Allegato n. 1

CAMERA DI COMMERCIO
DEL SUD EST SICILIA

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

Modello organizzativo, ruoli e sistema di responsabilità

ai sensi del Regolamento UE 2016/679

SOMMARIO

PREMESSA

SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è definire il modello organizzativo per la gestione degli adempimenti "sistemici" in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali, (di seguito Regolamento UE o GDPR), il D.Lgs. n. 196/2003, come modificato a seguito dell'entrata in vigore del D.Lgs. n. 101/2018 ed i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali (di seguito anche "Garante Privacy" o "Garante").
In particolare, il documento regolamenta:

a) i **ruoli e le responsabilità** assegnate ai vari livelli gestionali, di controllo ed operativi, al fine di garantire la corretta tenuta del predetto modello e, di conseguenza, la compliance alla normativa di riferimento;
b) le modalità per il rilascio delle necessarie **istruzioni** ai soggetti autorizzati, ai vari livelli, al trattamento dei dati personali;
c) gli strumenti per il **monitoraggio e controllo** del sistema, al fine di garantire il miglioramento continuo dello stesso ed il mantenimento della *compliance*;

Il presente documento è portato a conoscenza, anche attraverso attività di sensibilizzazione o formazione, a tutti i Dirigenti, funzionari o, comunque, referenti delle Aree/Servizi/Uffici della Camera di Commercio del Sud Est Sicilia

RIFERIMENTI NORMATIVI

Il presente documento risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37 e ss. del GDPR);
3. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
4. Attribuzione di funzioni e compiti a soggetti designati (art. 2-quaterdecies del D.Lgs. n. 196/2003);
5. Garante per la protezione dei dati personali, Comunicato 11 dicembre 1997 "Privacy: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche";
6. WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento";
7. Garante per la protezione dei dati personali, Provvedimento 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.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo per la protezione dei dati) – EDPB (European Data Protection Board)

RPD/DPO	Responsabile della Protezione dei Dati
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 Sud Est Sicilia

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La Camera di Commercio di Sud Est Sicilia è un ente pubblico dotato di autonomia funzionale che svolge, nell'ambito della circoscrizione territoriale di competenza, funzioni di interesse generale per il sistema delle imprese curandone lo sviluppo nell'ambito dell'economia locale. Le funzioni istituzionali sono definite dalla legislazione nazionale (a partire dalla legge n. 580/1993 e successive modificazioni), nonché da quella regionale (Legge regionale n. 4/2010).

Lo Statuto camerale, da ultimo, aggiornato il 16 gennaio 2018, elenca, all'art. 8, gli organi della Camera di Commercio che sono: 1) il Presidente; 2) il Consiglio; 3) la Giunta; 4) il collegio dei Revisori dei Conti.

La Struttura amministrativa è definita dallo Statuto e dalla deliberazione della Giunta camerale n. 16 dell'11 dicembre 2018 (in quanto ad articolazione delle funzioni e responsabilità ai vari livelli e in quanto alla strutturazione della stessa in Aree ed Uffici), nonché da appositi Ordini di servizio. Per l'identificazione della Struttura vigente nel tempo, si rinvia alla specifica sezione del sito istituzionale "Amministrazione trasparente"[1].

La ridefinizione dell'assetto delle responsabilità in materia di gestione dei dati personali si rende ora necessario:

a) per effetto delle modifiche apportate al sistema gestionale interno che, ai sensi del D.Lgs. n. 196/2003 prevedeva due figure: una opzionale, il responsabile del trattamento (art. 29), finora coincidente con il Segretario Generale e i Dirigenti; una obbligatoria, l'incaricato del trattamento (art. 30); in tal senso, il Regolamento UE esemplifica il quadro di riferimento, in quanto:
   - con il termine "responsabile del trattamento", l'art. 28 del GDPR, si riferisce esclusivamente a soggetti esterni all'organizzazione del Titolare, che operano sulla base di un contratto o atto giuridico analogo;
   - tutti gli ulteriori soggetti che abbiano accesso a dati personali, non possono trattarli se non previo rilascio di adeguate istruzioni (art. 30 del GDPR);

   Sul punto, il D.Lgs. 101/2018 di armonizzazione del quadro normativo interno al GDPR ha parzialmente abrogato e modificato il D.Lgs. 196/2003 prevedendo (art. 2-quaterdecies) la possibilità che:
   - specifici compiti e funzioni connessi al trattamento di dati personali possano essere attribuiti, nell'ambito dell'assetto organizzativo vigente, a persone fisiche, espressamente designate, che operano sotto l'autorità e responsabilità del Titolare del trattamento;
   - le persone che operano sotto l'autorità diretta del Titolare possano essere autorizzate al trattamento con le modalità ritenute più opportune dal Titolare stesso;

b) previsione di una nuova funzione, il Data Protection Officer (o Responsabile della Protezione dei Dati – RPD/DPO) che assomma le funzioni di cui all'art. 39 del GDPR (sostanzialmente, supporto al titolare del trattamento e verifica/controllo delle politiche implementate);

c) in ragione della complessità delle funzioni svolte e delle relazioni istituzionali con altri Organismi pubblici e Organizzazioni private, che comporta la revisione (anche in funzione dell'autonomia gestionale propria delle figure apicali ai vari livelli) e riallocazione delle responsabilità ai fini della più complessiva *compliance* al GDPR.

