. 4. - Sicurezza del trattamento e data breach

Ciascuna Parte:

a) è tenuta a mettere in atto tutte le misure di sicurezza tecniche, organizzative e gestionali adeguate a proteggere i dati personali trattati o utilizzati nell'ambito del rapporto di contitolarità. I Contitolari verificano regolarmente il rispetto di tali misure e collaborano, ove necessario, al miglioramento di tali misure;

b) adotta tutte le misure di sicurezza, tecniche e organizzative adeguate al tempestivo recupero della disponibilità dei dati personali che ricadono sotto la loro esclusiva responsabilità, in caso di incidente fisico o tecnico.

Le Parti convengono che ciascuna, per i dati nella propria diretta disponibilità, è responsabile dell'adozione di misure di sicurezza adeguate ex art. 32 del GDPR.

In ogni caso le Parti si impegnano a considerare strettamente confidenziale tutto il materiale non generalmente di dominio pubblico, e si impegnano a utilizzare tali informazioni solamente per gli scopi e le finalità di trattamento previste dal presente accordo.

Ciascuna Parte si impegna ad informare tempestivamente, e comunque entro e non oltre 48 ore [*coerenziare il termine indicato con la procedura di data breach della Camera*] decorrenti dalla scoperta dell'evento, l'altra Parte in caso di violazione dei dati personali trattati in base al presente accordo e agli altri accordi (se vigenti) sottoscritti fra le Parti.

Con riferimento alle attività di trattamento oggetto del presente accordo, gli eventuali adempimenti di cui agli artt. 33 e 34 del GDPR saranno svolti da una delle Parti a seguito di tempestiva idonea valutazione concordata e condivisa da entrambi i Contitolari da effettuare caso per caso.

Art. 5. - Obblighi ed attività relative all'informativa da rendere agli interessati

I Contitolari assumono le seguenti responsabilità per quanto riguarda il rilascio dell'informativa …. *[definire chi fornisce l'informativa e con quali modalità, a seconda che sia ex art. 13 o 14 del GDPR. In quest'ultimo caso verificare l'applicazione dell'art. 14, par. 5]*

Qualora debba essere acquisito il consenso dell'interessato, stabilirne le modalità [in calce al modulo, etc.].

L'informativa per gli interessati viene previamente condivisa nei suoi contenuti dalle Parti e deve, fra l'altro, riportare in modo chiaro e comprensibile:

- la contitolarità del trattamento dei dati;

- che il contenuto essenziale del presente accordo, qualora richiesto, sarà messo a disposizione degli interessati;

- l'indicazione dei punti di contatto (ovvero dell'unico punto di contatto) ai quali gli interessati possono inoltrare le richieste ed esercitare i propri diritti.

Resta fermo che ciascuna Parte è direttamente responsabile e vincolata all'utilizzo dei dati secondo le finalità congiuntamente definite e concordate e riportate nelle informative rilasciate agli interessati.

Art. 6 – Nomina di Responsabili esterni del trattamento

[*Definire, se del caso, possibilità e modalità di designazione di Responsabili e/o Sub-Responsabili del trattamento*]

Art. 7. - Assenza (*o presenza*) di un processo decisionale automatizzato

I Contitolari si impegnano a non adottare alcun processo automatizzato dei dati personali degli interessati, compresa la profilazione, di cui all'art. 22, parr. 1 e 4, del GDPR *[qualora intendano invece adottare processi automatizzati o la profilazione devono rispettare l'art. 22 nonché quanto previsto – rispetto all'informativa – dall'art. 13, par. 2, lett. f), del GDPR*].

Art. 8 - Trasferimento dei dati in paesi non appartenenti all'Unione europea o a organizzazioni internazionali

I Contitolari prendono atto che i dati personali possono essere trasferiti solo in paesi terzi o organizzazioni internazionali localizzati nel territorio dell'Unione europea e/o in paesi extra UE per i quali esistano modalità di trasferimento ai sensi del Capo V del GDPR (art. 45 ss.).

Quanto indicato vale, soprattutto, per l'utilizzo di social network.

Art. 9 – Durata dell'accordo

Il presente accordo decorre dal… e termina la sua efficacia il ……

…. mesi prima della sua scadenza, le Parti possono convenire di prorogarne, alla scadenza, la validità per un ulteriore anno.

Art. 10. - Trattamento dei dati al termine dell'accordo di contitolarità

Alla cessazione del presente accordo, secondo quanto definito al precedente art. 9, indipendentemente dalla causa, ciascuna Parte potrà continuare a trattare i dati personali oggetto del presente accordo in qualità di Titolare autonomo del trattamento dei dati personali nel rispetto delle disposizioni normative applicabili e nei limiti di quanto eventualmente già indicato agli interessati mediante adeguate informative ai sensi degli artt. 13 e 14 del GDPR.

Qualora non sia stata previamente indicata tale possibilità ed i suoi limiti, la Parte, prima di avviare il trattamento come Titolare autonomo, provvederà a rilasciare la relativa informativa agli interessati.

Le Parti provvederanno, al termine delle operazioni di trattamento, tranne il caso in cui scelgano di proseguire il trattamento per ulteriori autonome diverse finalità previa specifica informativa agli interessati, alla integrale cancellazione ovvero alla anonimizzazione dei dati personali (per es., per finalità di studio o statistiche), fatti salvi i casi in cui la conservazione degli stessi sia richiesta da norme di legge.

Art. 11. – Punto/i di contatto per l'esercizio dei diritti da parte degli interessati

Per la gestione dei reclami e delle richieste di esercizio dei diritti presentate dagli interessati, i Contitolari concordano di non designare [*ovvero di designare*] un punto unico di contatto per gli interessati. Pertanto [In ogni caso], ai sensi dell'art. 26, par. 3, del GDPR, gli interessati possono far valere i loro diritti, di cui agli artt. 15-22 del GDPR, indistintamente nei confronti di ciascuna delle parti.

Il/I punto/i di contatto, per gli interessati, è/sono quello/i indicati, da ciascuna Parte, nell'informativa fornita all'interessato.

Ciascun Contitolare agevola l'esercizio dei diritti dell'interessato collaborando reciprocamente senza ingiustificato ritardo per fornire all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 del GDPR.

A seguito della richiesta dell'interessato di voler esercitare un proprio diritto, il destinatario della comunicazione provvederà ad informare, senza ritardo, l'altro Contitolare anche ai fini dell'eventuale assolvimento di quanto richiesto dall'interessato.

In caso di ricezione di una richiesta di esercizio di un proprio diritto, le Parti si impegnano a concordare di volta in volta le modalità di gestione della richiesta ed il riscontro all'interessato che, salvo diverso accordo delle Parti, verrà inviato dalla Parte destinataria della richiesta. Resta inteso che entrambe le Parti, si impegnano a concludere le operazioni di gestione dei diritti dell'interessato entro 30 giorni dalla ricezione della richiesta di esercizio.

Art. 12. - Disposizioni finali

Il contenuto essenziale del presente accordo, da mettere a disposizione degli interessati, ai sensi dell'art. 26, par. 2, del GDPR è costituito dalle Premesse e dagli artt. ……. *[Il contenuto essenziale può anche essere pubblicato su una pagina (espressamente indicata) di uno o tutti i siti web istituzionali delle Parti]*

Eventuali modifiche al presente accordo dovranno essere concordate e apportate per iscritto tra le Parti.

L'invalidità anche parziale, di una o più delle clausole del presente accordo, non pregiudica la validità delle restanti clausole.

Per ogni altro aspetto non trattato esplicitamente nel presente accordo, le Parti rinviano alle disposizioni comunitarie e nazionali applicabili.

Letto, approvato e sottoscritto tra le Parti.

Luogo _____, data _____

3 - RESPONSABILI ESTERNI DEL TRATTAMENTO

3.1. - DEFINIZIONE E IDENTIFICAZIONE DEL RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento, così come definito all'art. 4 GDPR: "è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
Si tratta di soggetti che non decidono le finalità del trattamento (il "perché" vengono raccolti e trattati i dati), ma trattano i dati personali nell'interesse del Titolare, sulla base di una nomina che "accede" ad un contratto (o altra tipologia di atto che vincola il Responsabile al Titolare).

Il Responsabile del trattamento non va confuso:
- con l'"incaricato" del trattamento, citato all'art. 29 del GDPR, che è costituito dalla *persona fisica* – nell'ambito dell'organizzazione del Titolare o del Responsabile – che è preposta al trattamento. Il Codice privacy, indica tali soggetti, senza alcuna differenza disciplinare, come "soggetti designati" (art. 2-*quaterdecies*, D.Lgs. n. 196/2003);
- con il c.d. "responsabile privacy" (che assume varie denominazioni, anche a seconda dell'inquadramento contrattuale: come nel caso dei dirigenti indicati come "privacy manager") che non ha – rispetto a quanto disposto dal GDPR – alcun ruolo 'esterno' nei confronti degli interessati, né delle autorità di controllo.

Alcuni dubbi possono sorgere nei casi in cui un Titolare debba comunicare dati personali ad altri soggetti. Al riguardo se:
a) Il soggetto li riceve sulla base di quanto previsto dalla base giuridica di colui che li comunica, è qualificabile come Titolare autonomo;
b) Il soggetto che li riceve li utilizza per proprie finalità, distinte da quelle del soggetto che li comunica, e con una idonea base giuridica, agirà come Titolare autonomo.

Si ricorda che tanto il soggetto che comunica i dati, quanto quello che li riceve, in qualità di Titolari autonomi dei rispettivi trattamenti, saranno tenuti a fornire la "propria" informativa agli interessati.

Nel caso in cui non si riscontrino le situazioni di cui alle lett. a) e b), il soggetto ricevente agirà in qualità di Responsabile, ex art. 28 del GDPR, e renderà disponibile agli interessati l'informativa predisposta dal Titolare.

