CAMERA DI COMMERCIO
BRINDISI-TARANTO

MODELLO ORGANIZZATIVO

INDIVIDUAZIONE DEI RUOLI *PRIVACY*

E DEL CONNESSO SISTEMA DI RESPONSABILITÀ

(approvato con delibera di Giunta n. 160 del 18/11/2024)

Il presente documento si inserisce nel
piano di *accountability* dell'Ente,
in linea con i principi di cui al
Regolamento (UE) 2016/679 – GDPR

SOMMARIO

PREMESSA

OBIETTIVI 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/Unità Operative della Camera di Commercio Brindisi-Taranto.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR / Regolamento	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice *privacy*	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29 / EDPB	Già Article 29 Working Party, Gruppo di lavoro *ex* art. 29, ora EDPB, European Data Protection Board
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Interessato	La persona fisica cui si riferiscono i dati personali
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 del GDPR)
DPO	Data Protection Officer / Responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR

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, ai sensi dell'art. 28 GDPR
Designato	Soggetto a cui, ai sensi dell'art. 2-*quaterdecies* del Codice *privacy*, l'Ente ha attribuito specifici poteri, oltre che compiti e funzioni, ai fini non solo dell'esecuzione di attività materiali di trattamento, ma anche e soprattutto per contribuire ad assicurare la *compliance* dell'Ente al GDPR.
SG	Segretario Generale della Camera di Commercio di Brindisi -Taranto

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Descrizione	Stato
24.09.2019	Bozza realizzata da Unioncamere nazionale	Distribuita alle Camere di Commercio
18/09/2024	Versione modificata, integrata ed adattata alla realtà della Camera di Commercio di Brindisi -Taranto	Avvio dei lavori di modifica, integrazione e adattamento
18/11/2024	Versione modificata, integrata ed adattata alla realtà della Camera di Commercio di Brindisi-Taranto	Adottata

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La Camera di Commercio di Brindisi -Taranto 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), nonché da quella regionale.

Lo Statuto camerale approvato, da ultimo, con delibera consiliare n. 13 del 24/04/2024., elenca, all'art. 9, gli organi della Camera di Commercio che sono: 1) il Consiglio; 2) la Giunta; 3) il Presidente 4) il Collegio dei revisori dei conti.

La Struttura amministrativa è definita dallo Statuto e dal Regolamento degli Uffici e dei Servizi (in quanto ad articolazione delle funzioni e responsabilità ai vari livelli), da appositi Ordini di servizio in quanto alla strutturazione della stessa in Aree e Unità Operative. Per l'identificazione della Struttura vigente nel tempo, si rinvia allo specifico Organigramma qui allegato [1].

La ridefinizione dell'assetto delle responsabilità in materia di gestione dei dati personali si rende ora necessario in ragione non solo delle modifiche normative apportate dal GDPR e dal D.Lgs. 101/2018, ma anche 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* alle disposizioni normativa in materia di trattamento dei dati personali.

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*.

[1] Allegato 1: Assetto Organizzativo adottato con Delibera Presidenziale d'urgenza n.4 del 29.2.2024, ratificata dalla Giunta con deliberazione n.6 del 12.4.2024.

RUOLI E RESPONSABILITÀ

LA CCIAA QUALE TITOLARE DEL TRATTAMENTO

Posto quanto sopra e tenuto altresì in considerazione l'orientamento costante del Garante per la protezione dei dati personali, viene individuata la CCIAA, nel suo complesso, quale – a seconda dei casi – Titolare, Contitolare o Responsabile del trattamento.

Con riferimento specifico ai casi di Titolarità del trattamento di dati personali, giova qui richiamare le precisazioni fornite dal Garante al Ministero delle finanze in data 9 dicembre 1997 [doc. web. n. 39785], mediante cui è stata richiamata l'attenzione sulla necessità di individuare in maniera corretta la figura del Titolare del trattamento con riguardo alle Pubbliche Amministrazioni.

In tale documento, il Garante ha precisato che i principi di cui alla l. 675/1996 – i medesimi ad oggi contenuti nel GDPR – impongono che qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il Titolare sia "*l'entità nel suo complesso (ad esempio, la società, il ministero, l´ente pubblico, l´associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all´esterno (ad esempio, l´amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)*". Tali persone fisiche "*potrebbero assumere, semmai,*" la qualifica – ad oggi – di Designati del trattamento (ciò in considerazione dell'abrogazione delle norme riferite ai "vecchi" responsabili interni e di cui *infra*).

