Camera di Commercio
Cagliari - Oristano

Modello Organizzativo Privacy (MOP)

Ruoli e sistema di responsabilità, ai sensi del Regolamento UE 2016/679, art. 24

Approvato con deliberazione della Giunta camerale n. 45 del 23 marzo 2021

Camera di Commercio
Cagliari - Oristano

SOMMARIO

ACRONIMI E DEFINIZIONI UTILIZZATE…….. 3

PREMESSA.....**4**

- SCOPO E CAMPO DI APPLICAZIONE.....4

- RIFERIMENTI NORMATIVI.....4

CONTESTO ORGANIZZATIVO DI RIFERIMENTO.....**5**

RUOLI E RESPONSABILITÀ **6**

- TITOLARE DEL TRATTAMENTO.....6

- RESPONSABILE DELLA PROTEZIONE DEI DATI.....7

- DELEGATI DEL TITOLARE DEL TRATTAMENTO 10

- Il Segretario Generale 10

- I Dirigenti 12

- REFERENTI PRIVACY …….14

- SOGGETTI AUTORIZZATI AL TRATTAMENTO.....14

- AMMINISTRATORI DI SISTEMI 17

- RESPONSABILI DEL TRATTAMENTO ...……..……18

- FORNITORI - CONSULENTI - COLLABORATORI
INCARICATI A QUALSIASI TITOLO…….……..…22

FORMAZIONE ED INFORMAZIONE INTERNA **22**

STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA **23**

- REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI.....23

- INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY 24

- PRIVACY AUDIT 26

RIESAME DEL SISTEMA DI GESTIONE DELLA PRIVACY **26**

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"
Garante	Garante per la protezione dei dati personali
EDPB e WP29	Comitato europeo per la protezione dei dati (European Data Protection Board) che ha sostituito il Gruppo di lavoro ex art. 29 (Working Party article 29)
RPD/DPO	Responsabile della Protezione dei Dati
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate e il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della conformità al GDPR
Referente Privacy	Soggetto che supporta il RPD/DPO
SG	Segretario Generale della Camera di Commercio di Cagliari
PO	Posizione/i Organizzativa/e

PREMESSA

SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è definire il modello organizzativo per la gestione degli adempimenti in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali, il vigente D.Lgs. n. 196/2003, e i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali.
In particolare, il documento regolamenta:

a) i **ruoli e le responsabilità** assegnate ai vari livelli gestionali, di controllo e operativi, al fine di garantire la corretta tenuta del predetto modello e, di conseguenza, la conformità 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 e il mantenimento della conformità alla normativa vigente.

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/Strutture/Uffici della Camera di Commercio.

RIFERIMENTI 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. Linee Guida EDPB 7/2020 sui concetti di Titolare e Responsabile 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.

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La Struttura amministrativa della Camera di commercio di Cagliari-Oristano è definita dallo Statuto e dal Regolamento degli Uffici e dei Servizi, oltre che dagli atti di Macro e Micro Organizzazione assunti dalla Giunta, dal Segretario Generale e dai Dirigenti nell'ambito delle rispettive competenze.

La Struttura amministrativa della Camera è articolata nei seguenti livelli di responsabilità, primari, secondari, di base: Aree, Strutture/Servizi e Uffici.

Per l'identificazione della Struttura vigente nel tempo, si rinvia alla specifica sezione del sito istituzionale "Amministrazione trasparente – Organizzazione – Articolazione degli Uffici"

L'assetto delle responsabilità in materia di trattamento e gestione dei dati personali si conforma alla struttura propria della Camera di commercio di Cagliari-Oristano come risultante dal delineato sistema organizzativo interno.

Con il presente Regolamento è definito il contenuto specifico delle responsabilità in materia di trattamento e gestione dei dati personali ed è delineato, nell'ambito della più generale *governance* dell'Ente, il Modello Organizzativo Privacy (MOP), caratterizzato da una articolazione **"a rete"** di 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 e organizzativa, che riferisce direttamente al Titolare, e a cui si aggiungono gli altri Dirigenti; tali soggetti assumono il ruolo di **Delegati del Titolare o Delegati Privacy**, e sono da considerare soggetti designati ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003, per effetto della documentata preposizione alla direzione; agli stessi 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 (RPD/DPO)**, con funzioni di supporto al Titolare del trattamento e di monitoraggio e controllo del sistema implementato;
c. l'individuazione di uno o più **Referenti Privacy** che supportano il RPD nell'affrontare le questioni connesse alla sicurezza e alla gestione dei dati personali per la corretta applicazione del regolamento europeo, partecipando a tal fine agli appositi incontri periodici e riferendo direttamente ai vertici dirigenziali dell'Ente Camerale;
d. i meccanismi e le modalità per **l'identificazione e autorizzazione degli ulteriori soggetti responsabili**, che effettuano i trattamenti di dati personali, sotto la diretta autorità del Titolare e dei Delegati di cui alla precedente lett. a), come segue: i Responsabili delle unità organizzative, quali "Autorizzati Responsabili"; gli altri dipendenti, quali "Autorizzati"; entrambe le categorie;

A tali soggetti interni si aggiungono i Responsabili del Trattamento, soggetti esterni all'Amministrazione individuati dal Titolare con proprio provvedimento cui accede apposito contratto.