[1] In http://www.cz.camcom.it/content/amministrazione-trasparente

Per queste motivazioni, **per effetto dell'approvazione del presente modello organizzativo**, nell'ambito della più generale *governance* dell'Ente Camerale, è promossa un'articolazione **"a rete"** delle funzioni e competenze di gestione e controllo in materia di *privacy compliance*.

In tale contesto, i processi coordinati a livello centrale dal Titolare del trattamento coadiuvato dal Responsabile della Protezione dei Dati (RPD), trovano attuazione all'interno della Struttura organizzativa dell'Ente attraverso:

a) un livello dirigenziale, a cominciare dal Segretario Generale, con autonomia gestionale ed organizzativa, che riferisce direttamente al Titolare ("**Delegato del Titolare**"), ai cui si aggiungono gli altri Dirigenti e i Responsabili delle unità organizzative; a tali soggetti, da considerarsi designati ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003 per effetto della documentata preposizione alla direzione o alla responsabilità, sono affidati specifici compiti e funzioni connessi al trattamento dei dati personali di competenza successivamente delineati;
b) la nomina del **Responsabile della protezione dei dati**, con funzioni di supporto al Titolare del trattamento e di monitoraggio e controllo del sistema implementato;
c) i meccanismi e le modalità per **l'identificazione ed autorizzazione degli ulteriori soggetti** che, sotto la diretta autorità del Titolare e dei Delegati di cui alla precedente lett. a), effettuano i trattamenti di dati personali.

RUOLI E RESPONSABILITÀ

TITOLARE DEL TRATTAMENTO

L'interpretazione da sempre avallata dal Garante per la protezione dei dati personali prevede che il meccanismo di imputazione delle responsabilità in materia di privacy sia mutuato dallo schema organizzativo in concreto adottato dall'ente con riguardo alle potestà decisionali.

In linea con tale interpretazione e sulla base della lettura delle competenze istituzionali degli organi di vertice della Camera di Commercio e ferma restando la qualifica di *Titolare del trattamento* da **identificarsi nella struttura nel suo complesso e, quindi, in capo all'Ente Camerale medesimo,** le funzioni di natura gestionale che la legge attribuisce al *Titolare*, non possono che essere originariamente individuate in capo alla **Giunta Camerale** che è organo amministrativo e di indirizzo politico.

In tal senso, si ritiene che la Giunta, in materia debba determinare - considerando la natura, l'ambito di applicazione, il contesto, i rischi per i diritti e le libertà degli interessati - le finalità e le modalità del trattamento, assicurando che venga adottato un sistema di gestione degli adempimenti privacy ed adeguate misure (tecniche ed organizzative) di sicurezza, in conformità ai requisiti del Regolamento ed ai principi di accountability e di privacy by design & by default.

In considerazione di tali funzioni, la Giunta provvede:

a) a nominare il **Responsabile della Protezione dei Dati (RPD/DPO);**
b) ad approvare o delegare all'approvazione dei **principali documenti gestionali** per il regolare ed efficiente funzionamento del sistema privacy ovvero:
   - ✓ il presente modello organizzativo;
   - ✓ il registro dei trattamenti;
   - ✓ la procedura di gestione dei data breach;
   - ✓ gli altri documenti a carattere generale.
c) a conferire **espresso mandato** al Segretario generale dell'ente per la gestione dei vari adempimenti rilevanti, anche per rinvio alle funzioni previste dal presente modello;
d) ad adottare tutte le **decisioni** che eventualmente non rientrino nelle competenze ordinarie e nei limiti di spesa del segretario generale, ovvero conferite ai "delegati";
e) **a riesaminare ed aggiornare** periodicamente, avvalendosi del Responsabile della Protezione che riferisce direttamente al citato organismo, le misure a tutela degli interessati ai fini della *compliance* generale dell'Ente al GDPR.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Nel rispetto di quanto previsto dall'art. 37 del Reg. 2016/679, con deliberazione della Giunta Camerale n. 94 del 16 ottobre 2018, la Camera di commercio ha aderito al servizio di sistema "RPD Unioncamere" il quale prevede che le funzioni di responsabile della protezione dei dati per la Camera di Commercio sono svolte da Unioncamere attraverso un suo referente in possesso di un adeguato livello di conoscenza e delle competenze richieste dalla legge; il referente all'uopo individuato è il Dr. Marco Conte. L'incarico è stato ulteriormente prorogato per l'anno 2020 con deliberazione n. 108 del 19 dicembre 2019 e per l'anno 2021 con deliberazione n. 83 del 23 novembre 2020.