Tra le situazioni in cui vi può essere un dubbio se il soggetto tratti i dati come Titolare o Responsabile, si indicano i seguenti:
- Gli appartenenti a professioni regolamentate (notai, avvocati, medici, etc.), seppur svolgano un servizio per il Titolare, non sono nominati Responsabili del trattamento, poiché lo svolgimento delle rispettive funzioni è determinata dalla legge e/o da obblighi deontologici che non possono essere condizionati da istruzioni del Titolare. In particolare, tra i Titolari autonomi, vi è il medico del lavoro che, seppur agisca nel contesto del luogo di lavoro (quindi di altro Titolare), svolge in autonomia, secondo quanto disposto dalla legge, le funzioni in materia di igiene e sicurezza dei luoghi di lavoro, nonché la sorveglianza sanitaria obbligatoria;

- I soggetti che operano sulla base di specifiche disposizioni di legge (es: istituti bancari, vettori del trasporto aereo, marittimo e ferroviario), svolgono i rispettivi servizi in qualità di Titolari autonomi;
- Le società assicurative alle quali un (Titolare) datore di lavoro si rivolga per l'assicurazione dei dipendenti, instaurando un rapporto contrattuale con questi ultimi – benché per il "tramite" del datore di lavoro – è un Titolare autonomo;
- Il fornitore di servizi di pagamento on line – ai sensi della direttiva UE n. 2015/2366 – opera quale Titolare;
- I gestori di servizi postali operano in qualità di Titolari autonomi;
- Quanti forniscono servizi "non negoziabili" (per esempio dal punto di vista tecnico: come i cloud provider, i fornitori di posta elettronica/pec), agiscono come Titolari; quando invece operano su "istruzioni" specifiche del "committente-cliente" allora operano quali Responsabili;
- Nell'offerta di sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché nell'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, Internet service providers, fornitori di servizi video specialistici, ecc.). A riguardo, pur utilizzando la stessa infrastruttura tecnologica, i soggetti che si avvalgono di tali sistemi per il trattamento delle immagini raccolte nei loro locali, conservano il ruolo di autonomi Titolari (il gestore di tale infrastruttura, avrà invece il ruolo di Responsabile di trattamento per conto dei Titolari).

Venendo ora all'ambito che più ci riguarda, ci sono situazioni in cui L'Ente camerale, esternalizzando un servizio, si trova a dover consentire ad un soggetto terzo (ovvero diverso dall'interessato e dal Titolare e relativa struttura organizzativa) di accedere ai dati personali necessari per espletarlo.

Per evitare che si rientri in una fattispecie di *comunicazione* di dati personali, in questi casi deve essere applicato lo schema di responsabilità ex art. 28 del GDPR: in altre parole, il soggetto esterno entra sostanzialmente a far parte del sistema di trattamento dei dati personali del Titolare (ovvero del suo ambito di titolarità, operando sotto la sua autorità); tale configurazione del rapporto legittima il terzo ad utilizzare, per la parte di competenza, i dati che rientrano nel *dominio* del Titolare, vincolandolo però a standard prestazionali e di comportamento ben definiti.

Al Responsabile esterno è riservata una parziale autonomia riguardante la sola concreta disciplina del servizio ed alcune scelte tecnico-operative che, peraltro, per alcuni servizi sono spesso previste anche da specifiche norme di legge (come, ad esempio, per i servizi bancari di tesoreria, di cui si dirà più avanti), **ma non anche le principali decisioni sulle finalità e sulle modalità di utilizzazione dei dati che spettano esclusivamente al Titolare del trattamento**; il Responsabile esterno risponderà dell'attività di trattamento in termini di corretto adempimento delle prestazioni, ai sensi degli artt. 1218 e 1223 del Codice civile[8].

Parimenti il Titolare gestirà – mediante la relazione contrattuale connessa all'incarico – i dati personali del soggetto incaricato delle attività di Responsabile esterno.

[8] Si ricorda, inoltre, che, ai sensi dell'art. 28, par. 10, del GDPR, il Responsabile (esterno) che determina le finalità ed i mezzi del trattamento (e con ciò oltrepassando i suoi compiti) è considerato Titolare del trattamento in questione, con l'applicazione di tutte le relative responsabilità e le relative sanzioni.

Per i **servizi inerenti la gestione di cassa/tesoreria della CCIAA**, ad esempio, l'istituto cassiere potrebbe svolgere il servizio di Tesoriere, previsto per legge, come Responsabile esterno dei trattamenti, da scegliere e nominare con specifica procedura ad evidenza pubblica (e a norma del GDPR), ovvero come Contitolare/Titolare autonomo dei trattamenti necessari per lo svolgimento del servizio. In questo secondo caso, bisogna però comunque definire o un "*accordo fra i due Contitolari*" ed individuare le reciproche responsabilità e gli obblighi di ciascuno nei confronti degli interessati, ovvero i due Titolari autonomi dovrebbero prendere atto, con un'intesa preliminare, che nello svolgimento del servizio contrattualmente affidato da una parte e fornito dall'altra, che comporta il trattamento di dati personali, ciascuna parte ha una competenza/qualifica/ruolo non esclusiva nella determinazione delle "*finalità e dei mezzi del trattamento*" dei dati personali per lo svolgimento del servizio.

Una soluzione potrebbe essere quella di prevedere nella procedura per l'assegnazione del servizio da parte della CCIAA il ruolo/qualifica che si ritiene debba rivestire l'istituto cassiere, ovvero rimandare ad una successiva intesa preliminare fra le parti la definizione del ruolo e degli obblighi di ciascuna parte tenendo conto e considerando, in modo concreto, chi definisce "*le finalità*" del servizio (di regola la CCIAA), e chi "*i mezzi e le modalità*" organizzative, tecnico-operative e telematiche per la fornitura dello stesso che, di solito, sono di competenza della banca (spesso definite da obblighi di leggi speciali a questa applicabili).

3.2. – PRESUPPOSTI PER LA NOMINA DI UN RESPONSABILE DEL TRATTAMENTO

Il presupposto per l'affidamento di trattamenti a soggetti esterni, è che sia valutata nella fase istruttoria (ad es., mediante specifica previsione dei capitolati tecnici, o altrimenti mediante acquisizione di specifica documentazione della controparte) l'affidabilità del soggetto – in relazione all'esperienza, capacità, alle misure di sicurezza organizzative e tecnico-informatiche – affinché fornisca idonea garanzia del pieno rispetto delle disposizioni di cui al Regolamento UE 679/2016[9].

Elementi utili a tale verifica possono essere, a puro titolo esemplificativo:

- con riferimento ai requisiti di **capacità morale e di affidabilità**, l'assenza di condanne rilevanti in materia, ad es., con riferimento:
  - ✓ ad uno o più dei reati precedentemente previsti dal D. Lgs. n. 196/2003 (artt. 167 e ss.) o dall'art. 24-bis del D.Lgs. n. 231/2001 in relazione agli apicali dell'Ente o direttamente in capo all'Ente (sanzioni amministrative dipendenti da reato);
  - ✓ alle sanzioni amministrative in capo al Titolare del trattamento precedentemente previste dal D.Lgs. n. 196/2003 (cfr. artt. 161 e ss.) o successivamente dal GDPR (art. 83);

[9] Cfr. considerando 81 del GDPR: "…quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento".

- con riferimento ai requisiti speciali (**capacità tecnica**):
  - ✓ il possesso di sistemi certificati di gestione della sicurezza delle informazioni (es., ISO 27001), di continuità operativa (es., ISO 22301) ovvero la dichiarata adesione a Linee guida o Codici di condotta specifici (es., ISO 17799, ISO/IEC 27032, Codici di condotta specifici[10]), in attesa di analoghi strumenti definiti ai sensi degli artt. 40 e ss. del GDPR;
  - ✓ l'attestazione di adozione dei controlli di natura tecnologica, organizzativa e procedurale definiti dalla Circolare AgID n. 2 del 18 aprile 2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (G.U. n. 103 del 5 maggio 2017), a partire dal livello minimo (per la generalità dei casi, mentre i livelli superiori – Standard ed Alto – potrebbero essere utilizzati nei casi di trattamenti che presentino livelli di rischio più elevato);
  - ✓ idonea e documentata attestazione e descrizione delle misure di accountability adottate ai sensi del GDPR (ad es., registro dei trattamenti, nomina RPD) e delle misure di sicurezza organizzative e tecniche implementate ai sensi degli artt. 24 e 32 del GDPR.

Le specifiche per la valutazione del soggetto esterno sono definite dal RUP – in funzione della "criticità" delle attività da affidare - ed oggetto di valutazione da parte dello stesso RUP in caso di affidamento diretto, dalla Commissione di aggiudicazione, nel caso in cui sia prevista, dal Dirigente/Responsabile posizione organizzativa proponente l'eventuale atto deliberativo che formalizza gli accordi convenzionali in assenza di evidenza pubblica.

NB: ove l'appalto o l'incarico preveda lo sviluppo di applicativi informatici, portali web e strumenti analoghi, l'applicazione dei principi di *privacy by design* o di *privacy by default* prevede che debbano essere chiaramente definite, in relazione alla "consistenza" dei trattamenti e degli strumenti da implementare, nell'ambito del capitolato tecnico ovvero in un documento progettuale successivo, le **specifiche non funzionali** (misure di sicurezza) da implementare, sulla base di una preliminare o successiva analisi d'impatto che dovrà costituire specifico dato di input per la realizzazione delle attività. L'identificazione delle soluzioni da ritenere adeguate (specifiche non funzionali) può anche essere rimessa al soggetto esterno (ad es., mediante richiesta di un documento di progettazione preliminare) ma in questo caso devono comunque essere sottoposte a validazione da parte del Titolare.
In sede di applicazione dei principi di *privacy by design* e di *privacy by default* è altresì opportuno che il Titolare consulti il DPO, in virtù delle competenze consulenziali attribuitegli ex art. 39, par. 1, lett. a) e c), del GDPR.