RUOLI E RESPONSABILITA'

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, a mente dello Statuto 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 e adeguate misure di sicurezza, in conformità ai requisiti del Regolamento e ai principi di accountability (affidabilità e responsabilizzazione) e di privacy by design & by default (adozione di misure tecniche e organizzative adeguate per la protezione - trattamento dati per impostazione predefinita).

In considerazione di tali funzioni, la Giunta provvede:

a) a nominare il Responsabile della Protezione dei Dati (RPD/DPO);
b) a nominare, anche mediante delega alla dirigenza, i Responsabili del Trattamento laddove ne ricorrano i presupposti;
c) ad approvare, anche mediante delega alla dirigenza, i 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.
d) a conferire espressa delega, considerandosi tale anche quanto attribuito con il presente MOP, al Segretario generale e ai Dirigenti, per la gestione dei vari adempimenti rilevanti, anche per rinvio alle funzioni previste dal presente atto;
e) ad adottare tutte le decisioni che eventualmente non rientrino nelle competenze ordinarie e nei limiti di spesa del Segretario generale, ovvero conferite ai "Delegati Privacy";
f) a riesaminare e aggiornare periodicamente, avvalendosi del Responsabile della Protezione che riferisce direttamente al Titolare, 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, il Responsabile della Protezione Dati è nominato dalla Giunta Camerale, anche tra i dipendenti camerali, e fino a diversa sua disposizione.

Il RPD è individuato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti di legge.

Il RPD costituisce presso la Camera di commercio di Cagliari-Oristano una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali.

Al RPD della Camera di Commercio di Cagliari-Oristano sono affidati i seguenti compiti:

a) supportare, informare e fornire consulenza al Titolare (in tutte le sue articolazioni) e ai Responsabili del Trattamento nel percorso di implementazione del GDPR a livello organizzativo e gestionale, nonché per l'applicazione delle adeguate misure di sicurezza per la corretta gestione dei dati personali e per la definizione di eventuali misure più idonee di cui sia indispensabile programmare l'implementazione;
b) sovraintendere alla tenuta del Registro dei Trattamenti di cui all'art. 30 del GDPR, coordinando, con la piena collaborazione dei Delegati, le attività di compilazione da parte dei soggetti Autorizzati Responsabili e Autorizzati, e consolidando il Registro - previa verifica del rispetto delle regole impartite dal Titolare - con la creazione di versioni consequenziali, ordinate cronologicamente;
c) esprimere, se richiesto, formale parere sui documenti di carattere gestionale (es., configurazione delle responsabilità interne, procedure, linee guida, istruzioni formalizzate ai soggetti autorizzati) e sulle adeguate misure di sicurezza che sono o verranno proposte per la gestione dei dati personali della Camera;
d) informare e fornire consulenza al Titolare (in tutte le sue articolazioni), ai Responsabili del Trattamento e ai dipendenti camerali sui loro obblighi derivanti dal GDPR e da altre vigenti disposizioni; in questo ambito, al RPD potrà essere richiesto di partecipare a incontri operativi ai vari livelli nell'ambito degli organi di governance della Camera in cui vengano assunte decisioni relative al trattamento dei dati personali;
e) sorvegliare e valutare l'osservanza del RGPD e le politiche interne in materia di protezione dei dati personali, compresi gli strumenti e le attività realizzate per la sensibilizzazione e la formazione del personale, anche attraverso la conduzione di audit e visite ispettive programmate e/o a sorpresa;
f) fornire, se richiesto, un parere sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del RGPD, in particolare: valutando le metodologie utilizzate, provvedendo a esaminarne gli esiti finali e supportando le decisioni connesse agli eventuali obblighi di consultazione preventiva del Garante della protezione dei dati personali;
g) partecipare alle istruttorie e valutazioni circa eventuali violazioni di dati personali occorsi presso la Camera, supportando il soggetto competente - secondo quanto previsto in appositi atti interni della Camera - nelle decisioni circa:

- la gestione delle notificazioni e comunicazioni dei data breach di cui agli artt. 33 e 34 del RPGD;
- la segnalazione di tali violazioni a eventuali Contitolari o Titolari autonomi, secondo le istruzioni contrattualmente definite;

h) provvedere alla alimentazione e aggiornamento del Registro dei data breach;
i) cooperare con il Garante per la protezione dei dati personali (o altra Autorità di controllo competente) e fungere da punto di contatto per facilitare l'accesso, da parte di questa, ai documenti e alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal RGPD;
j) fungere da punto di contatto e curare i rapporti con gli interessati, per il tramite e con la collaborazione diretta dei responsabili di Area/Ufficio/processo competenti, rispetto alla materia oggetto della questione con l'interessato, nell'analisi ed evasione di ogni questione che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento e alimentando il Registro delle richieste di esercizio dei diritti degli interessati;
k) fornire inoltre il suo apporto alla verifica della funzionalità del programma di formazione e istruzione funzionale del personale camerale rientrante nelle attività della Camera di commercio; se del caso potrà svolgere attività di formazione introduttiva al personale sulle principali tematiche del RGPD;
l) tenere l'elenco dei Responsabili del Trattamento;
m) provvedere alla istituzione, alimentazione e aggiornamento del Registro delle richieste di esercizio dei diritti degli interessati.

I compiti del Responsabile della Protezione dei Dati attengono all'insieme dei trattamenti di dati effettuati dalla Camera di commercio di Cagliari-Oristano e comprendono:

a. tutti i trattamenti di dati personali gestiti dalla Camera di commercio sia presso la sede centrale di Cagliari che presso la sede di Oristano ed eventuali altre sedi, compresa l'attività eventualmente delegata a soggetti esterni;
b. la vigilanza su eventuali trattamenti camerali svolti, su incarico della Camera di commercio, da Aziende speciali o Società in house del Sistema camerale e in tutti i casi di attribuzione di Responsabilità del trattamento.

Il RPD, in relazione all'esercizio delle proprie funzioni e dei relativi compiti è tenuto:

a) a stringenti vincoli di riservatezza nel trattamento dei dati personali/informazioni acquisite; tale vincolo non opererà in relazione agli obblighi connessi a eventuali richieste formalizzate da Pubbliche autorità con funzioni inquirenti, giudicanti e di controllo;
b) a comunicare immediatamente eventuali situazioni di conflitti d'interesse sopravvenuti ovvero l'insorgenza di una delle situazioni che costituiscono causa di decadenza dell'incarico;
c) ad adempiere ai compiti affidati con la diligenza richiesta dalla natura dell'incarico stesso, dalla natura dell'attività esercitata e dalle specifiche competenze detenute, garantendo un atteggiamento leale nello svolgimento del proprio ruolo ed evitando, con la propria azione o con la propria inerzia, di causare problematiche o criticità non riconducibili al rigoroso adempimento degli obblighi di supporto o vigilanza connessi al ruolo.

Il RPD riferirà direttamente al Titolare della Camera di commercio e al suo vertice gerarchico, e in particolare:

a. ordinariamente al Segretario generale, in qualità di vertice organizzativo dell'Ente e, quindi, in grado di intervenire tempestivamente in caso di criticità rilevate;
b. periodicamente alla Giunta camerale, mediante la formalizzazione della reportistica ovvero esprimendo le sue valutazioni quando lo riterrà opportuno o si renderà necessario, o quando gli verrà espressamente richiesto. Il RPD potrà essere convocato dalla Giunta, compatibilmente con le sue esigenze di servizio o personali, per riferire in merito al funzionamento del sistema di gestione dei dati personali o a situazioni specifiche.

Al fine di garantire i necessari requisiti di autonomia e indipendenza nell'esecuzione dell'incarico, per effetto dell'approvazione del presente modello, al RPD sono attribuiti i seguenti poteri e prerogative, in assenza di qualsivoglia istruzione (come stabilito dall'art. 38, comma 3, GDPR):

a) la Camera gli mette a disposizione, al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate, adeguate risorse economiche, strumentali e umane, con particolare riferimento a una idonea postazione di lavoro in grado di garantire la funzionalità delle attività e la riservatezza che deve caratterizzare il loro svolgimento, nonché la necessaria strumentazione informatica per la normale operatività in loco, e compreso uno o più "Referenti Privacy", con il compito di supporto giuridico-amministrativo del RPD nelle attività che esso dovrà svolgere, e un referente ICT (Tecnologie dell'informazione e della comunicazione) che dovrà supportare operativamente il RPD in tutte le attività di valutazione, analisi e indicazioni legate all'infrastruttura e agli applicativi informatici e telematici in uso presso la Camera, rendendo disponibile, a tal fine, il servizio di assistenza tecnica di InfoCamere;

b) la Camera non potrà rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni e garantisce che il RPD eserciterà le proprie funzioni in autonomia e indipendenza, non potendo assegnare allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

c) il RPD deve essere coinvolto, tempestivamente e adeguatamente, da parte della Camera, in tutte le questioni che riguardano la protezione dei dati personali sin dalle fasi iniziali, fornendo il quadro completo di tutte le informazioni pertinenti;

d) al RPD è garantita, da parte della governance e di tutto il personale, la dovuta considerazione, con particolare riferimento ai pareri e alle indicazioni fornite;

e) la Camera deve mettere a disposizione una specifica casella di posta elettronica che sarà utilizzata per tutte le comunicazioni ufficiali in ingresso e uscita, nonché quale dato di contatto per il Garante per la protezione dei dati personali e per gli interessati;