Il RPD costituisce una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali.
In particolare, all'RPD della Camera di Commercio di Sud Est Sicilia sono affidati i seguenti compiti:

a) supportare il Titolare del trattamento nel percorso di implementazione del GDPR a livello organizzativo-gestionale e tecnico-informatico, sia in fase di avvio (provvedendo a valutare la "consistenza" del registro dei trattamenti e dell'assessment formalizzato anche al fine di supportare la

definizione di eventuali misure idonee di cui sia indispensabile programmare l'implementazione), che per tutta la durata dell'incarico (esprimere formale parere sui documenti di carattere gestionale e sulle soluzioni tecnico-informatiche che verranno progettate per la compliance generale dell'Ente Camerale);

b) informare e consigliare il Titolare del trattamento, i dirigenti ed i dipendenti sugli obblighi derivanti dal GDPR e dalla normativa nazionale; in questo ambito, all'RPD potrà essere richiesto di partecipare ad incontri operativi ai vari livelli in cui vengano assunte decisioni relative al trattamento dei dati personali;
c) sorvegliare l'osservanza del GDPR e delle politiche interne in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale, anche attraverso la conduzione di audit e visite ispettive programmate e/o a sorpresa;
d) fornire se richiesto un parere sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del Regolamento, in particolare: sorvegliandone lo svolgimento, provvedendo ad esaminarne gli esiti finali e supportando le decisioni connesse agli obblighi di consultazione preventiva del Garante;
e) partecipare alle istruttorie e valutazioni circa eventuali violazioni di dati personali occorsi presso la Camera, supportando il Titolare nelle decisioni circa la gestione delle notificazioni dei data breach di cui agli artt. 33 e 34 del GDPR secondo quanto previsto nell'apposita procedura gestionale;
f) con riferimento al punto precedente, anche avvalendosi della propria struttura di supporto, provvedere alla alimentazione ed aggiornamento del "Registro dei data breach" – istituito e tenuto dall'Ente- come previsto da apposita procedura gestionale;
g) cooperare con il Garante italiano e con quello di eventuali paesi esteri con cui la Camera dovesse entrare in contatto, e fungere da punto di riferimento per facilitare l'accesso, da parte di questa, ai documenti ed alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal GDPR;
h) fungere da punto di contatto e curare i rapporti con gli interessati, coinvolgendo i dirigenti competenti *ratione materiae* nell'analisi ed evasione di ogni questione[2] che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento; in proposito si specifica che, pur nel caso in cui la richiesta di esercizio dei diritti sia sottoposta al RPD, la decisione sul riconoscimento o meno del diritto – e la relativa comunicazione all'interessato – spetta esclusivamente al Titolare
i) con riferimento al punto precedente, anche avvalendosi della propria struttura di supporto, provvedere alla istituzione, alimentazione ed aggiornamento del "Registro delle richieste di esercizio dei diritti degli interessati";
j) formalizzare periodiche relazioni al Titolare del trattamento contenenti la descrizione delle attività di supporto interno e di controllo effettuate, il resoconto relativo all'implementazione delle misure suggerite, nonché una valutazione generale e specifica sulla compliance dell'Ente Camerale al GDPR.

L'ambito d'intervento del RPD comprende tutti i trattamenti di dati personali posti in essere dalla Camera, compresa l'attività eventualmente delegata a soggetti esterni (persone fisiche e giuridiche), nonché quelli per i quali la Camera è stata nominata responsabile ex art. 28.

L'RPD riferirà direttamente alla governance del Titolare del trattamento a seconda delle circostanze e delle prerogative specifiche degli Organi (ad es., decisioni strategiche/operative ovvero caratterizzate da urgenza) anche sulla base della ripartizione dei compiti e delle responsabilità interne alla Camera specificamente definite nel prosieguo del presente documento.

Al fine di garantire i necessari requisiti di autonomia ed indipendenza nell'esecuzione dell'incarico, per effetto dell'approvazione del presente modello, al RPD sono attribuiti i seguenti poteri e prerogative:

a) **potere di autoregolamentazione**. Il RPD potrà programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle

[2] Ad.es., reclami, richieste di esercizio dei diritti di cui agli artt. 12 e ss del GDPR , richieste di riesame di eventuali risposte ottenute da altri referenti camerali.

attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione sistema privacy implementato rispetto agli obblighi di cui al GDPR; il RPD potrà farsi coadiuvare da personale appartenente alla propria Struttura organizzativa dotato di competenze specifiche nella materia, ferma restando la responsabilità finale dello stesso sugli atti ed indicazioni formalizzate;

b) **poteri ispettivi**: nell'esercizio delle proprie funzioni di controllo, il RPD potrà:
   - ✓ utilizzare le risultanze delle attività ispettive interne (ad es., verifiche di I livello dei "delegati del Titolare", audit del Sistema qualità certificato, audit tecnici su sistemi informativi, etc.) ovvero svolgere autonomamente verifiche anche a sorpresa;
   - ✓ accedere liberamente ad ogni documento rilevante per lo svolgimento delle sue funzioni;
   - ✓ disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
   - ✓ richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
   - ✓ esercitare i poteri, come precedentemente esplicitato, anche nei confronti delle società in house del sistema camerale, quando svolgano le funzioni di Responsabili esterni del trattamento (in questi casi, affiancando il dirigente competente).

Il RPD non potrà essere rimosso o penalizzato arbitrariamente a causa dell'esercizio delle proprie funzioni, non potendo inoltre assumere attività o compiti concorrenti che risultino in contrasto o conflitto di interesse.