La definizione di Titolare del trattamento, "*se interpretata in maniera diversa, e cioè ritenendo che la persona giuridica, la pubblica amministrazione o l'ente possano individuare al proprio interno una o più persone fisiche titolari del trattamento, renderebbe illogica la sequenza dei soggetti indicati nella norma medesima*". Ciò comporta che, rispetto all'individuazione del Titolare, la normativa in materia di protezione dei dati personali "*presuppone un approccio assai diverso da quello, ben noto, che deve essere seguito nell´applicazione della legge […] in materia di sicurezza e igiene del lavoro*".

Quanto alla formazione della "volontà" del Titolare, questa è formata "*tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo e dallo statuto*".

Nell'ambito di tale contesto di riferimento, la CCIAA di Brindisi-Taranto, ha individuato nella Giunta camerale e nel Segretario generale i soggetti a cui competono, ai sensi di legge, dell'Atto costitutivo e dello Statuto, la determinazione delle finalità e delle modalità di trattamento dei dati personali, nei limiti e nelle facoltà di cui alla normativa vigente.

Resta dunque in capo a tali Soggetti la responsabilità di determinare finalità e modalità del trattamento nel rispetto della vigente normativa nazionale ed europea in materia di trattamento dei dati personali, in particolare con riferimento ai principi di cui all'art. 5 GDPR e a quelli di *privacy by design* e di *privacy by default*, anche ai fini dell'adozione e della verifica dell'adeguatezza delle misure di sicurezza implementate.

Con riguardo alla suddivisione dei compiti derivanti dai poteri decisionali assegnati dalla legge, dallo Statuto e dell'Atto costitutivo ai diversi Organi, si precisa quanto segue:

a) scelta e nomina del DPO – Data Protection Officer (DPO – Responsabile della Protezione dei Dati) – di competenza della Giunta;

b) provvedere periodicamente alla consultazione del DPO per la verifica della compliance privacy da parte dell'Ente, nonché provvedere a coinvolgerlo tempestivamente ed adeguatamente in tutte le questioni riguardanti la protezione dei dati personali – di competenza della Giunta e del Segretario Generale;
c) approvazione, rivalutazione e/o verifica periodica dei principali documenti di accountability per il regolare ed efficiente funzionamento del sistema privacy, ovverosia:
   - ✓ il presente modello organizzativo di prima approvazione della Giunta e di rivalutazione periodica – di competenza del Segretario Generale;
   - ✓ il registro dei trattamenti (approvazione della prima versione e verifica almeno annuale degli aggiornamenti apportati) – di competenza del Segretario Generale.;
   - ✓ la procedura di gestione dei data breach (approvazione e rivalutazione della sua adeguatezza) – di competenza del Segretario Generale;
   - ✓ le nomine ai Responsabili del trattamento (approvazione e verifica) – di competenza del Segretario Generale.;
   - ✓ gli eventuali patti di contitolarità – di competenza del Segretario Generale;
   - ✓ le nomine ai Designati / Autorizzati al trattamento di dati personali (approvazione e verifica) – di competenza del Segretario Generale;
   - ✓ le nomine agli Amministratori di Sistema (approvazione e verifica) – di competenza del Segretario Generale.;
   - ✓ gli atti relativi all'organizzazione, anche logistica, degli Uffici camerali, aventi potenziali ripercussioni in ottica di privacy by design e by default (approvazione e verifica) – di competenza del Segretario Generale.;
   - ✓ le informative in materia di trattamento dei dati personali (verifica) – di competenza del Segretario Generale.;
   - ✓ i moduli per l'espressione dei consensi da parte degli interessati (verifica) – di competenza del Segretario Generale.;
   - ✓ le analisi preliminari (rispetto alle eventuali DPIA) del rischio privacy, al fine di determinare se vi è o potrebbe esservi un rischio elevato per gli interessati (verifica) – di competenza del Segretario Generale;
   - ✓ le valutazioni d'impatto privacy, ove necessario (approvazione e rivalutazione periodica) – di competenza del Segretario Generale.;
   - ✓ i regolamenti interni che hanno un impatto sul trattamento dei dati personali (verifica) – di competenza del Segretario Generale

DPO – DATA PROTECTION OFFICER

Nel rispetto di quanto previsto dall'art. 37 del GDPR, con provvedimento n.13, del 3/04/2024 di ratifica della deliberazione presidenziale d'urgenza n.11 del 04/03/2024, la Camera di Commercio di Brindisi-Taranto ha nominato, il proprio DPO, dipendente dell'Ente. La CCIAA ha provveduto in data 05/04/2024 a comunicare formalmente la nomina all'Autorità garante per la protezione dei dati personali. Tale DPO resta in carico sino a nuova determinazione. Prima di tale nuova determinazione, il DPO non sarà rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

I Il DPO è scelto e nominato dalla Giunta camerale sulla base di una attenta valutazione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. Il DPO può

essere un dipendente dell'Ente. In ogni caso, l'Ente si assicurerà che eventuali altri compiti e funzioni svolti dal DPO non possa dare adito a conflitti di interesse.