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

g) al RPD sono inoltre riconosciuti, per effetto del presente atto:

- potere di autoregolamentazione, in forza del quale il RPD 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 del sistema privacy implementato rispetto agli obblighi di cui al GDPR;

- poteri ispettivi, in forza dei quali, nell'esercizio delle proprie funzioni di controllo, il RPD potrà:

a) utilizzare le risultanze delle attività ispettive e svolgere autonomamente verifiche anche a sorpresa;
b) accedere liberamente a ogni documento rilevante per lo svolgimento delle sue funzioni;
c) disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
d) richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
e) 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).

DELEGATI DEL TITOLARE DEL TRATTAMENTO

Ai seguenti soggetti, ai sensi dell'art. 2-quaterdecies, comma 1, del D.Lgs. n. 196/2003 e 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 e 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 SG esercita, in materia di privacy, le seguenti funzioni delegate:

a) sottoscrizione degli accordi di contitolarità con enti e istituzioni minori (a titolo di esempio Istituti scolastici, Organismi di Mediazione e Arbitrato);
b) sottoscrizione degli accordi di contitolarità con le principali e strategiche Istituzioni e Autorità nazionali, regionali e comunali (come per esempio, Ministeri e Autorità Indipendenti, Regione, Provincia, Comuni di Cagliari e Oristano e loro Assessorati o Agenzie, Autorità Portuale), solo su delega espressa e specifica da parte della Giunta, e previa approvazione da parte della stessa anche del relativo accordo di contitolarità;

c) approvazione con propria determinazione del Registro dei Trattamenti con individuazione di apposite regole per la sua tenuta e per il suo periodico aggiornamento;
d) aggiornamento e manutenzione, con propria determinazione, dei documenti gestionali approvati dalla Giunta Camerale in funzione delle modifiche normative e organizzative eventualmente intervenute e all'emergere di eventuali criticità o necessità di miglioramento gestionale;
e) predisposizione e 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;
f) sottoscrizione delle notifiche dei data breach e approvazione delle comunicazioni agli interessati, secondo quanto previsto da apposita procedura gestionale;
g) garanzia che i dati personali oggetto del trattamento siano trattati in modo lecito e secondo correttezza, nel rispetto delle disposizioni contenute nel Regolamento (UE) 2016/679 e nei provvedimenti del Garante della Privacy applicabili nonché nel rispetto di eventuali istruzioni che saranno fornite dal Titolare: deve dare disposizione che i dati personali siano raccolti e registrati per scopi inerenti alle funzioni istituzionali dell'ente, che gli uffici verifichino che i dati siano esatti, completi, non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, e che siano conservati rispettando le misure di sicurezza predisposte dalla Camera;
h) attuazione delle misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza idoneo rispetto al rischio, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
i) indicazione della necessità di predisporre misure di sicurezza più efficaci o alternative rispetto alle pre-esistenti, non solo in caso di rilevante modifica normativa di settore;
j) gestione degli adempimenti derivanti dall'esercizio dei diritti degli interessati (artt. 15 e ss. del GDPR) e/o dai reclami pervenuti direttamente alla Segreteria Generale ovvero relativi a processi o fasi di attività ricadenti nella propria diretta competenza, attivandosi per alimentare il "Registro delle richieste di esercizio dei diritti degli interessati", e fornendo supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;
k) approvazione, sentito il 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;
l) controllo sull'attività svolta dalle persone autorizzate al trattamento al fine di verificare l'effettivo rispetto da parte di questi delle misure di sicurezza adottate e delle istruzioni impartite;
m) utilizzo delle informative;
n) supporto al Garante in caso di richiesta di informazioni o di controlli relativi alla protezione dei dati;
o) proposta in caso di cessazione del trattamento delle modalità di dismissione delle banche dati (distruzione- cessione – conservazione definitiva) secondo le formalità di legge;

p) affidamento incarichi di Responsabile del Trattamento dei dati e definizione e sottoscrizione delle clausole contrattali o atti giuridici analoghi per il conferimento delle relative responsabilità (art. 28);
q) accettazione di incarichi di Responsabile del Trattamento da parte della Camera, conferiti da parte di altri Titolari, laddove sia funzionale alla erogazione dei servizi all'utenza, e regolati da apposito atto;
r) istruzioni ai soggetti autorizzati sottoposti alla sua diretta responsabilità;
s) nomina degli Amministratori di Sistema;
t) gestione dei flussi informativi al RPD, 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.