Nell'esercizio dell'incarico, il RPD garantisce il vincolo di riservatezza sui dati e sulle informazioni acquisite, fermi restando gli obblighi connessi ad eventuali richieste formalizzate da Pubbliche autorità con funzioni inquirenti, giudicanti e di controllo.

I dati di contatto del RPD (recapito postale, telefono, email), comunicati al Garante per la protezione dei dati personali, sono resi disponibili. ad esclusione del suo nominativo, sul sito internet istituzionale della Camera di Commercio, riportati nelle informative rese agli interessati.

DELEGATI DEL TITOLARE DEL TRATTAMENTO

Ai seguenti soggetti, ai sensi dell'art. 2-quaterdecies, comma 1, del D.Lgs. n. 196/2003 ed in forza dei poteri statutari e delle deleghe gestionali conferite, è assegnata la gestione delle funzioni di seguito descritte.

IL SEGRETARIO GENERALE

Il **Segretario Generale**, in qualità di organo di vertice dell'amministrazione, sovrintende alla gestione complessiva ed all'attività amministrativa, esercita i poteri di coordinamento, verifica e controllo dell'attività dei dirigenti, vigila sull'efficienza e rendimento degli uffici e ne riferisce agli organi secondo le rispettive competenze. Adotta tutti gli atti di organizzazione riservati dalla legge all'ambito d'autonomia della dirigenza di vertice.

Coerentemente con le competenze statutarie, il Segretario Generale esercita le seguenti funzioni:

a) sottoscrizione degli **accordi di contitolarità,** su delega specifica e previa approvazione della Giunta Camerale;
b) aggiornamento e manutenzione, con propria determinazione, dei **documenti gestionali** approvati o delegati all'approvazione dalla Giunta Camerale in funzione delle modifiche normative ed organizzative eventualmente intervenute ed all'emergere di eventuali criticità o necessità di miglioramento gestionale;
c) predisposizione ed approvazione di eventuali **documenti operativi** (es., linee guida, procedure, istruzioni operative, format di informative e consensi, etc.) del sistema di gestione che si rendessero necessari per garantire la più efficace implementazione dei requisiti del GDPR;

d) **sottoscrizione delle notifiche dei data breach** ed approvazione delle comunicazioni agli interessati, secondo quanto previsto da apposita procedura gestionale;
e) gestione degli adempimenti derivanti dall'esercizio **dei diritti degli interessati** (artt. 15 e ss. del GDPR) e/o i **reclami** pervenuti direttamente alla Segreteria Generale ovvero relativi a processi o fasi di attività nella propria diretta competenza[3], provvedendo a far alimentare il "Registro delle richieste di esercizio dei diritti degli interessati"; fornisce supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;
f) **dotazione di misure di sicurezza di tipo tecnico-informatico** da applicarsi unitariamente alla Camera di Commercio, ovvero non rientranti nelle specifiche responsabilità e budget delle Aree Dirigenziali o nelle Unità organizzative;
g) approvazione (previa valutazione positiva dell'RPD) di **percorsi formativi e strumenti informativi periodici**, al fine di definire necessarie istruzioni ai dirigenti, ai funzionari, nonché ai soggetti che – agendo sotto l'autorità del Titolare - svolgono trattamenti nell'ambito delle Aree, Servizi ed Uffici dell'Ente Camerale;
h) definizione e sottoscrizione – ove rientrante nelle proprie nelle proprie competenze, deleghe e poteri di spesa – delle **clausole contrattali o atti giuridici analoghi** per il conferimento delle responsabilità del trattamento a soggetti esterni (art. 28);
i) gestione dei **flussi informativi** al RPD di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicazione **allo stesso di ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati.

Svolge infine per gli uffici e le funzioni di staff nella sua afferenza diretta, le funzioni di cui al par. successivo.

I RESPONSABILI DELLE AREE DIRIGENZIALI

Alla dirigenza spetta la gestione finanziaria, tecnica e amministrativa, mediante autonomi poteri di spesa, di organizzazione delle risorse umane e strumentali, nonché di controllo. La dirigenza è responsabile della gestione e dei relativi risultati.

In coerenza con le funzioni statutarie, ai Dirigenti sono delegate le seguenti funzioni:
a) **applicano -** nel contesto della specifica mission dell'Area di riferimento **- la normativa e le istruzioni** definite dal Titolare in collaborazione con il RPD attraverso i documenti gestionali del sistema privacy; i Dirigenti sono destinatari di ogni comunicazione concernente l'adozione da parte dell'Ente di atti di carattere generale (ad es., regolamenti, procedure, circolari, linee guida, provvedimenti...) in materia di privacy garantendone l'applicazione[4];
b) verificano le esigenze di integrazione od aggiornamento dei documenti gestionali predisposti, ad es., evidenziando al Segretario Generale ed al RPD le eventuali **necessità di modifica/integrazione del registro dei trattamenti** di cui all'art. 30 del Regolamento, in relazione – a puro titolo esemplificativo a:
   - esigenze derivanti da nuovi servizi/progetti diversi o nuovi rispetto a quelli attualmente censiti;
   - modifiche organizzative interne all'Area di competenza che comportino diverse modalità di gestione dei trattamenti di dati, anche ai fini dell'analisi dei rischi (ad es., acquisizione di applicativi informatici per la gestione di determinate attività rientranti nella propria autonomia gestionale);
c) rilevano e segnalano al Segretario Generale le eventuali e specifiche **esigenze formative o di approfondimento** da considerare ai fini della progettazione e programmazione dei percorsi formativi interni;

[3] Ove non ricadenti nella specifica responsabilità *ratione materiae* di un'area dirigenziale.