[10] Ad es., le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale" adottate dal Garante per la protezione dei dati personali con un provv. del 19 dicembre 2018 e pubblicate ai sensi dell'art. 20, comma 4, del D.Lgs. n. 101/2018 sulla G.U. n. 11 del 14 gennaio 2019.

3.3.- CHECK-LIST PER LA VALUTAZIONE PREVENTIVA (E PER L'AUDIT SUCCESSIVO) DEL RESPONSABILE

Ai fini della verifica del possesso dei requisiti per poter effettuare la nomina di un Responsabile, ex art. 28 del GDPR, è adottata la *check-list* contenuta nel successivo riquadro[11]. Tale lista di "controllo" può essere impiegata anche per gli *audit* durante la vigenza dell'incarico conferito (in particolare con i quesiti indicati in neretto).

CHECK-LIST / AUDIT RESPONSABILE ESTERNO (art. 28 DEL GDPR)			
Dati del Responsabile			
Nome, Cognome o Ragione sociale:			
Codice Fiscale:			
E-mail – PEC:			
Riferimento del Responsabile da contattare:			
Riferimenti (atto deliberativo, data, protocollo, oggetto) dell'incarico da cui origina il trattamento/i di dati personali:			
Trattamenti oggetto della nomina, ex art. 28 GDPR, del Responsabile:			
Istruzioni per la compilazione: Selezionare la casella "Sì" solo se la proposizione del quesito corrisponde alla situazione del soggetto oggetto di verifica **in tutte le sue parti**. Se la proposizione corrisponde solo parzialmente, selezionare "No" e specificare quali difformità sono presenti nel campo "Note" Nel campo "Documenti" indicare il riferimento ai pertinenti documenti del Responsabile (che vengono consegnati o che sono disponibili alla richiesta del Titolare).			
QUESITO	**CHECK**	**NOTE**	**DOCUMENTI**
Sez. I Informazioni sul Responsabile			
1.1. Il Responsabile possiede delle certificazioni relative ai processi impiegati per i trattamenti dei dati	Sì ☐ No ☐		

[11] Si faccia attenzione che la check-list è solo *indicativa* nel senso che può essere ulteriormente implementata, ovvero ridotta o, ancora, in alternativa, a seconda dei contesti in cui viene utilizzata (da specificare da parte della Camera di commercio), indicare quali siano le domande con risposta "obbligatoria" (positiva), oppure quelle la cui risposta negativa impedisce la nomina a Responsabile esterno. Alcune domande possono, infine, essere utilizzate per attribuire una "preferenza" (si pensi alle 1.2. e 1.3.).

La *check-list* compilata può anche costituire uno dei documenti da allegare per l'iscrizione nell'elenco dei fornitori dell'Ente. (*le informazioni vanno, comunque, verificate al momento della nomina*).

personali oggetto della nomina (Es. certificazioni relative alla sicurezza delle informazioni, alla continuità operativa, alla resilienza organizzativa etc.)			
1.2. Il Responsabile aderisce ad un codice di condotta approvato ai sensi dell'art. 40 del GDPR	Sì ☐ No ☐		
1.3. Il Responsabile possiede una certificazione ai sensi dell'art. 42 del GDPR	Sì ☐ No ☐		
1.4. Il Responsabile ha subito violazioni dei dati personali negli ultimi dodici mesi. (Se sì specificare quante in Note)	Sì ☐ No ☐		
1.5. *(solo in caso di risposta affermativa alla precedente)* Il Responsabile ha comunicato tempestivamente al Titolare del trattamento le violazioni dei dati personali	Sì ☐ No ☐		
1.6. Il Responsabile ha ricevuto – in assoluto e negli ultimi 12 mesi – ispezioni in materia di trattamento dei dati da parte della Guardia di finanza o altre autorità (es: polizia postale)	Sì ☐ No ☐		
1.7. Il Responsabile ha ricevuto – in assoluto e negli ultimi 12 mesi – ingiunzioni o sanzioni da parte del Garante	Sì ☐ No ☐		
1.8. Il Responsabile, per le sue attività di trattamento, è stato attore o convenuto, negli ultimi 12 mesi, in procedure giudiziarie penali, civili o amministrative	Sì ☐ No ☐		
Sez. II **Rispetto del contenuto della nomina**			
2.1. Il Responsabile ha adottato, documentandoli, processi idonei a garantire che tutti i trattamenti di dati personali effettuati sulla base della nomina siano effettuati conformemente a quanto pattuito con il Titolare	Sì ☐ No ☐		

2.2. Il Responsabile ha adottato, documentandoli, processi diretti ad informare il Titolare che uno o più dei trattamenti oggetto della nomina potrebbero essere in contrasto con il GDPR	Sì ☐ No ☐		
2.3. Il Responsabile ha adottato, documentandoli, processi idonei a garantire la cessazione dei trattamenti non appena ciò venga richiesto dal Titolare	Sì ☐ No ☐		
2.4. Il Responsabile ha adottato, documentandoli, processi idonei ad ottenere l'autorizzazione alla nomina di un Sub-responsabile del trattamento	Sì ☐ No ☐		
2.5. Il Responsabile ha adottato, documentandoli, processi che consentano di informare il Titolare dei trattamenti della nomina di Sub-responsabili effettuata sulla base di un'autorizzazione scritta generale	Sì ☐ No ☐		
2.6. (se pertinente) Il Responsabile ha effettivamente informato il Titolare della nomina di Sub-responsabili avvenuta sulla base di una precedente autorizzazione generale scritta	Sì ☐ No ☐		
2.7. Il Responsabile verifica che la nomina dei Sub-responsabili preveda il rispetto dei medesimi obblighi imposti dal Titolare al Responsabile stesso	Sì ☐ No ☐		
2.8. Il Responsabile ha implementato, documentandoli, processi di verifica delle caratteristiche organizzative e tecniche dei Sub-responsabili, affinché garantiscano il medesimo livello di sicurezza imposto al Responsabile stesso dal Titolare	Sì ☐ No ☐		
2.9. Il Responsabile ha implementato, documentandoli, processi di verifica periodica (almeno annuale) relativi al rispetto degli obblighi imposti al Sub-Responsabile	Sì ☐ No ☐		

2.10. Il Responsabile ha implementato sanzioni contrattuali nei confronti dei Sub-responsabili che non rispettino gli obblighi ad essi imposti in materia di protezione dei dati personali	Sì ☐ No ☐		
2.11. Il Responsabile ha implementato o aggiornato uno o più dei processi di cui ai precedenti punti da 2.1. a 2.5., nonché da 2.8. a 2.10. ***(In caso di riposta positiva, nel campo "Note", indicare quali processi)***	Sì ☐ No ☐		
Sez. III **Trattamento dei dati personali oggetto della nomina**			
3.1. Il Responsabile ha effettuato un'adeguata valutazione dei rischi connessi ai trattamenti dei dati oggetto della nomina	Sì ☐ No ☐		
3.2. Il Responsabile tiene in maniera puntuale ed aggiornata un registro dei trattamenti oggetto della nomina	Sì ☐ No ☐		
3.3. I Trattamenti dei dati oggetto della nomina vengono interamente effettuati:			
a) entro l'ambito materiale e territoriale di applicazione del GDPR	Sì ☐ No ☐		
b) *ovvero* in paesi destinatari di una Decisione di adeguatezza della Commissione Europea	Sì ☐ No ☐		
c) in paesi terzi ma con la copertura di Clausole Contrattuali Standard di cui all'Art. 46 del GDPR	Sì ☐ No ☐		
d) in paesi terzi, ma nell'ambito di Norme Vincolanti d'Impresa ai sensi dell'art. 47 del GDPR	Sì ☐ No ☐		
3.4. Il Responsabile ha stipulato un accordo di riservatezza con i propri autorizzati al trattamento dei dati	Sì ☐ No ☐		

personali, ovvero si è assicurato che gli stessi siano vincolati da un obbligo legale di riservatezza			
3.5. Il personale (anche non dipendente) del Responsabile che ha accesso ai dati personali oggetto della nomina sono identificati o identificabili	Sì ☐ No ☐		
3.6. Il personale (anche non dipendente) del Responsabile ha ricevuto la formazione e le istruzioni necessarie al trattamento dei dati oggetto della nomina	Sì ☐ No ☐		
3.7. Il Responsabile ha adottato processi idonei a portare a conoscenza di tutto il personale (anche non dipendente) delle procedure, delle tempistiche e delle modalità con cui dovranno essere trattati, conservati e cancellati i dati personali oggetto della nomina	Sì ☐ No ☐		
3.8. Il Responsabile ha adottato, documentandoli, processi che gli permettano di effettuare la cancellazione dei dati personali al termine del periodo di conservazione stabilito dal Titolare	Sì ☐ No ☐		
3.9. La cancellazione dei dati oggetto della nomina avviene con tecniche che rendano ragionevolmente improbabile il loro recupero (ad es. sovrascrittura del supporto)	Sì ☐ No ☐		
3.10. Il Responsabile ha adottato, documentandoli, processi che gli permettano di effettuare, con la sicurezza adeguata, la trasmissione o ricezione al/dal Titolare dei dati personali oggetto della nomina	Sì ☐ No ☐		
3.11. Il Responsabile ha adottato, documentandoli, processi idonei a fornire, senza ritardo, informazioni relative ai trattamenti oggetto della nomina	Sì ☐ No ☐		