I Dirigenti

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[1];
b) verificano le esigenze di integrazione o aggiornamento dei documenti gestionali predisposti, ad esempio, evidenziando al Segretario Generale e 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) collaborano con il RPD nelle attività di impulso volte ad alimentare il Registro dei Trattamenti, raccogliendo presso i servizi affidati alla propria responsabilità le informazioni a tal fine necessarie;
d) 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;
e) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, tutte le misure preventive e correttive[2] a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere (rientranti nell'ambito delle funzioni e budget attribuite),

[1] 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.
[2] Connesse ad es., all'organizzazione interna del lavoro, alla gestione di eventuali fornitori e strumenti informatici, ai flussi informativi e documentali di competenza, etc.

rappresentando al SG ed al RPD specifiche esigenze cui non possono far fronte ordinariamente;

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

g) 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, previa autorizzazione espressa della Giunta;

h) in caso di affidamento di servizi e 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 di responsabile unico del procedimento, o in collaborazione con questo, provvedono:
     - alla individuazione degli elementi di esperienza e affidabilità che costituiscono il presupposto per l'affidamento dell'incarico di trattamento[3];
     - 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;
     - all'affidamento al fornitore, se sussistono i presupposti, anche dell'incarico di Responsabile del Trattamento dei dati con definizione e sottoscrizione delle clausole contrattali o atti giuridici analoghi per il conferimento delle relative responsabilità (art. 28);
   - in qualità di Responsabile/Direttore dell'esecuzione del contratto/Referente contrattuale, (ovvero in collaborazione con questo) verificano il rispetto delle regole definite contrattualmente;

i) accettano incarichi di Responsabile del Trattamento da parte della Camera, conferiti da parte di altri Titolari, laddove sia funzionale alla erogazione dei servizi all'utenza di propria competenza, e regolati da apposito atto;

j) 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, oltre che ad attivarsi per alimentare il "Registro delle richieste di esercizio dei diritti degli interessati", o 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;

u) 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

[3] "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.

breach al Garante e agli interessati, compresa l'alimentazione del "Registro dei Data breach", informando in ogni caso, con tempestività, il RPD;

k) 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;
l) 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 europee e del Garante, provvedono a eseguire, in collaborazione con il RPD, la valutazione d'impatto sulla protezione dei dati e a supportare il Titolare nell'attivazione della consultazione preventiva del Garante ove ritenuta necessaria;
m) impartiscono istruzioni ai soggetti autorizzati sottoposti alla loro diretta responsabilità;
n) nominano gli Amministratori di Sistema dei settori posti sotto la loro diretta responsabilità;
o) 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.

REFERENTI PRIVACY

I Referenti privacy sono dipendenti della Camera di Commercio di Cagliari-Oristano, nominati dal Segretario Generale e individuati in funzione delle qualità professionali che permettano di prestare adeguato supporto giuridico-amministrativo al RPD nell'esecuzione dei suoi compiti.

Se possibile il Segretario Generale nomina un Referente per la sede centrale di Cagliari e uno per la sede di Oristano, con compiti di supporto al RPD nell'affrontare le questioni connesse alla sicurezza e alla gestione dei dati personali per la corretta applicazione del GDPR, partecipando, a tal fine, agli appositi incontri periodici e riferendo direttamente ai vertici dell'Ente Camerale.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

L'art. 4, punto 10, del Regolamento UE prevede espressamente la figura delle *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"*.

I soggetti autorizzati, ai sensi dei successivi articoli 29 e 32, comma 4, del Regolamento UE, non possono trattare i dati personali se non sono istruiti in tal senso dal Titolare del trattamento, atteso che le istruzioni rientrano tra le idonee misure che devono essere assunte per garantire un adeguato livello di sicurezza nella protezione dei dati.

Il D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018, inoltre, lascia 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.

Pertanto, i Delegati Privacy (dirigenti) autorizzano, con la stessa nota di incarico, i Responsabili delle unità organizzative, quali "Autorizzati Responsabili", al trattamento dei dati pertinenti al settore di responsabilità affidato, con assegnazione di specifiche istruzioni che devono avere come contenuto minimo quelle indicate nel presente Regolamento. I Responsabili hanno cura di consegnare a loro volta le predette istruzioni ai dipendenti incardinati negli uffici sottoposti alla loro responsabilità che si considerano, in automatico, in forza del presente Regolamento, e secondo gli ordini di servizio che dispongono la mobilità interna, soggetti "Autorizzati".

I soggetti così Autorizzati svolgono i trattamenti "per conto" del Titolare e sono formalmente autorizzati anche *per relationem* con rinvio al presente Regolamento e al Registro dei Trattamenti.