[4] Ad es., personalizzazione dei format e modelli per la gestione degli adempimenti in relazione alle necessità di volta in volta emergenti nell'ambito della propria attività.

d) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, **tutte le misure preventive e correttive**[5] **a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere** (rientranti nell'ambito delle funzioni e budget attribuite), rappresentando al Segretario Generale ed al RPD specifiche esigenze cui non possono far fronte ordinariamente;

e) garantiscono, in relazione alle necessità di volta in volta emergenti nell'ambito dei servizi di competenza, il rilascio del**l'informativa** di cui agli artt. 13 e 14 del GDPR e l'acquisizione del **consenso** dagli interessati (ove necessario);

f) effettuano, nell'ambito delle funzioni istruttorie connesse alla proposta dei relativi atti, l'istruttoria necessaria per la definizione degli **accordi di contitolarità** da sottoporre alla firma del Segretario generale;

g) in caso di **affidamento di servizi ed incarichi professionali mediante appalto, contratti di servizi o altre tipologie contrattuali che comportino il conferimento/trattamenti di dati affidati all'esterno**:
   - in qualità di **dirigente proponente** (ovvero in collaborazione con il) **responsabile unico del procedimento** provvedono:
     - alla individuazione degli elementi di esperienza ed affidabilità che costituiscono il presupposto per l'affidamento dell'incarico di trattamento[6];
     - alla definizione degli adempimenti gestionali e tecnici che devono essere garantiti dal fornitore, in ragione della tipologia di dati e dei trattamenti da eseguire sugli stessi, da prevedere nel contratto di servizi o in atto giuridico analogo quale parte delle obbligazioni negoziali e quindi di carattere cogente;
   - in qualità di (ovvero in collaborazione con il) **Responsabile/Direttore dell'esecuzione del contratto/Referente contrattuale**, verificano il rispetto delle regole definite contrattualmente;

h) istruiscono le **richieste di esercizio dei diritti** degli interessati (artt. 15 e ss. del GDPR) e/o i **reclami** pervenuti direttamente all'Area ovvero relativi a progetti, processi o fasi di attività nella propria competenza e provvedono a formalizzare le risposte (e ad alimentare il "Registro delle richieste di esercizio dei diritti degli interessati"); le propongono al SG ove rientranti nella sua diretta responsabilità; forniscono supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;

j) gestiscono – secondo quanto definito da apposita procedura gestionale - il coordinamento del processo di analisi, gestione e risposta alle violazioni di dati verificatesi in relazioni a processi, progetti, basi di dati rientranti nella propria specifica responsabilità o competenza; acquisiscono gli elementi informativi utili a valutare la necessità/obbligo di notifica dei **data breach** al Garante ed agli interessati, compresa l'alimentazione del "Registro dei Data breach", informando in ogni caso, con tempestività, il RPD;

i) garantiscono che la **diffusione** dei dati personali (diversi da quelli sensibili e giudiziari che risulta allo stato essere vietata) avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero solo se prevista da specifica normativa (ad es., con riferimento agli obblighi di pubblicazione per finalità di pubblicità integrativa dell'efficacia e di trasparenza (ai sensi del D.Lgs. 33/2013 e s.m.i.) per quanto di competenza;

j) si attivano - in collaborazione con il RPD - per fare in modo che, in relazione ad **ogni nuova iniziativa o progetto** che comporti un trattamento di dati personali, sia effettuata **una verifica preventiva della liceità e della legittimità del trattamento,** nonché delle modalità con le quali si intende eseguirlo; ove necessario, sulla base degli artt. 35 e 36 del Regolamento e delle Linee guida WP29 e del Garante, provvedono ad eseguire, in collaborazione con il RPD, la **valutazione d'impatto sulla protezione dei dati** e supportare il Presidente nell'attivazione della **consultazione preventiva** del Garante ove ritenuta necessaria;

---

[5] Connesse ad es., all'organizzazione interna del lavoro, alla gestione di eventuali fornitori e strumenti informatici, ai flussi informativi e documentali di competenza, etc.

[6] "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato", art. 28, par. 1, del GDPR.

k) gestiscono i **flussi informativi** al RPD di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicano **allo stesso di ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

In merito è da puntualizzare che, pur non essendo prevista espressamente dal Regolamento quale qualifica soggettiva, il D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018, ha lasciato ampia scelta al Titolare del trattamento nel definire le modalità ritenute più idonee per autorizzare al trattamento i soggetti che operano sotto la propria autorità diretta.