Il DPO viene periodicamente consultato per la verifica, in generale, della *compliance privacy* da parte dell'Ente, nonché viene tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il DPO riferisce direttamente al vertice gerarchico dell'Ente, e dunque alla Giunta camerale e al Segretario generale.

Tutti gli interessati, compresi i dipendenti della CCIAA, possono contattare direttamente il responsabile della protezione dei dati ai recapiti che seguono, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR:
email: dpo@brta.camcom.it
tel: 0831228239

Al DPO spettano i compiti di:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) esprimere formale parere su tutte le questioni privacy su cui viene interpellato, supportare l'Ente nella rivalutazione delle misure di sicurezza adeguate, fornire le valutazioni di verifica degli adempimenti individuati nell'elenco dei "*principali documenti di accountability*" di cui al paragrafo "La CCIAA quale Titolare del trattamento del presente modello organizzativo);
g) partecipare, se richiesto, ad incontri operativi ai vari livelli in cui vengono assunte decisioni relative al trattamento dei dati personali, al fine di fornire la propria opinione;
h) rendersi immediatamente disponibile, in caso di data breach, fornendo consulenza all'Ente per la valutazione circa la necessità di notificazione al Garante e agli Interessati, nonché fornendo supporto per la corretta predisposizione delle stesse e per la tenuta del registro dei data breach;
i) fungere da punto di contatto e curare i rapporti con gli interessati, coinvolgendo e supportando il vertice gerarchico dell'Ente e i singoli dirigenti competenti nell'analisi e nella gestione delle istanze che vengano sottoposte dagli Interessati, rivolgendosi questi ultimi all'Ente o direttamente al DPO, con riferimento ai diritti di cui agli artt. 12 e ss. del GDPR (in proposito si specifica che, anche nel caso in cui la richiesta di esercizio dei diritti sia sottoposta dall'Interessato direttamente al DPO, il riconoscimento o meno del diritto fatto valere spetta unicamente al Titolare del trattamento);
j) formalizzare periodiche relazioni, almeno semestrali, al vertice gerarchico dell'Ente, contenenti la descrizione delle attività di supporto interno e di controllo effettuate, il resoconto relativo all'implementazione delle misure suggerite, nonché una valutazione sia generale che specifica sulla *compliance* della CCIAA al GDPR.

L'ambito d'intervento del DPO 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.

Il DPO 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 DPO sono attribuiti i seguenti poteri e prerogative:

a) **potere di autoregolamentazione**. Il DPO potrà programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione sistema privacy implementato rispetto agli obblighi di cui al GDPR; il DPO 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 DPO 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;

Nell'esercizio dell'incarico, il DPO 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.

Sul DPO esterno ricade la **piena responsabilità contrattuale**, anche per l'eventuale danno d'immagine cagionato all'Ente, in ragione dell'attività da questi svolta, con particolare riferimento alla consulenza e al supporto prestati, nonché alla veridicità, completezza ed idoneità delle relazioni da questi presentate.

SOGGETTI DESIGNATI

Ai seguenti soggetti, ai sensi dell'art. 2-*quaterdecies* 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 e le indicazioni di cui al paragrafo "La CCIAA quale Titolare del Trattamento" lettera c) del presente modello organizzativo, il SG esercita, quindi, 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** 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[2], provvedendo a far alimentare il "Registro delle richieste di esercizio dei diritti degli interessati"; fornisce supporto al DPO 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 del DPO) 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 DPO 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 ed in loro assenza agli incaricati delle Elevate Qualificazioni 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 DPO 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[3];
b) verificano le esigenze di integrazione od aggiornamento dei documenti gestionali predisposti, curano l'aggiornamento, la revisione e l'**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);

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

[3] 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.

c) rilevano e segnalano al SG le eventuali e specifiche **esigenze formative o di approfondimento** da considerare ai fini della progettazione e programmazione dei percorsi formativi interni;
d) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, **tutte le misure preventive e correttive**[4] **a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere** (rientranti nell'ambito delle funzioni e budget attribuite), rappresentando al SG ed al DPO 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[5];
     - 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 DPO 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 DPO;
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 DPO - 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 DPO, la **valutazione d'impatto sulla protezione dei dati** e supportare il Presidente nell'attivazione della **consultazione preventiva** del Garante ove ritenuta necessaria;

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

[5] "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 DPO 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.