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

1) accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati facendo riferimento alla specifica scheda analitica del Registro dei Trattamenti per l'individuazione degli elementi fondamentali dei trattamenti che si è autorizzati a effettuare;
2) 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, non comunicandoli a terzi in alcun modo se non nei casi espressamente previsti, e non utilizzandoli per altri fini;
3) trattare i dati in modo lecito, corretto e trasparente, raccogliendoli per finalità legittime e trattandoli in modo che non vi sia incompatibilità con tali finalità, acquisendo solo dati adeguati, pertinenti e non ridondanti rispetto alle finalità, in attuazione del principio di minimizzazione dei dati, ed esatti e aggiornati, provvedendo a semplice richiesta, previa verifica, o d'ufficio, alla cancellazione o rettifica dei dati inesatti;
4) fornire all'interessato l'informativa secondo i modelli predisposti da ciascun ufficio competente, conservandone, ove ritenuto opportuno, copia controfirmata per ricevuta di avvenuta consegna;
5) conservare i dati personali raccolti per un periodo non superiore a quello indicato dal Titolare in base alla vigente normativa e provvedere periodicamente, a norma di legge, alla cancellazione dei dati personali per i quali non sussistono ragioni di fatto o di diritto che ne giustificano la conservazione;
6) custodire i dati personali raccolti con la massima diligenza, escludendo dall'accesso tutti coloro che non sono autorizzati, e tenendo, a tal fine, gli atti, i documenti e i supporti informatici contenenti dati personali in armadi muniti di serratura; qualora gli armadi in

dotazione all'ufficio non fossero disponibili o sufficienti informare per iscritto il diretto superiore;

7) valutare l'opportunità di tenere archivi separati per la conservazione di dati particolari;
8) riferire al responsabile di eventuali richieste di accesso ai documenti amministrativi che comportino la conoscenza di dati personali di terzi;
9) seguire obbligatoriamente i percorsi formativi che saranno organizzati dall'Ente;
10) 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 saranno dagli stessi soggetti formalizzate;
11) 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, con particolare riferimento al controllo e custodia degli atti e dei documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati da parte di terzi, compresi i dipendenti di altri uffici o servizi camerali; in particolare è doveroso:

- custodire con la massima diligenza le credenziali di autenticazione al fine di assicurarne la totale segretezza, potendole comunicare esclusivamente ad altro dipendente dello stesso ufficio per i soli casi di necessità, ossia solo se dalla omessa comunicazione potesse derivare una interruzione del servizio pubblico che l'Ente deve erogare, e avendo cura di modificarle prontamente una volta venuto meno lo stato di necessità;
- adottare password di almeno otto caratteri di cui almeno due numerici, senza riferimenti riconducibili agevolmente ai dati anagrafici propri o dei propri familiari, e modificarle almeno ogni sei mesi;
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- utilizzare esclusivamente software reso disponibile dall'ente;
- non collegare modem o dispositivi che consentano un accesso non controllato al computer o alla rete;
- non rimuovere il sistema antivirus installato sul computer;
- in caso di utilizzo di supporti removibili verificarne sempre preliminarmente l'integrità a mezzo del programma antivirus installato;
- non scaricare file eseguibili o documenti di testo da siti internet senza verificare l'assenza di virus;
- attivare una password di screensaver per evitare accessi non autorizzati al computer quando la postazione non è presidiata;
- non condividere il proprio hard disk con altro computer salvo ciò non sia richiesto da ragioni organizzative imposte per iscritto dall'amministrazione;

12) 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 e i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati (data breach);
13) collaborare più in generale con il RPD provvedendo a fornire ogni informazione da questi richiesta.

In aggiunta alle predette istruzioni, ai soggetti Autorizzati Responsabili sono assegnati compiti di controllo e monitoraggio sul rispetto da parte degli Autorizzati delle istruzioni ricevute e del dovere di riservatezza.

Le istruzioni sopra elencate sono quelle minime da rispettare. I soggetti Autorizzati Responsabili possono proporre ai Delegati l'adozione di ulteriori istruzioni in relazione agli specifici trattamenti curati dal servizio di competenza. I Delegati possono dunque integrare le istruzioni sopra elencate per le specifiche esigenze dell'Area di competenza.
Qualora si rendesse necessario derogare o modificare le istruzioni minime in parola, i Delegati dovranno darne apposita motivazione e puntuale giustificazione.

Il mancato rispetto delle istruzioni impartite a tutela della privacy potrebbe comportare l'insorgere di responsabilità della Camera con conseguente possibile contestazione disciplinare, in base al vigente CCNL, a carico del dipendente.

AMMINISTRATORI 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 procede alla nomina dei necessari Amministratori 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.

RESPONSABILI DEL TRATTAMENTO

A norma dell'art. 28 del Regolamento UE, la Camera di commercio di Cagliari-Oristano può incaricare, quali Responsabili del Trattamento, persone fisiche, enti e società che trattano i dati per suo conto.

Possono essere incaricati unicamente soggetti in possesso di requisiti di esperienza, capacità ed affidabilità tali da fornire idonea garanzia del rispetto delle disposizioni stabilite nel Regolamento UE, con particolare riferimento alla capacità di mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento garantisca la tutela dei dati personali di cui la Camera è Titolare.