L'Ente Camerale, in merito ritiene di dover mantenere le modalità gestionali precedentemente utilizzare per la designazione degli "incaricati del trattamento"; quindi i soggetti che svolgono trattamenti "per conto" del Titolare sono **formalmente autorizzati:**

a) **"per relationem"** ove dipendenti, all'atto dell'assegnazione/allocazione (anche temporanea, con ordini di servizio successivi) in un centro di responsabilità (Area/Servizio/Ufficio) per il quale sia definito per iscritto l'ambito del trattamento (mediante rinvio al registro dei trattamenti ed alle istruzioni impartite);

b) per i **collaboratori esterni e consulenti/professionisti** (ove nel concreto operanti sotto l'autorità diretta del Titolare) mediante previsione di idonee clausole contrattuali in riferimento ai trattamenti oggetto dell'incarico stesso, contenenti le eventuali istruzioni specifiche necessarie per l'esecuzione delle attività previste.

Il personale autorizzato deve effettuare le operazioni di trattamento secondo le **istruzioni impartite dal Titolare anche per il tramite dei soggetti di cui ai paragrafi precedenti**, e rimane soggetto al potere di vigilanza e controllo di questi ultimi. Nello specifico, i soggetti autorizzati dovranno:

- ✓ garantire la massima **riservatezza** su qualsiasi informazione e dato personale di cui vengano a conoscenza nell'esercizio delle proprie funzioni, in conformità a quanto previsto normativamente in tema di **segreto d'ufficio** e di **segreto d'impresa**;
- ✓ fare riferimento alla specifica scheda analitica del registro dei trattamenti per l'individuazione **degli elementi fondamentali dei trattamenti** che si è autorizzati ad effettuare;
- ✓ seguire obbligatoriamente i **percorsi formativi** che saranno organizzati dall'Ente;
- ✓ rispettare le **disposizioni impartite per iscritto** dal Titolare o dal Delegato del Titolare competente attraverso la documentazione rilevante a fini privacy, nonché tutte le ulteriori istruzioni che possono essere formalizzate dai soggetti di cui ai par. precedenti;
- ✓ utilizzare le **misure di sicurezza** per la protezione fisica, informatica e telematica dei dati personali secondo le specifiche istruzioni definite nell'ambito del sistema di gestione privacy e dal Regolamento per l'utilizzo degli strumenti informatici e delle misure di sicurezza;
- ✓ **comunicare al RPD**, attraverso il Delegato, **ogni notizia rilevante** ai fini della protezione dei dati personali e degli interessati; qualora ne venga a conoscenza nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, **informare** tempestivamente (possibilmente entro il limite di 24 ore dal momento in cui si viene a conoscenza del fatto) **il RPD**, attraverso il Delegato/Referente privacy, del **verificarsi di eventuali violazioni dei dati personali** che possano esporre a rischio le libertà ed i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati **(data breach**);
- ✓ **collaborare più in generale con il RPD** provvedendo a fornire ogni informazione da questi richiesta.

Il soggetto autorizzato potrà fare riferimento direttamente al RPD per l'**esercizio dei diritti** che gli sono propri in qualità di interessato al trattamento dei propri dati personali (artt. 15 e ss. del GDPR).

AMMINISTRATORE DI SISTEMI

Il 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. definisce l'amministratore di sistema come la *«figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali».*

I soggetti che svolgono funzioni di amministrazione di sistemi (ad es., addetti alla gestione e manutenzione di un impianto di elaborazione o di sue componenti; amministratori di basi di dati; amministratori di reti e di apparati di sicurezza, amministratori di applicativi complessi):

- ✓ sono "responsabili" di specifiche fasi lavorative ovvero di strumenti che possono comportare elevate criticità rispetto alla protezione dei dati;
- ✓ pur non essendovi preposti istituzionalmente, possono anche "solo incidentalmente" trovarsi nella necessità di trattare dati personali ai soli fini dell'espletamento delle loro consuete attività.

Il Provvedimento del Garante definisce gli **adempimenti da formalizzare** sia in relazione ai dipendenti che svolgano tali funzioni sia nel caso di servizi affidati in outsourcing.

In attuazione di tale provvedimento, l'Ente Camerale ha, a suo tempo, proceduto alla designazione di InfoCamere, quale amministratore di sistema, i cui compiti, specificatamente e limitatamente a tale contesto, consistono in:

- assicurare la corretta custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in ambito camerale, anche impartendo apposite istruzioni agli incaricati del trattamento che utilizzino strumenti elettronici;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di *backup* e *disaster recovery*) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici, nella sua qualità di "amministratore di sistema"; tali registrazioni (access log) devono essere effettuate in modo da avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- relazionare, periodicamente, circa l'attività svolta e lo stato di attuazione delle politiche in tema di protezione dei dati personali, segnalando eventuali criticità.

