Allegato n. 2

CAMERA DI COMMERCIO
DEL SUD EST SICILIA

Camera di commercio, industria, artigianato e agricoltura del Sud Est Sicilia

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

ai sensi del Regolamento UE 2016/679

PREMESSA

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 di soggetti esterni in rapporti contrattuali/convenzionali con la Camera di Commercio del Sud Est Sicilia e la relativa allocazione 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) 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[1].

Le presenti linee guida sono portate a conoscenza, anche attraverso attività di sensibilizzazione e di formazione, a tutti i Dirigenti, funzionari o, comunque, referenti delle Aree/Uffici della Camera di Commercio di Sud Est Sicilia, di seguito anche "Ente" o "CCIAA".

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Contitolare del trattamento (art. 4, n. 7 e art. 26 del GDPR);
2. Responsabile del trattamento (art. 4, n. 8 e art. 28 del GDPR);
3. 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" e s.m.i.);
4. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (WP169).

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. n. 101/2018
Garante	Garante per la protezione dei dati personali

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

WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati)
RPD/DPO	Responsabile della protezione dei dati (*Data Protection Officer*)
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 CCIAA
Responsabile	Responsabile (esterno) del trattamento ex art. 28 GDPR

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

RAPPORTI DI CONTITOLARITÀ

Due soggetti possono assumere la qualifica di **Contitolari** ai sensi dell'art. 26 del GDPR, quando, in relazione ed 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.

La Contitolarità dovrebbe dunque rinvenirsi ogniqualvolta due Titolari decidono insieme di trattare i dati per una finalità (interamente o parzialmente) comune e ciascuno dei due abbia l'effettiva facoltà / il diritto (gli elementi essenziali dei) mezzi dell'attività di trattamento.
La contitolarità determina la responsabilità comune per un'attività di trattamento.
Tale rapporto deve essere disciplinato in un accordo specifico in cui vengono individuate le rispettive responsabilità in merito all'osservanza degli obblighi previsti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e alle informazioni di cui agli artt. 13 e 14 GDPR.
In proposito, si specifica che la qualifica di contitolari del trattamento può verificarsi:

a) in forza di una Legge o disposizione di fonte secondaria[2] (c.d. "**esplicita competenza giuridica**") che attribuiscano alla Camera di Commercio una "funzione istituzionale" (cfr. la legge n. 580/1993, nonché le altre disposizioni nazionali o regionali che attribuiscono una competenza istituzionale, quali riportate – nel trattamento dei dati personali – nel Registro dei trattamenti);

b) in forza di un **contratto o atto analogo tra le parti** che consentano di assegnare ad una od entrambe le parti tale qualifica;

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 580/1993, ovvero da altra disposizione normativa, l'Ente Camerale ponga in essere progettualità o servizi gestiti congiuntamente con altre Camere di commercio o con l'Unioncamere, o con altri soggetti appartenenti al sistema camerale.

2 Ad es., decreti ministeriali.

La preliminare 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 ovvero il Responsabile per la Protezione dei Dati di uno dei due titolari) 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[3] 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[4].

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 & by default, e 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……

---

3 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 04/10/2017, reperibile al seguente link: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati .

Più di recente cfr. Garante per la Protezione dei dati Personali, Provvedimento n. 467 dell'11/10/2018 "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", in GU n. 269 del 19/11/2018.

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

4 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).

Di seguito si riporta una bozza di accordo di contitolarità:

Camera di Commercio di ….. con sede legale in …. (indirizzo, pec. etc.)

in persona del _____ *qualifica*_____, _____*nome*_____, che agisce in qualità di soggetto delegato ad acta dal Titolare del trattamento

e il **CONTRAENTE (CONTITOLARE)** _____, in persona del _____ *qualifica*_____, _____*nome*_____, che agisce in qualità di soggetto delegato ad acta dal Titolare del trattamento

d'ora in poi anche congiuntamente denominate le '**Parti**', ai sensi e per gli effetti dell'art. 4 n. 7 e dell'art. 26 del Regolamento UE 2016/679 , convengono e stipulano quanto segue:

Art. 1. Oggetto.

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'attività di cui trattasi comporterà il trattamento di dati _____ *qualificare le categorie di dati personali acquisiti* _____, relativi a _____ *qualificare le categorie di interessati* _____

Art. 2. Ripartizione delle responsabilità

Le Parti, come in effetti con il presente accordo pongono in essere, intendono trattare i dati acquisiti e gestiti, stante le medesime/correlate finalità e modalità del trattamento definite in sede progettuale, in regime di contitolarità, e per ragioni di sinergia, di condivisione delle strutture, delle risorse come di seguito delineato:

CAMERA DI COMMERCIO DI …….	CONTRAENTE (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

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 richiamare il contenuto essenziale del presente accordo che, se richiesto, sarà messo a disposizione degli interessati.