L'incarico come Responsabile può essere disposto o direttamente dal Titolare, con deliberazione di Giunta camerale, o dal Delegato Segretario Generale, con propria determinazione, o dai Delegati, nell'ambito delle proprie Aree di competenza. In tal caso, il Delegato informa la Giunta camerale nella prima riunione successiva, al fine di consentire al Titolare l'esercizio della facoltà di opporsi, con applicazione dell'istituto del silenzio-assenso.

I trattamenti effettuati da un Responsabile sono disciplinati da un contratto/atto collegato al provvedimento amministrativo che vincoli il Responsabile stesso al Titolare del trattamento e

che definisca la materia disciplinata e la durata del trattamento, la natura e la finalità, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

L'atto di incarico dovrà contenere le seguenti indicazioni:

- il tipo di dati trattati;
- la natura e la finalità del trattamento;
- le categorie di interessati;
- la precisazione che le informazioni di dettaglio, relative a ciascun trattamento affidato dal Titolare al Responsabile, sono descritte nel proprio "Registro dei Trattamenti" informatico che costituisce parte integrante dell'atto di nomina e che sarà aggiornato dal Responsabile per le attività di propria competenza, consentendo eventuale visibilità al Titolare di tutte le informazioni necessarie affinché questo possa esercitare il controllo sui trattamenti affidati;
- la durata che deve essere pari al periodo per il quale i trattamenti dei dati sono affidati al Responsabile prescelto;

Lo stesso atto di incarico dovrà, inoltre, prevedere, quale contenuto minimo, le prescrizioni e gli obblighi appresso indicati:

1) effettuare il trattamento dei dati personali in modo lecito e secondo correttezza nel rispetto delle istruzioni del Titolare delle disposizioni contenute nel Regolamento UE 2016/679 e nei provvedimenti del Garante della Privacy;
2) impartire alle persone autorizzate al trattamento dei dati personali, dipendenti o collaboratori del Responsabile, il dovere, con rilevanza di obbligo legale, di riservatezza dei dati e del rispetto della normativa vigente e dei provvedimenti del Garante applicabili, e impartire, altresì, la necessaria formazione, comprensiva delle necessarie e opportune istruzioni;
3) adottare tutte le necessarie e appropriate misure di sicurezza tecniche e organizzative così come disciplinate dal Regolamento UE, tenendo conto del rischio per i diritti e le libertà delle persone fisiche, e mettere in atto le predette misure al fine di garantire un livello di sicurezza adeguato al rischio, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, al qual proposito, il Responsabile deve garantire, e il Titolare ne prenderà atto, di essere dotato di un proprio Sistema di gestione della sicurezza delle informazioni in costante aggiornamento in relazione allo stato del progresso tecnico;
4) provvedere, in particolare, ad attivare le seguenti misure minime di sicurezza:
   - effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema informatico usato;
   - per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati;
   - effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore;

- verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova;
- assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura;
- assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza;

5) comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico, nonché informare il Titolare qualora, a suo parere, un'istruzione violi disposizioni relative alla protezione dei dati;

6) attuare un controllo sull'attività svolta dalle persone autorizzate al trattamento al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate e, comunque, delle istruzioni impartite;

7) fornire al Titolare, a semplice richiesta e con le modalità indicate da quest'ultimo, tutti i dati e le informazioni oggetto dei trattamenti affidati al Responsabile, atteso che le valutazioni sulla legittimità del trattamento di tali dati, dell'eventuale comunicazione a terzi o diffusione degli stessi spettano al Titolare, congiuntamente ai relativi adempimenti, ivi comprese le informative ai propri dipendenti e agli altri interessati inerenti al trattamento dei dati;

8) trattare, se del caso, per conto del Titolare, con le modalità indicate da quest'ultimo, dati e informazioni necessari a effettuare comunicazioni a carattere informativo e promozionale nonché a svolgere indagini o ricerche di mercato, fermo restando che le valutazioni di legittimità sull'utilizzo dei dati ai fini delle predette comunicazioni nonché gli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali sono di competenza del Titolare;

9) cancellare e/o restituire, su scelta del Titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi a ciascun trattamento, fatto salvo il caso in cui si verifichino circostanze autonome che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate previamente concordate con il Titolare del trattamento;

10) assistere il Titolare, tenendo conto della natura del trattamento, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;

11) in caso di violazione di dati personali, informare il Titolare del trattamento senza ritardo - e comunque entro quarantotto ore dal momento in cui è venuta a conoscenza della violazione - e collaborare attivamente con il Titolare stesso, nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante Privacy e ai soggetti interessati, per quanto previsto nella normativa vigente;