che dovessero essere richieste dal Titolare			
3.12. Il Responsabile ha implementato o aggiornato uno o più dei processi di cui ai precedenti punti da 3.7. a 3.11. ***(In caso di riposta positiva, nel campo "Note", indicare quali processi)***	Sì ☐ No ☐		
Sez. IV **Salvaguardia dei diritti degli interessati**			
4.1. Il Responsabile ha adottato una procedura per classificare i dati personali in base alla tipologia dei dati personali (es. dati identificativi, particolari, etc.), con riferimento ai singoli interessati	Sì ☐ No ☐		
4.2. Il Responsabile, qualora sia tenuto ad erogare informative e a raccogliere consensi da parte degli interessati, ha adottato funzionalità tecniche, processi e procedure per la idonea storicizzazione delle informative erogate e dei consensi raccolti	Sì ☐ No ☐		
4.3. Il Responsabile ha adottato, documentandoli, processi che gli permettano, su richiesta del Titolare, di effettuare, senza ritardo, la cancellazione o la rettifica o la trasformazione in forma anonima dei dati personali relativi ad un interessato qualora sussistano i relativi diritti	Sì ☐ No ☐		
4.4. Il Responsabile ha adottato una procedura da seguire e dispone delle funzionalità tecniche ed organizzative necessarie a garantire l'ottemperanza alle richieste di portabilità dei dati pervenute dagli interessati qualora, per uno specifico trattamento, sussista tale diritto	Sì ☐ No ☐		
4.5. Il Responsabile ha adottato, documentandoli, processi idonei a garantire, senza ritardo, la	Sì ☐ No ☐		

cessazione o la limitazione del trattamento dei dati personali oggetto della nomina su richiesta del Titolare			
4.6. Il Responsabile ha adottato una procedura per la verifica della provenienza dei dati personali da parte di soggetti terzi (altre amministrazioni, privati, etc.)	Sì ☐ No ☐		
4.7. Il Responsabile ha adottato una procedura per consentire al Titolare la verifica della correttezza della comunicazione o divulgazione dei dati personali se previsti dal trattamento	Sì ☐ No ☐		
4.8. Il Responsabile ha adottato, documentandoli, processi idonei a fornire, senza ritardo, al Titolare la necessaria collaborazione per rispondere e provvedere rispetto alle richieste degli interessati	Sì ☐ No ☐		
4.9. Il Responsabile ha implementato o aggiornato uno o più dei processi o delle procedure di cui ai precedenti punti da 4.1. a 4.8. ***(In caso di riposta positiva, nel campo "Note", indicare quali processi)***	Sì ☐ No ☐		
4.10. Il Responsabile fornisce, dietro richiesta e con le modalità stabilite dal Titolare, le informazioni sulla numerosità dei dati personali trattati e sui consensi raccolti.			
Sez. V **Misure organizzative**			
5.1. Il Responsabile ha adottato, documentandola, una struttura organizzativa che includa misure idonee a garantire un livello di sicurezza adeguato al rischio correlato alla natura del trattamento da esso effettuato	Sì ☐ No ☐		

5.2. Il Responsabile è un soggetto obbligato alla nomina di un DPO ai sensi dell'art. 37 del GDPR	Sì ☐ No ☐		
5.3. Il Responsabile ha nominato un DPO interno/esterno.	Sì ☐ No ☐		
5.4. Il Responsabile ha nominato, nell'ambito della sua struttura organizzativa, altre figure di supporto generale ai trattamenti: privacy manager, data manager, etc.	Sì ☐ No ☐		
5.5. Il Responsabile si avvale di società/consulenti specializzati nelle questioni giuridiche/tecniche del trattamento dei dati personali	Sì ☐ No ☐		
5.6. La struttura organizzativa del Responsabile prevede una chiara ripartizione delle funzioni e delle responsabilità in materia di trattamento e protezione dei dati personali oggetto della nomina	Sì ☐ No ☐		
5.7. Il Responsabile effettua, documentandoli, audit periodici per verificare che i processi aziendali siano conformi al proprio modello organizzativo	Sì ☐ No ☐		
5.8. Il Responsabile ha adottato una struttura organizzativa che include una verifica periodica dell'efficacia delle misure tecniche ed organizzative a presidio della sicurezza dei dati personali oggetto della nomina	Sì ☐ No ☐		
5.9. Il Responsabile, dietro richiesta del Titolare, fornisce un resoconto degli audit e delle verifiche di cui ai precedenti punti 5.7. e 5.8.	Sì ☐ No ☐		
Sez. VI Misure tecniche			
6.1. Il Responsabile ha implementato nella propria organizzazione misure tecniche idonee a garantire un livello di sicurezza adeguato al rischio e ne ha documentato l'adozione	Sì ☐ No ☐		

6.2. Il Responsabile ha implementato le proprie misure tecniche per adeguarle ai trattamenti oggetto della nomina	Sì ☐ No ☐		
6.3. I documenti cartacei ed i supporti informatici contenenti i dati personali oggetto della nomina sono conservati in luoghi protetti ove hanno accesso solamente i soggetti autorizzati dal Responsabile ad effettuare le operazioni di trattamento (ad esempio stanze o armadi chiusi a chiave)	Sì ☐ No ☐		
6.4. Il sistema informatico del Responsabile permette l'accesso ai server in cui sono conservati i dati personali oggetto della nomina alle sole utenze aziendali dei soggetti specificamente autorizzati	Sì ☐ No ☐		
6.5. Il Sistema degli accessi è stato implementato secondo il principio del "privilegio minimo"	Sì ☐ No ☐		
6.6. Il Responsabile ha stabilito, documentandolo e rendendolo accessibile a tutti i propri operatori autorizzati al trattamento dei dati personali, un regolamento interno relativo all'utilizzo degli strumenti informatici ed in particolare relativo ai metodi di utilizzo di Computer aziendali, account di posta elettronica aziendali e modalità di accesso ai sistemi informatici/telematici	Sì ☐ No ☐		
6.7. Il Responsabile ha chiaramente individuato (registrandone gli estremi identificativi) gli Amministratori di Sistema, il cui incarico risulta da documento scritto	Sì ☐ No ☐		
6.8. Il Responsabile ha riportato, per ciascun Amministratore di Sistema, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato	Sì ☐ No ☐		

6.9. Il Responsabile ha implementato, documentandoli, processi di verifica periodica (con cadenza almeno annuale) l'operato degli Amministratori di Sistema, in particolare con riferimento all'applicazione delle misure organizzative, tecniche e di sicurezza per il trattamento dei dati personali previste dalle norme vigenti	Sì ☐ No ☐		
6.10. Il Responsabile ha implementato, documentandoli, sistemi di registrazione degli accessi logici ai sistemi di elaborazione ed archiviazione da parte degli Amministratori di Sistema. Gli accessi logici così registrati vengono conservati per un periodo non inferiore a sei mesi	Sì ☐ No ☐		
6.11. Il Responsabile ha predisposto, documentandolo, un Sistema di Gestione della sicurezza informatica e delle informazioni idoneo a prevenire attacchi o incidenti informatici che potrebbero determinare una violazione dei dati personali trattati	Sì ☐ No ☐		
6.12. Il Responsabile implementa, documentandoli, processi idonei a garantire la comunicazione al Titolare di avvenute violazioni di dati personali (*data breach*), senza ritardo, e comunque, entro il termine stabilito dal Titolare dal momento in cui è venuto a conoscenza della violazione	Sì ☐ No ☐		
6.13. Il Responsabile ha implementato nel proprio sistema informatico *software antivirus*, *firewall* e procedure di aggiornamento periodico dei sistemi operativi, la cui adozione risulta documentata	Sì ☐ No ☐		
6.14. Il Responsabile ha implementato un sistema di accesso ai sistemi informatici protetto da password che preveda cambi frequenti e vincoli di	Sì ☐ No ☐		

complessità per le *password* adottate			
6.15. Il Responsabile ha implementato un sistema di VPN/VDI per le operazioni di trattamento effettuate all'esterno della rete informatica aziendale (ad esempio in caso di lavoratori distaccati in telelavoro o smart working)	Sì ☐ No ☐		
6.16. Il Responsabile ha implementato, documentandone l'adozione, dei sistemi di *Back-up* dei propri sistemi ed ha stabilito, documentandoli, dei processi di continuità operativa e *Disaster recovery*.	Sì ☐ No ☐		
6.17. Il Responsabile ha previsto, documentandoli, processi di smaltimento dei supporti informatici e cartacei idonei ad evitare il recupero dei dati personali eventualmente presenti sugli stessi (ad es., sovrascrittura dei dischi fissi, tritadocumenti, distruzione fisica dei supporti informatici).	Sì ☐ No ☐		
6.18. Il Responsabile ha previsto l'effettuazione di attività di *Vulnerability Assessment* e *Penetration Test*	Sì ☐ No ☐		
6.19. Il Responsabile ha implementato, documentandone l'adozione, strumenti atti a rilevare e segnalare tempestivamente anomalie nella rete riconducibili ad azioni (seppur tentate) di *data exfiltration* e simili	Sì ☐ No ☐		
6.20. Il Responsabile ha previsto, documentandone l'adozione, misure tecnologiche (es.: cifratura dei dati) ed organizzative per la sicurezza dei dispositivi mobili (portatili, smartphone, tablet).	Sì ☐ No ☐		
6.21. Nel caso in cui il Responsabile fornisca software ed applicazioni, nel processo di sviluppo è prevista l'adozione di linee guida per lo sviluppo del	Sì ☐ No ☐		

software sicuro (es.: AGID, OWASP).			
6.22. Nel caso in cui il Responsabile fornisca prodotti o strumenti per il trattamento dei dati (es. gestionali, ovvero realizzi/gestisca siti/portali) sono rispettati (laddove applicabili) i principi della protezione dei dati dalla progettazione (privacy by design o by default).	Sì ☐ No ☐		
6.23. Nel caso in cui il Responsabile realizzi/gestisca siti/portali effettua una valutazione del rispetto, sui medesimi, delle disposizioni del GDPR (informative, cookie, etc.)	Sì ☐ No ☐		
6.24. Il Responsabile, dietro richiesta del Titolare, fornisce informazioni aggiornate sulle misure tecniche adottate.	Sì ☐ No ☐		

3.4. - MODELLI UTILIZZABILI PER LE NOMINE DEI RESPONSABILI

ART. XY… NOMINA/DESIGNAZIONE A RESPONSABILE ESTERNO DEL TRATTAMENTO AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 679/2016[12]

Posto che la realizzazione dell'attività di cui in premessa comporta il trattamento di dati personali …….. relativi alle seguenti categorie di interessati …… [13], in relazione ai quali la Camera di commercio di ….. è Titolare del trattamento ai sensi dell'art. 4, n. 7 del Regolamento UE n. 679/2016 (di seguito anche GDPR), si conviene quanto segue.