IL REFERENTE INTERNO PRIVACY

Il Referente interno privacy:

a) coordina le attività delle singole aree / uffici e servizi per l'adeguamento dell'Ente alla normativa in materia di protezione dei dati personali;

b) monitora costantemente secondo le modalità in seguito definite, l'applicazione e l'implementazione del sistema di gestione della privacy all'interno dell'Ente, segnalando al competente Dirigente e, se del caso, al SG, eventuali criticità riscontrate o necessità di adeguamento alla normativa;

c) rileva le esigenze di integrazione /modifica / aggiornamento dei documenti gestionali predisposti e le sottopone ai Dirigenti ed al SG (con particolare riferimento alla necessità di modifica/integrazione del registro dei trattamenti di cui all'art. 30 del Regolamento)

d) in caso di *data breach*, ha specifici compiti individuati nella apposita procedura di gestione *data breach*;

e) collabora con il Titolare e con il DPO per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;

f) offre supporto al DPO per l'espletamento dei propri compiti e funzioni come sopra delineati, garantendo la tempestività e la completezza dei flussi informativi;

l) gestisce i flussi informativi al DPO di propria competenza, come definiti nell'apposito paragrafo del presente documento, e più in generale comunica allo stesso ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati;

m) svolge in collaborazione con i Dirigenti coinvolti le valutazioni d'impatto secondo quanto previsto dagli artt. 35 e 36 del Regolamento e dalle indicazioni dell'EDPB e del Garante italiano.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

Con il termine "Autorizzati al trattamento" vengono ora individuati gli *ex* "Incaricati del trattamento"; ovverosia quei soggetti che svolgono materialmente i trattamenti all'interno dell'Ente.

La CCIAA ha provveduto ad autorizzare formalmente tutti i soggetti – non ricoprenti le qualifiche di cui sopra – che, nell'ambito dell'organizzazione camerale, in ragione del loro ruolo, mansioni, compiti, funzioni, trattano dati di carattere personale.

Gli ambiti di trattamento consentiti a tale personale sono stati definiti dalla Camera tramite rinvio alle rispettive Aree di competenza. Ciascun soggetto autorizzato può facilmente risalire alla propria Area di competenza) attraverso l'organigramma provvisorio di cui alla deliberazione di Giunta n. 6 del 03/04/2024 di ratifica della determinazione Presidenziale d'Urgenza n. 4 del 29/03/2024.

Le Aree di competenza rappresentano, pertanto, lo strumento con cui la CCIAA ha individuato e mantiene sempre aggiornati gli ambiti/settori rispetto ai quali detto personale è autorizzato al trattamento, e le istruzioni alle quali ciascuno deve attenersi, gestendo inoltre l'eventuale cambiamento delle mansioni e dei conseguenti ambiti di trattamento attribuiti.

A ciascun autorizzato è stata data la possibilità di trattare i dati personali nel rispetto e nei limiti delle attribuzioni assegnategli nonché delle ulteriori specifiche istruzioni che la CCIAA, in qualità di Titolare e/o di Responsabile, potrà di volta in volta impartirgli.

Ciascuna persona autorizzata al trattamento è obbligata a conoscere e a rispettare le procedure e le istruzioni tecniche che disciplinano le attività dell'Ente affidate alle Aree di competenza a cui appartiene, nonché a prendere parte attiva alla formazione obbligatoria erogata in materia di protezione dei dati personali.

Il personale autorizzato rimane soggetto al potere di vigilanza e controllo dei soggetti individuati nei paragrafi precedenti.

Tutti gli autorizzati sono inoltre soggetti ad obblighi di riservatezza circa qualunque informazione e dato personale di cui vengono a conoscenza nell'esercizio o in ragione delle loro funzioni. Sono inoltre tenuti a:

- ✔ attenersi a / mettere in atto tutte le misure di sicurezza definite dal Titolare per la protezione fisica, informatica e telematica dei dati personali;
- ✔ collaborare alla redazione, aggiornamento e integrazione dei contenuti del registro dei trattamenti, in base alle indicazioni del Titolare, dei dirigenti di riferimento e delle Elevate Qualificazioni;
- ✔ comunicare al loro Designato di riferimento ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati;
- ✔ informare tempestivamente il loro Designato di riferimento di ogni sospetto *data breach*;
- ✔ informare tempestivamente il loro Designato di riferimento di ogni istanza, presentata dagli Interessati, circa l'esercizio dei loro diritti in materia *privacy*;
- ✔ collaborare con il DPO provvedendo a fornire ogni informazione inerente la protezione dei dati personali da questi richiesta.