Art. 3. Dati

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.

Art. 4. Obblighi ed attività derivanti dalla contitolarità

Nello specifico i Contitolari assumono reciprocamente le seguenti responsabilità:

CAMERA DI COMMERCIO DI ……..	CONTRAENTE (CONTITOLARE)

Definire le responsabilità connesse ad es., al rilascio dell'informativa/acquisizione del consenso (se occorre previa condivisione tra le parti), all'adozione di specifiche misure di sicurezza, ai tempi di conservazione dei dati, alla possibilità di designazione di responsabili/sub-responsabili del trattamento (se occorre previa condivisione tra le parti)

Ai sensi dell' art. 26, par. 3 del Regolamento citato ed in relazione all'esercizio dei diritti degli interessati, questi potranno fare riferimento a ciascuno dei contitolari; al fine di agevolare tali soggetti, è definito quale punto unico di contatto: _____ *inserire contatti del punto unico di contatto, che risponderà agli interessati per conto delle due parti* _____ *(eventuale)* che dovrà essere esposto in tutte le informative rese all'esterno. In proposito, le Parti si impegnano comunque – ove la richiesta pervenga a soggetto diverso da quello cui compete l'attività di trattamento oggetto della richiesta stessa, secondo le responsabilità definite all'art. 2 – ad inoltrare immediatamente la richiesta al soggetto competente ed a supportarlo in tutto l'iter istruttorio della stessa.

In relazione all'adozione delle misure organizzativo-gestionali e tecniche (previste o meno nell'ambito del presente accordo) ed alla gestione di eventuali violazioni, le Parti convengono che:

a) ciascuna, per i dati nella propria diretta disponibilità, è responsabile dell'adozione di misure di sicurezza adeguate (art. 32 del GDPR);

b) ciascuna si impegna a gestire gli eventuali adempimenti connessi al data breach di cui agli artt. 33 e 34 del GDPR ove riguardino attività nella propria diretta responsabilità secondo quanto stabilito all'art. 2, previa opportuna comunicazione alle altre Parti ove la violazione e la successiva notifica possa comportare anche solo un danno reputazionale agli altri Soggetti coinvolti; in merito le parti si impegnano alla massima collaborazione al fine di mitigare gli eventuali impatti derivanti dalle violazioni sui diritti e libertà degli interessati.

Letto, approvato e sottoscritto tra le Parti.

RESPONSABILI DEL TRATTAMENTO

Vi 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.

In tali casi deve essere applicato lo schema di responsabilità ex art. 28 del GDPR: 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.

Nella previgente normativa era denominato responsabile esterno del trattamento, adesso il riferimento ad esterno è sparito dalla terminologia del GDPR. Al responsabile del trattamento 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 risponderà dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli art. 1218 e 1223 del Codice Civile[5].

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

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 2016/679 [6].

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. 196/2003 (artt. 167 e ss.) o dall'art. 24 bis del D.Lgs. 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. 196/2003 (cfr. artt. 161 e ss.) o successivamente dal GDPR (art. 83);
- 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[7]), in attesa di analoghi strumenti definiti ai sensi degli artt. 40 e ss. del GDPR;

---

5 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 è considerato titolare del trattamento in questione, con l'applicazione delle relative sanzioni.

6 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".

- ✓ 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. - Serie Generale 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 Regolamento UE.

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 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.

Gli stessi soggetti precedentemente identificati verificano che nel successivo contratto, convenzione o atto giuridico analogo[8] che comporti un trattamento di dati effettuato "per conto" dell'Ente Camerale, sia personalizzata ed inserita la seguente clausola contrattuale.

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

Posto che la realizzazione dell'attività di cui in premessa comporta il trattamento di dati personali relativi alle seguenti categorie di interessati _____ [9] in relazione ai quali la Camera di Commercio del Sud est Sicilia è Titolare del trattamento ai sensi dell'art. 4, n. 7 del Regolamento UE 2016/679 (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

7 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 in data 19.12.2018 e pubblicate ai sensi dell'art. 20, comma 4 , del D.Lgs. n. 101/2018 sulla G.U. n. 11 del 14.01.2019.

8 Ad es., lettera di accettazione dell'offerta, etc.

9 ATTENZIONE: Descrivere la tipologia dei dati personali oggetto di trattamento.

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. 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 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[10];
- 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.

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, par. 6-8, del GDPR.

Solo l'assunzione delle responsabilità ex art. 28 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[11] del GDPR.

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:

10 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).

11 "… 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*…".