Il contraente, nell'esecuzione delle attività affidate, opererà in qualità di Responsabile del trattamento ai sensi dell'art. 28, par. 1, del GDPR, impegnandosi a garantire la riservatezza dei dati personali degli interessati, che saranno affidati dall'Ente Camerale e/o autonomamente acquisiti durante l'intero processo di erogazione del servizio e a non comunicarli e/o diffonderli presso terzi. Con apposito allegato al presente contratto/convenzione, la cui sottoscrizione sarà condizione di efficacia delle obbligazioni contrattuali di cui al presente documento, potranno essere indicate le specifiche istruzioni cui il contraente dovrà attenersi.

La durata del trattamento coincide con la durata contrattuale di cui all'art. … del presente documento, fatte salve eventuali proroghe o rinnovi. La finalità del trattamento di cui al presente articolo è esplicitata nell'art. …. (oggetto del servizio).

In caso di violazione totale o parziale della normativa vigente (GDPR, D.Lgs. n. 196/2003, ….) o delle istruzioni impartite mediante il citato allegato, il contraente sarà soggetto a contestazione da parte dell'Ente Camerale che determinerà l'interruzione dei termini di pagamento. In tal caso, il contraente dovrà produrre, entro e non oltre 7 (sette) giorni lavorativi successivi alla suddetta contestazione, le proprie giustificazioni scritte. Ove le suddette giustificazioni non pervengano ovvero l'Ente Camerale non le ritenga condivisibili, si riserva l'insindacabilità di applicare le seguenti penalità:

- fino al … [xxx%] dell'importo contrattualmente previsto in caso di prima violazione;
- fino al … [yyy%] dell'importo contrattualmente previsto in caso di recidiva[14];

[verificare attentamente che l'importo delle penali non sia eccessiva]

- risoluzione del contratto con effetto immediato, ai sensi degli artt. 1453 e/o 1456 cod. civ. in caso di ulteriori violazioni.

Le penalità sono decurtate direttamente sull'importo del saldo da corrispondere. Rimane impregiudicata la possibilità di agire in sede di rivalsa in caso di eventuali danni subiti da terzi interessati o per le eventuali sanzioni amministrative comminate al Titolare.

[12] In alternativa, la previsione delle sanzioni per le violazioni della nomina ex art. 28 può essere indicata, secondo quanto previsto nel *format* di nomina riportato più avanti, nel successivo testo riquadrato.

[13] ATTENZIONE: Descrivere la tipologia dei dati personali oggetto di trattamento.

[14] Si tratta del noto meccanismo delle clausole penali, ex art. 1382 ss. c.c.

Si presti la dovuta attenzione a che l'entità non sia eccessivamente gravosa, posto il potere del giudice, in caso di controversia, di ridurne l'importo ex art. 1384 c.c. (Cfr., tra tante, Cass. 7 luglio 2016, n. 13902).

Le Parti di comune accordo adegueranno le clausole di cui al presente articolo e contenute nell'appendice contrattuale al modello di atto giuridico e/o clausole tipo ove predisposte dalla Commissione UE o dal Garante della protezione dei dati personali, ai sensi dell'art. 28, parr. 6-8, del GDPR.

Solo l'assunzione delle responsabilità ex art. 28 del GDPR a livello contrattuale (costituenti quindi specifica obbligazione contrattuale ai sensi dell'art. 1321 del c.c.) potranno consentire – in caso di danno causato da attività del Responsabile - l'attivazione della clausola di salvaguardia di cui all'art. 82, par. 2, del GDPR[15].

Gli stessi soggetti personalizzano e propongono, in allegato al **contratto, convenzione o atto giuridico analogo che definisce gli obblighi reciproci il seguente** documento (che quindi deve essere formalizzato contestualmente, quale elemento integrante e sostanziale del documento contrattuale). Si specifica che il contenuto di seguito riportato deve essere sempre **attentamente valutato e personalizzato** in funzione delle specifiche esigenze e "consistenza" dei trattamenti oggetto di regolamentazione:

ALLEGATO AL CONTRATTO _____

[ovvero lettera autonoma facente riferimento al contratto]

DISCIPLINA DELLA PROTEZIONE DEI DATI IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

(art. 28 del Regolamento UE 679/2016)

Oggetto: Nomina della Società …….. a Responsabile esterno del trattamento di dati personali ai sensi degli artt. 4, n. 8 e 28 del Regolamento UE 679/2016 per l'incarico relativo a "……." da parte della ……

Con riferimento al rapporto contrattuale in oggetto, al fine di adempiere agli obblighi formali e sostanziali disposti dal Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito indicato come "GDPR"), la Camera di commercio di …….. (indicata, di seguito, anche come "Camera di commercio" o "Titolare"), in qualità di Titolare del trattamento dei dati in oggetto – cui spettano le decisioni in ordine alle finalità ed ai mezzi dei trattamenti (anche affidati all'esterno) ai sensi dell'art. 4, n. 7), del GDPR – designa la Società …….. quale responsabile esterno del trattamento dei dati per le fasi di sua competenza, così come definite nella scheda tecnica/offerta presentata con la Vs. comunicazione n. …… del ……..

Premesso che:

- le attività oggetto dell'incarico comportano il trattamento delle seguenti tipologie di dati personali:
  1) …
  2) …
  3) …

[15] "… Un responsabile del trattamento 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*…".

[indicare, se del caso, anche le relative categorie di interessati]

- i suddetti dati personali sono trattati per le seguenti finalità:
  a) ……..;
  b) ……;
  c) ……;
  d) ……;

  [Se del caso, le tipologie di dati personali, le categorie di interessati e le specifiche finalità dei trattamenti, si possono indicare in uno o più appositi allegati]

- la verifica del possesso dei requisiti di esperienza, capacità ed affidabilità finalizzate a fornire "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessati" richiesta dall'art. 28, par. 1, del GDPR, è stata effettuata dalla scrivente Camera di commercio nell'ambito dell'iter istruttorio presupposto dell'affidamento contrattuale di cui trattasi; in particolare, le misure di sicurezza tecniche, informatiche ed organizzative in atto (**attestate dal legale rappresentante mediante produzione di un documento descrivente il dettaglio delle misure implementate**) sono state valutate come idonee, in relazione alla natura, oggetto, contesto e finalità del trattamento come definito nell'incarico di cui in oggetto. La Camera di commercio si riserva, comunque, a sua discrezione, una verifica, anche mediante apposito audit, con particolare riferimento alla loro adeguatezza e ai trattamenti effettuati per suo conto;

[I soggetti pubblici e le società in house del sistema camerale possono fare riferimento alle misure di sicurezza di natura tecnologica, organizzativa e procedurale definite come obbligatore per le Pubbliche amministrazioni e per le Società in controllo pubblico dalla Circolare AgID n. 2/2017 recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (che vanno astrattamente considerate come idonee, tenuto conto di quelle "minime" indicate nella *check list* allegata alla citata circolare. In ogni caso ne va **verificata e dichiarata la specifica adeguatezza** e, se del caso, devono essere implementate oltre il livello "minimo")].

- con la sottoscrizione del presente atto, la Società …….. in qualità di Responsabile esterno del trattamento ex art. 28 del GDPR, nella persona del Direttore Generale, ……, - che agisce in qualità di soggetto delegato dalla Società ad assumere impegni contrattuali in materia - accetta la suddetta nomina confermando la diretta ed approfondita conoscenza degli obblighi che si assume e assicura, sotto la propria responsabilità, di aver adempiuto o di adempiere, in funzione delle caratteristiche del trattamento affidato, alle seguenti istruzioni; in proposito, la Camera di commercio potrà, a sua completa discrezione ove ritenuto necessario, richiedere al soggetto sopra menzionato una dimostrazione documentale sull'osservanza delle disposizioni impartite, anche mediante una ispezione;

- la sottoscrizione per accettazione della presente lettera di nomina costituisce condizione di efficacia ed esecutività dell'incarico citato in oggetto.

Istruzioni impartite

L'attività oggetto di affidamento rientra nell'ambito delle funzioni istituzionali della Camera di commercio con riferimento ai compiti di cui all'art. 2, comma 2, della legge n. 580/1993.

Per effetto dell'accettazione del suddetto incarico, la Società …. è formalmente autorizzata a visionare e trattare tutte le informazioni di carattere personale il cui trattamento è strettamente necessario per l'assolvimento del medesimo.