AMMINISTRATORI DI SISTEMA

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.

Circa le modalità di implementazione degli obblighi derivanti da tale Provvedimento, si rinvia al "Disciplinare interno tecnico dell'amministratore di sistema", oggetto di separata adozione.

In attuazione di detto Provvedimento, la Camera di Commercio Brindisi-Taranto ha altresì provveduto a nominare quale Responsabile del trattamento le seguenti Società:

-InfoCamere S.C.p.A.

-CSA Consorzio Servizi Avanzati

espressamente affidando loro servizi di amministrazione dei sistemi e, dunque, incaricandole di provvedere all'individuazione e alla nomina di persone fisiche dalle adeguate competenze, che ricoprano il ruolo di amministratore di sistema.

FORMAZIONE ED INFORMAZIONE INTERNA

Al fine di ottemperare alle previsioni di cui all'art. 29 GDPR secondo le quali chiunque agisce sotto la diretta autorità Titolare del trattamento e "*abbia accesso a dati personali non può trattare tali dati se non è*

istruito", nonché al fine di promuovere la diffusione della cultura della protezione dei dati personali, la CCIAA provvede a:

- rendere disponibile tutta la documentazione relativa al Sistema di Gestione della Privacy mediante condivisione in apposita cartella nella intranet camerale ovvero con forme equivalenti;
- realizzare, secondo le modalità di volta in volta ritenute più opportune, progetti /interventi formativi:
  - di carattere specialistico, organizzativo e normativo rivolti ai Dirigenti e il Referente Interno Privacy;
  - di carattere tecnico / normativo per i soggetti incaricati di svolgere la funzione di amministratore di sistemi;
  - di base per tutti i soggetti autorizzati al trattamento e volti a sensibilizzare il personale dipendente circa l'importanza della tutela dei dati personali, nonché ad illustrare le misure tecniche ed organizzative (procedure, *policy*, regolamenti interni, etc.) adottati dall'Ente in materia di tutela dei 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.

I dipendenti e collaboratori dell'Ente Camerale possono inoltre fare riferimento direttamente sia al Referente interno privacy che al DPO nominato.

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 e 32 del GDPR.

Il sistema di monitoraggio, verifica e controllo poggia su tre livelli distinti di intervento:

- ❖ controllo di I livello, ad opera dei Dirigenti/Responsabili delle unità organizzative nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di II livello svolto dal Referente interno Privacy nell'ambito della propria attività di monitoraggio continuo
- ❖ controllo di II livello (c.d. "controllo di compliance") affidato al DPO.

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

a) Registro dei Data Breach
b) Registro delle richieste di accesso dei diritti degli interessati
c) Registro degli Amministratori di Sistema
d) Registro delle attribuzioni di responsabilità a soggetti esterni
e) Registro attività di formazione e sensibilizzazione
f) Registro dei Trattamenti

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

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	Segretario Generale

	Garante e di tutti i verbali di accesso e di contestazione a seguito di ispezioni e controlli	
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
Tempestiva	Rilevazione incidenti di sicurezza (cfr. procedura data breach)	*Come da procedura*
Tempestiva	Richieste di esercizio dei propri diritti avanzate degli interessati, laddove richiedano espressamente un intervento del DPO	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 gestiti senza il coinvolgimento del DPO	Delegati del Titolare
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile del trattamento	Delegati del Titolare

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 Referente Interno Privacy e al DPO.

Le 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 auditati 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 DPO 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** dovrà essere sottoposto a riesame / aggiornamento, almeno 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.

La necessità di riesame è segnalata dai Dirigenti, dal Referente interno Privacy e dagli Incaricati delle Elevate Qualificazioni ed è valutata in collaborazione con il DPO. Ove l'esigenza comporti la revisione/modifica strutturale dei documenti gestionali di sistema la stessa sarà demandata alla decisione della Giunta Camerale per l'assunzione delle eventuali decisioni necessarie a garantire la compliance ed il miglioramento continuo.

In caso, invece, si tratti di mero aggiornamento dei documenti del Sistema di Gestione della Privacy, lo stesso potrà essere attuato dal Segretario Generale, sempre in collaborazione e previa consultazione del DPO.