FORMAZIONE ED INFORMAZIONE INTERNA

Nell'ottica di diffondere le conoscenze relative alla materia e di fornire adeguate istruzioni a tutto il personale della Camera di Commercio del Sud est Sicilia:

- tutta la documentazione relativa al Sistema di Gestione della Privacy è resa disponibile mediante condivisione in apposita cartella della intranet ovvero con forme equivalenti;
- il funzionamento del Sistema di Gestione è presentato e descritto a tutti i Delegati del Titolare in specifici incontri di condivisione, al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste;
- sono realizzati progetti formativi specifici:

  - per i dipendenti che dovranno coadiuvare i Delegati del Titolare per gli adempimenti di propria competenza, ferme restando le relative responsabilità in capo ai questi ultimi;
  - per il dipendente incaricato di svolgere la funzione di amministratore di sistemi;
- è prevista, nel primo periodo di implementazione del presente modello e secondo le esigenze rappresentate dai Delegati, la progettazione e realizzazione di percorsi formativi, anche in forma di e-learning, per tutti i soggetti autorizzati al trattamento.

Potranno inoltre essere pianificati ulteriori specifici percorsi od eventi secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali…), nei quali si terrà conto anche delle specifiche esigenze comunicate dai delegati del Titolare.

L'organizzazione di tali percorsi ed eventuali specifiche azioni formative
- ✓ saranno progettati e gestiti operativamente dal Dirigente dell'Ufficio Risorse Umane, in accordo con il Segretario Generale ed il RPD;
- ✓ saranno monitorate sia per quanto riguarda la realizzazione che gli esiti dal RPD.

I dipendenti e collaboratori dell'Ente Camerale potranno inoltre fare riferimento direttamente al RPD (attraverso la specifica casella di posta elettronica: rpd-privacy@cz.camcom.it) per la proposta di quesiti, la richiesta di approfondimenti, previa condivisione con la sua struttura di supporto. Resta invece diretta la possibilità di contattare l'RPD qualora la questione proposta attenga alla tutela dei propri dati personali.

Ulteriori attività di formazione/informazione saranno programmate al momento dell'assunzione di nuove risorse, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA

REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI

L'attuazione di un sistema di **monitoraggio, verifica e controllo** del sistema privacy implementato rispetto alla normativa ed alle direttive ed istruzioni impartite è una specifica responsabilità del Titolare del trattamento, rientrante negli obblighi di accountability di cui agli artt. 24[7] e 32 del GDPR[8].

Il sistema di monitoraggio, verifica e controllo poggia su due livelli distinti di intervento:
- ❖ controllo di I livello (c.d. "controllo di linea"), posto in essere dai dirigenti/Responsabili delle unità organizzative ("delegati del Titolare") nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di II livello (c.d. "controllo di compliance") affidato al RPD come descritto nell'apposito paragrafo del presente documento.

Gli specifici strumenti messi a disposizione di tali soggetti sono i seguenti:

a) **Registro dei Data Breach**: il registro consente la registrazione e tracciamento degli eventi (anche non sfociate in un incidente), degli incidenti e quasi-incidenti (situazioni anomale o incidenti di sicurezza) nonché dei veri e propri data breach, a prescindere se l'evento abbia dato luogo alla notifica al Garante e/o alla comunicazione agli interessati di cui agli artt. 33 e 34. Così configurato, il Registro consente di identificare e circoscrivere (per "tipologia di eventi" ovvero per asset/trattamento) gli

[7] "… il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

[8] "… il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso… d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

ambiti di criticità maggiormente impattanti - in termini organizzativi, operativi e di compliance - sull'organizzazione ed eventualmente sugli interessati, al fine di poter evidenziare i principali o più critici ambiti di intervento da gestire mediante azioni correttive;

b) **Registro delle richieste di esercizio dei diritti degli interessati**: anche in questo caso, oltre a costituire un fondamentale strumento documentale per tracciare e poter dimostrare la compliance sul punto, il Registro consente di individuare eventuali attività o modalità di trattamento considerate "critiche" dagli interessati.

La tenuta dei Registri, affidata al RPD, è gestita dalla sua struttura di supporto, e l'alimentazione degli stessi è regolamentata da apposite istruzioni/procedure del Sistema di Gestione dei Dati Personali e garantita dai seguenti flussi informativi.

I format dei Registri sono riportati in Allegato ai rispettivi documenti cui si riferiscono.

Ulteriori documenti e dati di input ai fini del monitoraggio e controllo del sistema privacy sono i seguenti:

- ✓ rendicontazioni periodiche e/o finali dei progetti/servizi affidati all'esterno, mediante specifica previsione contrattuale in capo al Responsabile esterno ex art. 28 del GDPR di relazionare sul buon esito delle attività di trattamento secondo le istruzioni impartite;
- ✓ relazioni periodiche circa l'andamento delle attività di competenza dell'amministratore di sistema;
- ✓ audit report e relazioni periodiche formalizzate dal RPD nel corso degli audit e verifiche di competenza;
- ✓ rilevazione dei dati e valorizzazione degli indicatori di anomalia di cui al paragrafo seguente e conseguente verifica dello scostamento rispetto ai valori obiettivo ivi definiti (da considerarsi quali "alert" ovvero indici di situazioni di rischio potenziale).