La Società ….., nel precisare, confermare e garantire, con la sottoscrizione del presente atto, di offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi tutti i requisiti del GDPR e per garantire la tutela dei diritti degli interessati, si impegna a:

1) curare che i dati personali oggetto del trattamento siano trattati in modo lecito e corretto, nonché secondo gli ulteriori principi indicati all'art. 5 del GDPR. A tale scopo la Società …….. si atterrà alle disposizioni contenute nel GDPR, nel Codice della privacy (D. Lgs. n. 196/2003), nelle disposizioni vigenti anche successive al presente incarico, nei provvedimenti del Garante per la protezione dei dati personali (di seguito indicato come "Garante") applicabili, nonché ad eventuali ulteriori istruzioni che saranno fornite dalla Camera di commercio;

2) trattare come assolutamente riservata e confidenziale ogni informazione, notizia o dato personale di cui sia venuta o possa venire a conoscenza e ad autorizzare a compiere operazioni di trattamento di cui al presente atto esclusivamente soggetti che si siano impegnati, per iscritto, all'obbligo di riservatezza e/o al segreto d'ufficio (quest'ultimo se applicabile), impartendo loro adeguate e documentate istruzioni al fine di garantire il rispetto della normativa precedentemente richiamata;

3) mettere in atto le misure tecniche ed organizzative adeguate al fine di garantire e mantenere un livello di sicurezza adeguato al rischio, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

La Società …… si impegna espressamente:

a) a comunicare prontamente alla Camera di commercio – indirizzando le comunicazioni presso l'Ufficio legale/Altro Ufficio *[precisare]* dell'Ente - eventuali situazioni sopravvenute (tra cui a puro titolo esemplificativo, sanzioni comminate dal Garante o da Autorità giudiziarie ordinarie o amministrative, anche non relative alle attività di trattamento oggetto del presente atto) che, per qualsiasi ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico;
b) a non utilizzare i dati personali acquisiti per finalità che non siano strettamente necessarie per l'esecuzione del servizio come definiti nel contratto di cui in oggetto, ed a non utilizzare i dati personali acquisiti per finalità che non siano strettamente attinenti alle attività contrattualmente definite;
c) ad individuare ed autorizzazione i soggetti (persone fisiche), debitamente formati, che per suo conto svolgeranno il trattamento, impartendo loro adeguate e documentate istruzioni al fine di garantire il rispetto della normativa applicabile, delle condizioni di liceità del trattamento e dei vincoli impartiti attraverso il presente atto, nonché ad ottenere da questi un formale impegno alla riservatezza;
d) ad attuare un controllo sull'attività svolta dalle persone autorizzate al trattamento al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate e, comunque, delle istruzioni impartite;
e) ove il contratto di cui in oggetto non preveda una autorizzazione generale in proposito, a non ricorrere ad eventuali ulteriori sub-contraenti senza previa autorizzazione scritta da parte della

Camera di commercio, soprattutto nel caso in cui ciò comporti il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale; l'autorizzazione potrà essere eventualmente rilasciata sulla base di una preventiva verifica di affidabilità di tali soggetti condotta e rendicontata dal Responsabile al Titolare, finalizzata a garantire lo stesso livello di sicurezza nei trattamenti; in caso di autorizzazione, il Responsabile dovrà adottare opportune clausole contrattuali al fine di richiamare in capo ai sub-contraenti l'obbligo di rispettare le misure e gli accorgimenti stabiliti dalla presente designazione nonché un analogo livello di sicurezza adottato dal contraente e valutato come idoneo dalla Camera di commercio. Le stesse modalità sono valide anche per le eventuali aggiunte o sostituzione dei sub-responsabili *[ATTENZIONE: da personalizzare in funzione dell'autorizzazione generale/specifica che si vuole rilasciare]* ***ovvero*** nell'eventualità – consentita dal contratto di cui in oggetto *[se non è consentita si indicherà espressamente]* – di successivo affidamento a terzi (persone fisiche/giuridiche individuate come sub-responsabili esterni del trattamento, con l'esclusione che questi ultimi possano, a loro volta, nominare propri sub-responsabili) di parte delle attività previste, la Società …….. si impegna, altresì:

- a verificare preventivamente l'affidabilità di tali soggetti al fine di garantire al Titolare lo stesso livello di sicurezza nei trattamenti;
- ad adottare opportune clausole contrattuali al fine di richiamare in capo ai medesimi soggetti l'obbligo di rispettare le misure e gli accorgimenti stabiliti;

f) ad adottare procedure di controllo sull'attività svolta dai soggetti di cui ai punti d) ed e), al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate, degli obblighi di riservatezza e, comunque, delle istruzioni impartite;

g) a non comunicare comunque ad ulteriori soggetti terzi (soprattutto ove possibile qualificare un trasferimento di dati verso paesi terzi od organizzazioni internazionali) i dati oggetto di trattamento, senza preventiva autorizzazione scritta del Titolare;

h) ad adottare tutte le misure di sicurezza tecnico-informatiche ed organizzativo-gestionali **dichiarate in fase contrattuale**; nell'eventualità di modifica delle stesse (ad es., in caso di modifiche evolutive di infrastrutture, apparati, applicativi di lavoro e modalità gestionali) dovrà essere garantito – ad esito di specifica analisi di impatto – un livello di sicurezza almeno analogo a quello risultante dall'analisi dei rischi formalizzata; in caso contrario, è fatto specifico obbligo di condividere con la Camera di commercio le nuove specifiche di trattamento, al fine di consentire la verifica del mantenimento dell'idoneità allo svolgimento dell'incarico;

i) a conservare i dati personali oggetto di trattamento per tutto il periodo di tempo necessario per la realizzazione delle attività, ed a cancellarli in via definitiva entro e non oltre i xxx giorni successivi il decorso dei termini temporali previsti dal contratto e da eventuali rinnovi o proroghe. Sono fatte salve le conservazioni dei dati personali previste dall'adempimento di obblighi di legge ed esclusivamente per le finalità da queste indicate;

j) a provvedere, nei confronti degli interessati, al rilascio dell'informativa – relativa all'attività da svolgere, contenente tutti gli elementi necessari ai sensi dell'art. 13 del GDPR e ad acquisirne il consenso – ove necessario – con le modalità richieste per la specifica attività dalla stessa normativa; il format di informativa dovrà essere predisposto dalla Società … e concordato con la Camera di commercio alla quale, in qualità di Titolare, spetta ogni decisione in merito[16]. Se i dati personali non sono stati ottenuti dall'interessato bisogna fornire agli stessi le informazioni di cui all'art. 14 del GDPR;

[16] Questa previsione è stata concepita per i rapporti intercorrenti tra le Camere di commercio e strutture in house (proprie o nazionali), ovvero aziende speciali. Dato che spesso la progettualità – per esempio sul versante tecnico – 'proviene' da questi soggetti è chiesta una collaborazione maggiore nella redazione dell'informativa. L'informativa spetta, infatti, sempre al Titolare.

k) a garantire, sentito previamente il Titolare, idoneo riscontro all'interessato in caso di richiesta di esercizio dei diritti di cui agli artt. 15 e ss., del GDPR, ove indirizzata direttamente alla Società …, informando contestualmente il Titolare in tutti i casi in cui tale attività possa risultare dannosa ai fini della corretta esecuzione dell'incarico o possa comportare un qualsivoglia pregiudizio alla Camera di commercio stessa (ad es., richiesta di blocco o limitazione del trattamento)[17];
l) a fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultima, i dati e le informazioni necessarie per:
   - una tempestiva difesa in eventuali procedure instaurate davanti al Garante ovvero altra Autorità giudiziaria o amministrativa per effetto del trattamento dei dati in cui sia coinvolta la Società ….;
   - dare tempestivo riscontro all'interessato che eserciti i diritti di cui alla lettera precedente direttamente nei confronti del Titolare;
   - compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità giudiziaria o, comunque, dalle Forze dell'Ordine.

La Società …. si impegna inoltre:

m) a comunicare eventuali violazioni dei dati personali o presunte tali (a puro titolo esemplificativo: accessi abusivi, azione di malware, incendi o altre calamità, etc.) che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse, al fine di consentire alla Camera di commercio, se del caso, l'adempimento degli obblighi di notificazione al Garante ed agli interessati, come previsto dagli artt. 33 e 34 del GDPR. La comunicazione deve avvenire **entro 24 ore** dal momento in cui la Società … è venuta a conoscenza della violazione con l'obbligo di collaborare attivamente con la Camera di commercio, con i suoi delegati e con il Responsabile per la Protezione dei Dati (RPD/DPO), nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante e ai soggetti interessati, per quanto previsto nella normativa vigente;
n) a fornire, in caso di necessità, la massima disponibilità e collaborazione affinché il Titolare possa, direttamente o per il tramite di consulenti di propria fiducia, condurre verifiche anche presso la sede della Società … e degli altri Sub-responsabili eventualmente designati;
o) a prestare, in generale, la più ampia e completa collaborazione alla Camera di commercio e al suo RPD/DPO, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
p) in fase di rendicontazione delle attività svolte, a relazionare al Titolare sul buon esito delle attività di trattamento secondo gli standard precedentemente definiti, confermando esplicitamente la cancellazione definitiva dei dati personali acquisiti, fatto salvo quanto indicato alla precedente lett. i).

Inosservanza delle istruzioni e risoluzione

1. Fatte salve le disposizioni del GDPR e del Codice della privacy, qualora la Società …. violi gli obblighi che gli incombono a norma della presente nomina, la Camera di commercio può dare istruzioni per sospendere il trattamento dei dati personali fino a quando la Società … rispetti le presenti istruzioni o non sia risolto il contratto.

[17] Nelle stesse ipotesi indicate nella precedente nota, la gestione operativa della risposta agli interessati può essere demandata al Responsabile (si pensi alla situazione in cui questo gestisce una casella mail di pertinenza del Titolare specificatamente attivata per la gestione dell'incarico attribuito). Si ricorda, tuttavia, che spetta al Titolare rispondere alle richieste relative ai diritti degli interessati.