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 2016/679)

La Camera di Commercio del Sud est Sicilia, in qualità di Titolare del trattamento, con riferimento al rapporto contrattuale in oggetto, al fine di adempiere agli obblighi formali e sostanziali proposti dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito anche Regolamento o GDPR), conferma che il contraente opererà quale responsabile esterno del trattamento dei dati ai sensi dell'art. 28 del GDPR per le fasi di sua competenza, così come definite nella scheda tecnica/offerta presentata.

Si specifica, in proposito, che 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, comma 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.

Con la sottoscrizione del presente atto, che costituisce condizione di efficacia ed esecutività del contratto citato in oggetto, il contraente – nella persona di _____ che agisce in qualità di _____ - accetta la suddetta nomina confermando la diretta ed approfondita conoscenza delle responsabilità che si assume e assicura sotto la propria responsabilità, di aver adempiuto o di adempiere, in funzione delle caratteristiche del trattamento affidato, alle istruzioni di seguito specificate; in proposito, la Camera di Commercio del Sud est Sicilia potrà a sua completa discrezione, ove ritenuto necessario, richiedere al contraente una dimostrazione documentale sull'osservanza delle disposizioni impartite ovvero procedere - direttamente o per il tramite di consulenti di propria fiducia - a verifiche ed audit anche presso la sede del contraente.

Istruzioni impartite

Il contraente si impegna espressamente:

- a comunicare prontamente al Referente contrattuale/Responsabile dell'esecuzione del contratto del Titolare eventuali situazioni sopravvenute (tra cui a puro titolo esemplificativo, sanzioni comminate dal Garante o da Autorità Giudiziarie ordinarie, anche non relative alle attività di trattamento oggetto del presente atto) che, per qualsiasi ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico;
- a non acquisire dati personali (ove così previsto contrattualmente) ulteriori rispetto a quelli strettamente necessari per l'esecuzione del servizio come definiti nel contratto di cui in oggetto, ed a non utilizzare i dati personali acquisiti per finalità proprie e/o diverse dalle attività contrattualmente definite, salvo specifiche e preventive istruzioni del Titolare;
- ad autorizzare a compiere operazioni di trattamento di cui al presente atto esclusivamente soggetti che oltre ad essere stati adeguatamente formati 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, delle condizioni di liceità del

trattamento e dei vincoli impartiti attraverso il presente atto;

- 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 dell'Ente Camerale, 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 all'Ente Camerale, 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 dall'Ente Camerale *[da personalizzare in funzione dell'autorizzazione generale/specifica che si vuole rilasciare]*
- a seguire le stesse modalità di cui al punto precedente per tutte le eventuali aggiunte o sostituzioni dei sub-contraenti;
- ad adottare procedure di controllo sull'attività svolta dai soggetti autorizzati o sub-responsabili precedentemente identificati, al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza gestionali e tecniche adottate, degli obblighi di riservatezza e, comunque, delle istruzioni impartite;
- a non comunicare comunque ad ulteriori soggetti terzi (soprattutto se sia possibile qualificare un trasferimento di dati verso paese terzo od organizzazione internazionale) i dati oggetto di trattamento, senza preventiva autorizzazione scritta dell'Ente Camerale;
- ad adottare tutte le misure di sicurezza tecnico-informatiche ed organizzativo-gestionali **dichiarate in fase contrattuale**, da intendersi come adeguate rispetto all'elencazione non tassativa di cui all'art. 32 del GDPR; 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 preesistente; in caso contrario, è fatto obbligo di condividere con il Referente contrattuale/Responsabile dell'esecuzione del contratto della Camera di Commercio, le nuove specifiche di trattamento, al fine di consentire la verifica del mantenimento dell'idoneità allo svolgimento dell'incarico;
- ad assistere l'Ente Camerale nel garantire, da parte di quest'ultimo, il rispetto degli obblighi di cui agli artt. 32-36 del GDPR (in particolare circa l'effettuazione della DPIA), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile esterno del trattamento;
- a conservare i dati personali oggetto di trattamento per tutto il periodo di tempo necessario per la realizzazione delle attività contrattualmente previste; alla scadenza del contratto ed a seguito del completamento del pagamento delle spettanze (il cui presupposto è la regolare esecuzione del contratto) ovvero all'atto della cessazione per qualsiasi causa dello stesso, il contraente dovrà provvedere a restituire all'Ente Camerale i dati personali in qualunque modalità e forma detenuti, provvedendo quindi a cancellarne ogni copia in proprio possesso e confermando l'avvenuta distruzione per iscritto al referente contrattuale del Titolare (salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini, ad es., contabili, fiscali, ecc.) *[da personalizzare in funzione dell'oggetto e delle caratteristiche della fornitura]*
- a provvedere - nel caso in cui l'attività affidata comporti l'acquisizione diretta di dati personali dagli interessati - al rilascio dell'informativa agli stessi soggetti contenente tutti gli elementi necessari ai sensi dell'art. 13 del Regolamento e ad acquisirne il consenso, ove necessario e con le modalità previste per la specifica attività; il format di documentazione da utilizzare dovrà essere fornito o concordato con la