12) assistere il Titolare del trattamento nel garantire il rispetto dei obblighi, previsti dal Regolamento, relativamente all'attuazione delle misure di sicurezza, alla comunicazione in caso di violazione dei dati personali e alla valutazione di impatto sulla protezione dei dati

tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

13) fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessari per consentire allo stesso di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria e relative al trattamento dei dati personali;

14) compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine;

15) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento e il rispetto degli obblighi di cui all'atto di nomina, consentendo e contribuendo alle attività di revisione, comprese le ispezioni realizzate dal Titolare (o da un altro soggetto da questi incaricato);

16) in generale, prestare la più ampia e completa collaborazione al Titolare e al suo Responsabile per la Protezione dei Dati (Data Protection Officer), al fine di compiere tutto quanto sia necessario e opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

17) relativamente a quanto prescritto dal Provvedimento del Garante del 27 novembre 2008 relativo alle *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, al Responsabile del trattamento sono attribuite le attività di valutazione, designazione, verifica attività e registrazione degli accessi degli amministratori di sistema e pertanto lo stesso ha l'obbligo di:
   - procedere alla designazione individuale degli amministratori di sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità, e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
   - riportare, per ciascun amministratore di sistema designato, o figura equivalente, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
   - conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema o figura equivalente;
   - verificare, con cadenza almeno annuale, l'operato degli amministratori di sistema o figure equivalenti in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza per il trattamento dei dati personali previste dalle norme vigenti;
   - adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema o figure equivalenti; le registrazioni dovranno essere conservate per un congruo periodo, comunque non inferiore a sei mesi.

Ogni specifico atto di incarico potrà prevedere prescrizioni aggiuntive in relazione alla specificità del trattamento effettuato dal Responsabile per conto della Camera.

Qualora si rendesse necessario derogare o modificare tali prescrizioni, l'atto di incarico deve contenere apposita motivazione e puntuale giustificazione.

I Responsabili del Trattamento come sopra nominati sono autorizzati in forza del presente Regolamento, a norma dell'art. 28, comma 2, del Regolamento UE a ricorrere, se necessario per l'espletamento delle forniture e dei compiti assegnati, a ulteriori eventuali Responsabili del trattamento per specifiche attività di trattamento trasferendo su di essi le disposizioni del Titolare e adottando opportune clausole contrattuali al fine di richiamare l'obbligo in capo ai medesimi di rispettare le misure di sicurezza descritte nell'atto di nomina. La nomina di ulteriori Responsabili deve essere comunicata al Titolare, ove richiesto.

FORNITORI – CONSULENTI – COLLABORATORI – INCARICATI A QUALSIASI TITOLO

Ai fornitori, consulenti, collaboratori e a qualsiasi altro soggetto incaricato dalla Camera a svolgere a suo favore una determinata prestazione che implica la possibilità anche occasionale di venire a conoscenza dei dati personali posti nella titolarità dell'ente, devono essere impartite, mediante idonee clausole contrattuali, le opportune istruzioni, con attribuzione della relativa responsabilità in riferimento agli eventuali trattamenti oggetto dell'incarico stesso.

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 di Cagliari-Oristano:

- 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 a questi ultimi;
  - per i dipendenti eventualmente incaricati di svolgere la funzione di amministratore di sistema;
- potranno inoltre essere pianificati ulteriori specifici percorsi o eventi secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali e altri), 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 Servizio competente in materia di personale, in accordo con il SG e 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) per la proposta di quesiti, la richiesta di approfondimenti, anche previa condivisione con la sua struttura di supporto. E' sempre 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 e alle direttive e istruzioni impartite è una specifica responsabilità del Titolare del trattamento, rientrante negli obblighi di accountability di cui agli artt. 24[4] e 32[5] del GDPR.

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

- ❖ controllo di primo livello (c.d. "controllo di linea"), posto in essere dai dirigenti ("Delegati del Titolare") coadiuvati dai responsabili delle unità organizzative ("Autorizzati Responsabili" nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di secondo 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 sfociati 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 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;

[4] "… 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".

[5] "… 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".

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, appositamente approvati dal Titolare, è affidata al RPD e gestita dalla sua struttura di supporto, mentre l'alimentazione degli stessi è garantita dai flussi informativi appresso regolati.

Ulteriori documenti e dati di input ai fini del monitoraggio e controllo del sistema privacy possono essere 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 degli amministratori 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 NORMATIVA	Numero di richieste di esercizio dei diritti ex artt. 15 e ss. del GDPR o di reclami pervenuti dagli interessati nell'anno	> 5	Registro delle richieste di esercizio dei diritti
	Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento	> 3	
	Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati	≤ 30 gg	
	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	

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
	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 e 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 dalla struttura di supporto.

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 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 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 con la collaborazione del RPD, il quale redigerà, ove richiesto, apposita relazione in merito, tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo. L'eventuale relazione del RPD è trasmessa alla Giunta Camerale per l'assunzione delle eventuali decisioni necessarie a garantire la compliance e il miglioramento continuo.