2. La Società …. informa prontamente la Camera di commercio qualora, per qualunque motivo, non sia in grado di rispettare le istruzioni di cui alla presente nomina.
3. La Camera di commercio ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali qualora:

a) il trattamento dei dati personali da parte della Società … sia stato sospeso dal Titolare del trattamento ai sensi del precedente punto 1 e il rispetto delle istruzioni di cui alla nomina non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
b) la Società …. violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del GDPR o del Codice della privacy;
c) la Società … non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi sul trattamento dei dati personali.

4. Sono in ogni caso fatte salve le penalità, previste dal contratto indicato in oggetto, con riferimento al trattamento di dati personali. *Oppure, in alternativa al primo periodo:* 4. La violazione delle istruzioni comporta la corresponsione delle seguenti penalità …. [*se non sono definite nel contratto con riferimento al trattamento dei dati personali*].
5. La Società ….. ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali sulla base delle istruzioni della presente nomina qualora - dopo aver informato la Camera di commercio che, a suo parere motivato, le istruzioni del Titolare violano il GDPR o le disposizioni applicabili, nazionali o comunitarie, relative alla protezione dei dati - la Camera di commercio insista sul rispetto delle istruzioni.
6. In caso di violazione delle disposizioni impartite, determinando autonomamente le finalità e i mezzi del trattamento, oltre alla comminazione delle sanzioni contrattualmente previste, la Società ….. risponderà in solido per qualsiasi danno causato agli interessati.

La presente nomina è valida per tutto il periodo di durata degli accordi contrattuali e dei successivi eventuali rinnovi. È da ritenere revocata, con effetto immediato e senza obbligo di preavviso, in caso di recesso unilaterale o consensuale dall'incarico citato in premessa.

Pregando di restituire alla Camera di commercio una copia della presente lettera, datata e firmata per accettazione, via pec, all'indirizzo ……, si inviano i più cordiali saluti.

3.5. - LA DECISIONE DELLA COMMISSIONE EUROPEA N. 2021/915 DEL 4 GIUGNO 2021

La Commissione europea, con la decisione di esecuzione 2021/915 del 4 giugno 2021 – riportata in allegato alle presenti Linee guida – ha definito delle clausole contrattuali tipo per le nomine dei responsabili, ai sensi dell'art. 28 del GDPR.

Tali clausole contrattuali tipo **non sono obbligatorie** ma sono *consigliate* dalla Commissione, soprattutto quando ciò sia necessario per far sì che il Titolare possa definire le regole del trattamento in tutte quelle ipotesi in cui la controparte (cioè il Responsabile da nominare), data la sua potenziale prevalenza, tenda a "condizionare" le regole che lo riguardano, per esempio con una serie di clausole di esclusione di responsabilità. In una situazione del genere l'utilizzo del contratto-tipo definito dalla Commissione – che è ritenuto *ex lege* conforme con il GDPR (e con l'obiettivo appena indicato) – non può essere contestato dal Responsabile.

Il Titolare può comunque riferirsi a quanto indicato dall'art. 28, ovvero utilizzare alcune clausole contrattuali-tipo, a condizione che di queste ultime non sia vanificata la formulazione o il precetto

sottostante (per esempio con altre clausole od accordi che, indirettamente, ve vanifichino l'efficacia).

La parte più discussa di dette clausole è costituita dall'utilizzo di sub-responsabili. La clausola-tipo 7.7. prevede, al riguardo, due opzioni che sono riportate nel riquadro seguente.

"OPZIONE 1: AUTORIZZAZIONE PRELIMINARE SPECIFICA: Il responsabile del trattamento non può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del titolare del trattamento conformemente alle presenti clausole senza la previa autorizzazione specifica scritta del titolare del trattamento. Il responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno [SPECIFICARE IL PERIODO] prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al titolare del trattamento di decidere in merito all'autorizzazione. L'elenco dei sub-responsabili del trattamento autorizzati dal titolare del trattamento figura nell'allegato IV. Le parti tengono aggiornato tale allegato".

"OPZIONE 2: AUTORIZZAZIONE SCRITTA GENERALE: Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno [SPECIFICARE IL PERIODO], dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento in questione. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione".

La Camera di commercio verificherà se ritenga più opportuno approvare specificamente la possibilità di ricorso ad un sub-responsabile, ovvero "verificare" – in caso di autorizzazione generale – l'elenco dei sub-responsabili del Responsabile. Tutto ciò se intenda utilizzare una o l'altra di dette clausole-tipo.

Nel modello di nomina predisposta per il sistema camerale, nelle ipotesi in cui sia consentito l'utilizzo di sub-responsabili (benché possa essere esercitato un controllo anche su questi ultimi), tranne quando non siano autorizzati direttamente con la nomina del Responsabile, si lascia la possibile scelta al Responsabile, poiché non è sempre possibile in anticipo sapere quale situazione si deve affrontare e che richiede la presenza di un sub-responsabile. In quest'ultimo caso, il Responsabile è tenuto a garantire che tutto il complesso di valutazioni e di regole a lui applicabili siano *integralmente applicabili* anche al sub-responsabile.

Per maggiore cautela, nel modello di nomina, **non è ammessa la possibilità che la facoltà del Responsabile di individuare (successivamente) un sub-responsabile possa poi consentire al sub-responsabile di fare altrettanto, cioè di nominare un suo sub-responsabile** (che sarebbe un sub-sub-responsabile rispetto al Titolare).

3.6. - CHIARIMENTI IN CASO DI ATI/RTI

In caso di affidamenti ad Associazioni o Raggruppamenti Temporanei di Imprese, in relazione alle specifiche responsabilità derivanti dalla forma di associazione adottata (di tipo orizzontale, verticale o mista), le istruzioni di cui al paragrafo precedente vanno formalizzate:

- all'ATI/RTI, se il trattamento è effettuato unitariamente;
- per ciascuna Società, se il trattamento è effettuato settorialmente, per quanto di rispettiva competenza.

In proposito, si specifica che con la presentazione dell'offerta congiunta,

a) le imprese riunite in RTI/ATI orizzontale assumono una responsabilità solidale nei confronti della stazione appaltante;
b) per le imprese riunite in RTI/ATI verticale la responsabilità è invece limitata all'esecuzione delle prestazioni di rispettiva competenza (lavori scorporabili o, nel caso di servizi e forniture, prestazioni secondarie), ferma restando la responsabilità della mandataria per l'intero appalto.

3.7. - ACQUISIZIONE DI SISTEMI E SERVIZI CON FUNZIONI DI AMMINISTRAZIONE DEI SISTEMI

Gli affidamenti che comportino l'acquisizione di sistemi o servizi di tipo applicativo o infrastrutturale, prevedono di regola attività di **assistenza e manutenzione** svolta direttamente dal soggetto affidatario (o suoi delegati). Tale attività, seppur non ha come obiettivo o ad oggetto un "trattamento" di dati personali[18] può comportare comunque anche "solo incidentalmente" la conoscibilità dei dati, ai soli fini dell'espletamento delle loro consuete attività; tali soggetti sono comunque concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Il punto 3-bis del Provvedimento a carattere generale 27 novembre 2008 del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (in G.U. n. 300 del 24 dicembre 2008) e s.m.i., prevede che nel caso di servizi di amministrazione di sistema affidati in outsourcing, ciò avvenga **nell'ambito della designazione a Responsabile esterno del trattamento** (che in questi casi va quindi necessariamente effettuata).

In questi casi:

a) la valutazione preliminare all'affidamento deve essere "rafforzata" in considerazione della rilevanza e delicatezza di tali peculiari mansioni rispetto ai trattamenti di dati personali svolti per le proprie funzioni istituzionali;
b) l'allegato contrattuale deve contenere anche le seguenti specifiche gestionali:

Istruzioni impartite

…

Il contraente si impegna espressamente:

- relativamente a quanto prescritto dal Provvedimento del Garante del 27 novembre 2008 e s.m.i., a:
  - ✓ procedere alla designazione individuale degli amministratori di sistema o figura equivalente coinvolti nelle attività di cui in oggetto, previa valutazione delle caratteristiche di esperienza, capacità, e affidabilità, anche in considerazione delle responsabilità che possono derivare in caso di incauta o inidonea designazione;
  - ✓ a riportare, per ciascuna figura coinvolta, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

[18] A meno che il database che raccoglie i dati/le informazioni non sia residente presso sedi/apparecchiature del contraente ovvero in cloud, nel qual caso è qualificabile almeno il trattamento di "conservazione" dei dati.

- ✓ a conservare e fornire all'Ente Camerale, a semplice richiesta e secondo le modalità da esso indicate, il nominativo dell'amministratore di sistema o figure equivalenti designate;
- ✓ a verificare periodicamente – anche attraverso idonei sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici, che dovranno essere conservati per almeno sei mesi a far data dalla conclusione delle attività contrattuali - l'operato di tali figure in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza adottate; l'esito di tali valutazioni dovrà essere trasmesso alla Camera, a semplice richiesta e secondo le modalità indicate da quest'ultima.

4 - REGISTRI DEGLI ACCORDI DI CONTITOLARITA' E DELLE NOMINE DEI RESPONSABILI

Ai fini di un generale controllo sugli atti di gestione del trattamento dei dati personali, condiviso con altri Titolari, ovvero demandato a Responsabili (e sub-responsabili) esterni, rispettivamente sulla base degli artt. 26 e 28 del GDPR, vengono istituiti due appositi Registri: il Registro degli Accordi di Contitolarità ed il Registro delle nomine a Responsabile del trattamento.

[N.B: in luogo di istituire degli appositi "Registri" si può anche optare per la previsione di meri elenchi, contenenti gli stessi contenuti dei Registri]

4.1. - REGISTRO DEGLI ACCORDI DI CONTITOLARITA'

Il Registro degli Accordi di Contitolarità è costituito dalle seguenti informazioni

Registro degli Accordi di Contitolarità
(ex art. 26 del GDPR)
stipulati dalla Camera di commercio di ……..