Camera;

- ad informare immediatamente l'Ente Camerale in caso di richiesta di esercizio dei diritti di cui agli artt. 15 e ss. del Regolamento pervenuta direttamente al Contraente, ad es., nell'ambito dei contatti anche successivi al primo con gli interessati;
- a fornire all'Ente Camerale a semplice richiesta e secondo le modalità da esso indicate, i dati e le informazioni necessarie per:
    - ✓ verificare l'oggetto dei trattamenti affidati al Responsabile. Le valutazioni sulla legittimità del trattamento di tali dati, dell'eventuale comunicazione a terzi o diffusione degli stessi spettano al Titolare, congiuntamente ai relativi adempimenti, ivi comprese le informative ai propri dipendenti ed agli altri interessati inerenti al trattamento dei dati;
    - ✓ per dimostrare il rispetto degli obblighi di cui al presente atto di nomina, consentendo e contribuendo alle attività di revisione, comprese le ispezioni realizzate dal Titolare (o da un altro soggetto da questi incaricato);
    - ✓ una tempestiva difesa in eventuali procedure instaurate davanti all'Autorità Giudiziaria o al Garante o per effetto del trattamento dei dati in cui sia coinvolto l'affidatario;
    - ✓ dare tempestivo riscontro all'interessato, nei termini previsti dall'art. 12 del GDPR, che eserciti i diritti di cui al punto precedente direttamente nei confronti del Titolare;
- a comunicare al Referente contrattuale/Responsabile dell'esecuzione del contratto per la Camera, senza ingiustificato ritardo *[ovvero, per es. entro 24 ore]*, dopo l'avvenuta conoscenza di eventuali violazioni dei dati personali o presunte tali (a puro titolo esemplificativo: accessi abusivi, azione di malware, furto o smarrimento di computer o fascicoli cartacei, incendi o altre calamità...) che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse, al fine di consentire al Titolare – se del caso - l'adempimento degli obblighi di notificazione al Garante e di comunicazione agli interessati, come previsto dagli artt. 33 e 34 del Regolamento[12];
- prestare, in generale, la più ampia e completa collaborazione al Titolare e al suo Responsabile per la Protezione dei Dati (RPD ovvero DPO - Data Protection Officer), al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- in fase di rendicontazione periodica o finale delle attività svolte (sulla base di quanto previsto contrattualmente), a relazionare alla Camera sul buon esito delle attività di trattamento secondo gli standard precedentemente definiti;
- in generale, prestare la più ampia e completa collaborazione all'Ente Camerale ed al suo Responsabile per la Protezione dei Dati, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espleta-mento dell'incarico nel rispetto della normativa vigente.

Si fa presente che la violazione delle istruzioni comporta la corresponsione delle seguenti penalità …. [*se non sono definite nel contratto con riferimento al trattamento dei dati personali*]

La presente designazione è valida per tutto il periodo di durata degli accordi contrattuali e dei successivi eventuali rinnovi o affidamenti aventi lo stesso oggetto, salva richiesta di revisione di una delle parti che dovrà essere formalmente accettata da entrambe. È da ritenere revocata, con effetto immediato e senza obbligo di preavviso, in caso di recesso unilaterale o consensuale dall'incarico citato in premessa.

12 Si può stabilire, come indicato nell'esemplificazione riportata nel testo, una tempistica per gli obblighi di comunicazione. La procedura, qualora riguardi casi potenzialmente qualificabili come "data breach" (qualificazione – per inciso – che, ex art. 33 e 34 del GDPR, spetta al Titolare), deve essere coerenziata con quanto stabilito dalla Camera nell'apposito documento di gestione del Data breach.

Nel pregare di restituire alla scrivente una copia del presente allegato datato e firmato per accettazione, si inviano cordiali saluti.

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.

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[13] 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,

13 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.

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;
- ✓ 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.

ULTERIORI CASISTICHE

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**[14]**;**
b) responsabile esterno del trattamento ex 28 del GDPR[15];
c) soggetti autorizzati al trattamento (art. 29 del GDPR e art. 2 *quaterdecies*, comma 2 del D.Lgs. 196/2003[16], anche richiamando una precedente interpretazione del Garante per la Protezione dei dati personali[17] (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 al precedente paragrafo;
- 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

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 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).

---

14 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…

15 Il "responsabile del trattamento": la *persona fisica* o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, n. 8, del GDPR).

16 "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".

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

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 2016/679 (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.