Per effetto dell'approvazione del presente documento sono istituiti i seguenti **flussi informativi in favore del RPD**:

PERIODICITÀ	DESCRIZIONE FLUSSO INFORMATIVO	RESPONSABILE FLUSSO
Tempestiva	Copia delle richieste di informazioni da parte di organi di Polizia Giudiziaria (ad es., Carabinieri, Polizia, Guardia di Finanza, etc.) o dal Garante e di tutti i verbali di accesso e di contestazione a seguito di ispezioni e controlli	Segretario Generale
Tempestiva	Sanzioni comminate da Pubbliche autorità in materia di privacy	Segretario Generale
Tempestiva	Copia relazioni / verbali redatti in sede di audit di I livello in cui si evidenzino criticità lato privacy	Delegati del Titolare
Quadrimestrale	Schede di rilevazione eventi (cfr. procedura data breach)	Delegati del Titolare
Quadrimestrale	Verbali di analisi degli incidenti (cfr. procedura di data breach)	Delegati del Titolare
Quadrimestrale	Risposte agli interessati in caso di reclami/esercizio diritti	Delegati del Titolare
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile esterno del trattamento	Delegati del Titolare

INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY

Il seguente sistema di indicatori è gestito dal RPD ed è alimentato mediante gli strumenti di registrazione ed i flussi di cui al par. precedente.

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
COMPLIANCE ALLA	Numero di richieste di esercizio dei diritti ex	> 5	Registro delle richieste di

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
NORMATIVA	artt. 15 e ss. del GDPR o di reclami pervenuti dagli interessati nell'anno Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati	> 3 ≤ 30 gg	esercizio dei diritti
	Numero di ispezioni subite da pubbliche autorità su segnalazione/denuncia degli interessati nell'anno	> 1	Flussi informativi al RPD
	Numero di sanzioni comminate in materia da pubbliche autorità nell'anno	> 0	
	Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento	> 2	
CONTROLLO E MIGLIORAMENTO CONTINUO	Numero di privacy audit effettuati nell'anno	≤ 1	Verbali/relazioni di audit/ Relazioni agli Organi
	% di Non Conformità (NC) riscontrate (n. NC / n. audit)	≥ 20%	
	Numero relazioni del RPD agli Organi	< 1	Relazioni agli Organi
SICUREZZA E DISPONIBILITÀ DEI DATI	Numero di segnalazioni di incidenti inserite nel Registro dei Data Breach	≥ 3/anno	Registro data breach
	Numero di violazioni di dati personali notificate al Garante Privacy ex art. 33 GDPR	> 1	
	Numero di data breach notificati al Garante oltre i termini previsti dal GDPR (72h)	> 1	
	Numero di violazioni di dati personali comunicate agli interessati ex art. 34 GDPR	> 1	
	Tempi medi di risoluzione incidenti e problematiche di sicurezza (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 7	Sistema ticketing interno / fornitori esterni
	Tempi medi di risoluzione incidenti bloccanti (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 2	

PRIVACY AUDIT

La realizzazione di verifiche ed audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite è funzione affidata - nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al RPD coadiuvato da una struttura di supporto costituita dai seguenti funzionari camerali:

- Dott. Vito D'Antona, Capo Area Supporto Interno;
- Ins. Giuseppe Giacalone, Provveditore;
- Dott.ssa Agata Inserra, Dirigente Ufficio Personale;
- Sig. Stefano Alì, Coordinatore informatico .

e attività di verifica sono di regola **programmate** e previamente **comunicate** ai soggetti coinvolti (salvo esigenze di audit a sorpresa) e sempre **condotte alla presenza** degli stessi.

Gli esiti delle verifiche, formalizzati in forma di **audit report,** sono:

- condivise con i soggetti auditi che possono formalizzare chiarimenti e/o controdeduzioni,
- completate – in caso di rilevazione di Non conformità (**NC) –** dalla proposta di **azioni correttive/preventive,**
- formalizzate – immediatamente ove evidenzino NC, ovvero nell'ambito delle relazioni periodiche – alla Giunta.

A seguito della conduzione degli audit, il RPD provvede ad alimentare gli indicatori di cui al paragrafo precedente.

RIESAME ED AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di compliance alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "testata regolarmente" (art. 32, par. 1, lett. d), del GDPR), il **Sistema di gestione della Privacy** delineato nel presente documento dovrà essere sottoposto a riesame, in occasione:

- dell'emanazione di nuove disposizioni normative, di pronunce giurisprudenziali, ovvero in relazione ad eventuali provvedimenti del Garante per la Protezione dei Dati di carattere cogente e/o interpretativo che abbiano un impatto sulla disciplina della protezione dei dati rilevante per l'Ente Camerale;
- di cambiamenti significativi della struttura organizzativa o dei settori di attività dell'Ente che comportino la ridefinizione della governance interna, degli organigrammi e delle relative attività e responsabilità;
- in occasione dell'introduzione di nuovi significativi strumenti di gestione, rilevanti rispetto al trattamento di dati personali;
- nel caso di applicazione di sanzioni da parte dell'Autorità giudiziaria ovvero del Garante nella materia di cui trattasi.

Il riesame è istruito preliminarmente dal RPD, il quale redigerà apposita relazione in merito tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo. La Relazione è poi trasmessa alla Giunta Camerale per l'assunzione delle eventuali decisioni necessarie a garantire la compliance ed il miglioramento continuo.