N.	Contitolare/i	Oggetto dell'accordo	Data avvio dell'Accordo	Termine dell'Accordo (con indicazione eventuale rinnovo)	DPO del Contitolare/i	Ufficio del Titolare che gestisce l'Accordo

Il Registro è tenuto presso l'Ufficio del Delegato del Titolare, nell'ambito della quale sono conservati anche gli Accordi ed è aggiornato dal Gruppo di Lavoro del Delegato del Titolare, **previa comunicazione da parte degli uffici che sono competenti per la gestione del contratto**.

4.2. - REGISTRO DELLE NOMINE A RESPONSABILE DEL TRATTAMENTO

Il Registro delle nomine dei Responsabili del trattamento è costituito dalle seguenti informazioni.

Registro dei Responsabili del trattamento
(ex art. 28 del GDPR)
designati dalla Camera di commercio di ……..

N.	Nominativo Responsabile	Oggetto della nomina	Contratto cui è connessa la nomina (data/num. Determin.)	Data avvio Trattamento	Termine Trattamento (e sua proroga)	Sub-Respons.li nominati dal Responsabile	Ufficio del Titolare che gestisce il contratto

Il Registro è tenuto presso l'Ufficio del Delegato del Titolare, mentre le singole nomine sono tenute dagli uffici che sono competenti per la gestione del contratto cui accede la nomina a Responsabile.

Tali uffici sono tenuti a comunicare le singole nomine al Gruppo di lavoro Privacy – che provvederà ad aggiornare il suddetto Registro.

5. ULTERIORI CASISTICHE

5.1. - INCARICHI PROFESSIONALI O DI CONSULENZA

Teoricamente, un soggetto esterno – persona fisica – che tratti i dati per conto di un Titolare o Responsabile del trattamento può essere inquadrato nei seguenti schemi:

a) Titolare autonomo del trattamento, ad es., quando l'incarico conferito sia connotato da spiccata **autonomia professionale e gestoria**[19]**;**
b) Responsabile esterno del trattamento ex 28 del GDPR;
c) soggetti autorizzati al trattamento (art. 29 del GDPR e art. 2-*quaterdecies*, comma 2 del D.Lgs. n. 196/2003[20], anche richiamando una precedente interpretazione del Garante per la Protezione dei dati personali[21] (ove operanti sotto *l'autorità diretta* del Titolare).

In concreto, la valutazione deve essere effettuata in modo sostanziale, con specifico riguardo allo schema contrattuale alla base del rapporto *ed alla concreta regolamentazione delle modalità operative di realizzazione delle attività*. Di conseguenza:

- qualora si ricada nelle casistiche di cui alla lett. a), basterà richiamare nel documento contrattuale tale qualifica e l'assunzione diretta da parte del soggetto esterno delle relative responsabilità;
- qualora si ricada nella seconda soluzione, si rinvia per il dettaglio delle soluzioni gestionali ai precedenti paragrafi;
- nel caso in cui si scelga la soluzione sub c), a tali soggetti dovranno applicarsi idonee clausole contrattuali in riferimento ai trattamenti oggetto dell'incarico stesso, contenenti le eventuali istruzioni specifiche necessarie per l'esecuzione delle attività previste.

5.2. - CONTRATTI/CONVENZIONI PER LA FORNITURA DI PERSONALE

Nel caso di contratti/convenzioni con soggetti esterni (ad es., Società/Agenzie di somministrazione lavoro) che forniscano personale da impiegare presso le Strutture organizzative dell'Ente Camerale in processi/attività che possano comportare la conoscibilità di dati personali, non si concretizza una "comunicazione" di dati verso una struttura esterna (ovvero di un caso di trattamenti "esternalizzati" nell'ambito della Struttura organizzativa del soggetto esterno); in tali circostanze, l'utilizzo di personale esterno avviene nell'ambito dell'organizzazione del Titolare, e

[19] E' il caso ad es., dei componenti del Collegio Sindacale ovvero del revisore legale dei conti (i cui ampi poteri di controllo conferiti dalla normativa di riferimento non sono conciliabili con altre figure previste dalla legge - responsabile, autorizzato - che presuppongono una subordinazione al Titolare del trattamento in ordine alla definizione di compiti, istruzioni impartite e vigilanza sull'attività espletata); del notaio, dell'avvocato nell'ambito della procura alle liti, del consulente tecnico di parte, del medico competente in quanto operanti in totale autonomia, responsabilità professionale e con una autonoma organizzazione di mezzi (…). SI rinvia a quanto detto, in precedenza, nel testo, al paragrafo "Responsabili esterni del trattamento" (par. 3.1.).

[20] "Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

[21] Cfr. in particolare https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921

non è dunque necessario verificare l'affidabilità della controparte contrattuale e vincolarla ad operare ai sensi dell'art. 28 del GDPR.

In questi casi è però opportuno che i contratti/convenzioni/atti deliberativi rechino la seguente clausola (da personalizzare a cura del RUP/dirigente proponente).

ART. XY… TRATTAMENTO DEI DATI PERSONALI

Posto che la realizzazione dell'attività di cui in premessa potrà comportare la conoscibilità – da parte dei soggetti da Voi incaricati – di dati personali _____*descrivere*_____ in relazione ai quali la Camera di commercio di …… è Titolare del trattamento ai sensi dell'art. 4, n. 7 del Regolamento UE 679/2016 (di seguito anche GDPR), si conviene quanto segue.

Nel quadro degli obiettivi generali di tutela della dignità e riservatezza degli interessati promossi dalla normativa richiamata, il contraente garantisce che i professionisti/soggetti coinvolti siano a conoscenza della normativa rilevante e delle responsabilità relative al corretto trattamento dei dati che essi si assumono nello svolgimento delle attività oggetto della presente convenzione. Per effetto della sottoscrizione della presente convenzione, a tali professionisti/soggetti è richiesto:

- ✓ il rispetto dei più elevati standard di segreto professionale, con l'obbligo di mantenere riservati qualsiasi notizia, documentazione, dato e informazione concernente direttamente o indirettamente le prestazioni svolte, con esplicito divieto di: utilizzarli per finalità diverse da quelle oggetto della convenzione; divulgarli, comunicarli o renderli disponibili a terzi, in tutto o in parte, senza esplicita autorizzazione scritta della Camera; duplicarli, riprodurli od asportarli dai luoghi di trattamento convenuti;
- ✓ di adottare le procedure, le istruzioni operative e le misure di sicurezza che verranno loro trasferite dal Dirigente responsabile della Struttura organizzativa di allocazione, in qualità di soggetto delegato ad acta dal Titolare del trattamento.

Gli obblighi di riservatezza e segreto professionale rimarranno efficaci - in capo ai singoli professionisti/soggetti - anche oltre la data di conclusione delle attività di cui alla presente convenzione.

Il rapporto non prevede invece responsabilità relativamente all'ottemperanza ad altri obblighi normativi quali prestazione dell'informativa e acquisizione del consenso dell'interessato che restano, qualora necessari, in capo al Titolare del trattamento.

6 - LA NOMINA DI INFOCAMERE QUALE RESPONSABILE DEI TRATTAMENTI

La nomina di InfoCamere, quale Responsabile dei trattamenti per conto delle Camere, è caratterizzata da alcune sostanziali differenze che sono connesse alla peculiare situazione che connota detta società.

InfoCamere, spesso per esplicita indicazione del legislatore (v. art. 8, comma 6, della legge n. 580/1993 per il registro delle imprese, ovvero, per la crisi d'impresa, dove è qualificata "soggetto gestore"[22]), è un Responsabile "necessario" di alcuni trattamenti.

La sua "necessità" deriva, in massima parte, dalla circostanza che detti trattamenti vengono gestiti attraverso una complessa infrastruttura informatica e telematica che richiede una società altamente specializzata che è stata costituita appositamente per queste funzioni. Tale società, peraltro, determina parte consistente dei "mezzi" impiegati per il trattamento, sui quali non è possibile (a meno di compromettere la uniforme gestione del servizio a livello nazionale), prospettare che le singole Camere-Titolari possano indicare "istruzioni" del tutto autonome e potenzialmente in contraddizione.

InfoCamere è inoltre una società *in house* del sistema camerale, connotata dalle funzioni consortili, sicché alcune decisioni passano attraverso gli organi della società ed il collegamento tra questi ed il controllo analogo caratteristico delle società *in house*, ai sensi del D.Lgs. n. 175/2016.

Le Camere di commercio, socie di InfoCamere, per quanto attiene ai servizi consortili "obbligatori", sentita anche Unioncamere ed i rispettivi DPO, per le questioni inerenti il rispetto del GDPR, hanno concordato:

a) le modalità ed il testo della nomina di InfoCamere quale Responsabile, ex art. 28 del GDPR;

b) le informazioni, la forma e le modalità attraverso le quali InfoCamere, nel rendere disponibile una analitica Relazione sulle attività di trattamento, fornisce ai Titolari gli strumenti per operare, anche autonomamente, i controlli previsti dal citato art. 28[23].

Per i servizi consortili "a richiesta", le singole Camere – anche sulla base del modello precedentemente indicato – possono ovviamente definire delle specifiche istruzioni, ovvero controlli ed altre questioni legate alle modalità di gestione contrattuale dei rapporti.

[22] In attuazione dell'art. 3, comma 1, del D.L. 24 agosto 2021, n. 118, come convertito dalla legge 21 ottobre 2021, n. 147.

[23] Con la comunicazione n. D10000 del 2 maggio 2022, InfoCamere ha trasmesso alle Camere di commercio la "Relazione di InfoCamere alle Camere di commercio in merito al ruolo di Responsabile dei trattamenti affidati dalle Camere alla società consortile ai sensi dell'art. 28 del GDPR".