CAMERA DI COMMERCIO
REGGIO CALABRIA

Allegato 1 alla deliberazione della Giunta camerale n. 75 del 15/11/2021

Modello organizzativo, ruoli e sistema di responsabilità ai sensi del Regolamento UE 2016/679

SOMMARIO

PREMESSA

SCOPO E CAMPO DI APPLICAZIONE

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

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

Il presente documento è portato a conoscenza di tutto il personale della Camera di Commercio di Reggio Calabria

RIFERIMENTI NORMATIVI

Il presente documento risponde ai seguenti requisiti normativi:

a) Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
b) Responsabile della Protezione dei Dati (art. 37 e ss. del GDPR);
c) Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
d) Attribuzione di funzioni e compiti a soggetti designati (art. 2-quaterdecies del D. Lgs. n. 196/2003);
e) 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";
f) WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento";
g) Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D. Lgs. 101/2018
Garante	Garante per la protezione dei dati personali
RPD/DPO	Responsabile della Protezione dei Dati
Designato del Titolare	Soggetto che, secondo le deleghe/procure ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della compliance al GDPR

SG	Segretario Generale della Camera di commercio di Reggio Calabria
R.U.P.	Responsabile unico del procedimento

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La Camera di Commercio di Reggio Calabria 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.

Lo Statuto camerale approvato, da ultimo, con delibera consiliare n. 18 del 22/12/2020, elenca, all'art. 8, gli organi della Camera di Commercio che sono: 1) il Presidente; 2) il Consiglio; 3) la Giunta; 4) il Collegio dei Revisori dei Conti.

La Struttura amministrativa è definita dallo Statuto e dal Regolamento degli Uffici e dei Servizi (in quanto ad articolazione delle funzioni e responsabilità ai vari livelli), da apposite disposizioni e determinazioni del Segretario Generale in quanto alla strutturazione della stessa in Servizi ed Uffici. Per l'identificazione della Struttura vigente nel tempo, si rinvia alla specifica sezione del sito istituzionale "Amministrazione trasparente".

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

a) per effetto delle modifiche apportate al sistema gestionale interno che, ai sensi del D. Lgs. n. 196/2003 prevedeva due figure: una opzionale, il responsabile del trattamento (art. 29), finora coincidente con il Segretario Generale e i Dirigenti, ovvero i Responsabili delle Aree o delle unità organizzative; una obbligatoria, l'incaricato del trattamento (art. 30); in tal senso, il Regolamento UE esemplifica il quadro di riferimento, in quanto:

- con il termine "responsabile del trattamento", l'art. 28 del GDPR, si riferisce esclusivamente a soggetti esterni all'organizzazione del Titolare, che operano sulla base di un contratto o atto giuridico analogo;
- tutti gli ulteriori soggetti che abbiano accesso a dati personali, non possono trattarli se non previo rilascio di adeguate istruzioni (art. 29 del GDPR);

Sul punto, il D. Lgs. 101/2018 di armonizzazione del quadro normativo interno al GDPR ha parzialmente abrogato e modificato il D. Lgs. 196/2003 prevedendo (art. 2-quaterdecies) la possibilità che:

- specifici compiti e funzioni connessi al trattamento di dati personali possano essere attribuiti, nell'ambito dell'assetto organizzativo vigente, a persone fisiche designate che operano sotto l'autorità e responsabilità del Titolare del trattamento;
- le persone che operano sotto l'autorità diretta del Titolare possano essere autorizzate al trattamento con le modalità ritenute più opportune dal Titolare stesso;

b) previsione di una nuova funzione, il Data Protection Officer (o Responsabile della Protezione dei Dati – RPD/DPO) che assomma le funzioni di cui all'art. 39 del GDPR (sostanzialmente, supporto al Titolare del trattamento e verifica/controllo delle politiche implementate);
c) in ragione della complessità delle funzioni svolte e delle relazioni istituzionali con altri Organismi pubblici e Organizzazioni private, che comporta la revisione (anche in funzione dell'autonomia gestionale propria delle figure apicali ai vari livelli) e riallocazione delle responsabilità ai fini della più complessiva compliance al GDPR.

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.

RUOLI E RESPONSABILITÀ

TITOLARE DEL TRATTAMENTO

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

In linea con tale interpretazione e sulla base della lettura delle competenze istituzionali degli organi di vertice della Camera di Commercio - e ferma restando la qualifica di Titolare del trattamento da identificarsi nella struttura nel suo complesso e, quindi, in capo all'Ente Camerale medesimo - le funzioni di natura gestionale che la legge attribuisce al Titolare non possono che essere originariamente individuate in capo alla Giunta Camerale che, a mente dell'art. 23 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 ed adeguate misure (tecniche ed organizzative) di sicurezza, in conformità ai requisiti del Regolamento ed ai principi di accountability e di privacy by design & by default.

In considerazione di tali funzioni, la Giunta provvede:

a) a nominare il Responsabile della Protezione dei Dati (RPD/DPO);
b) ad approvare i principali documenti gestionali per il regolare ed efficiente funzionamento del sistema privacy ovvero:
   - ✔ il presente modello organizzativo;
   - ✔ la procedura di gestione dei data breach;
   - ✔ gli altri documenti a carattere generale.

c)a delegare, considerandosi tale quanto attribuito con il presente provvedimento, il SG ad approvare il registro dei trattamenti di cui all'art. 30 del GDPR;
d) alle designazioni per la gestione dei vari adempimenti rilevanti, anche per rinvio alle funzioni previste dal presente modello e può, inoltre, attribuire funzioni e compiti a soggetti designati che operano sotto l'autorità diretta del Titolare ex art. 2-quaterdecies del Codice;
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 o designati";
f) a monitorare le misure a tutela degli interessati ai fini della compliance generale dell'Ente al GDPR.

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Nel rispetto di quanto previsto dall'art. 37 del GDPR, la Camera di commercio ha provveduto alla nomina del Responsabile della protezione dei dati, con determinazione presidenziale n. 9 del 23/5/2018 ratificata dalla Giunta camerale con atto n. 28/2018. Il DPO costituisce una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali.

In particolare, al DPO della Camera di commercio di Reggio Calabria sono affidati i seguenti compiti:

a) supportare il Titolare del trattamento nel percorso di implementazione del GDPR a livello organizzativo-gestionale e tecnico-informatico, sia in fase di avvio (provvedendo a valutare la

"consistenza" del registro dei trattamenti e dell'assessment formalizzato anche al fine di supportare la definizione di eventuali misure idonee di cui sia indispensabile programmare l'implementazione), che per tutta la durata dell'incarico (in relazione ai documenti di carattere gestionale e soluzioni tecnico-informatiche che verranno progettate per la compliance generale dell'Ente Camerale);

b) informare sugli obblighi derivanti dal GDPR e dalla normativa nazionale;
c) sorvegliare l'osservanza del GDPR e delle politiche interne in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale, anche attraverso la conduzione di audit e visite ispettive programmate e/o a sorpresa;
d) fornire, se richiesto, un parere sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del GDPR, in particolare: sorvegliandone lo svolgimento, provvedendo ad esaminarne gli esiti finali e supportando le decisioni connesse agli obblighi di consultazione preventiva del Garante;
e) supportare il Titolare nelle decisioni circa la gestione delle notificazioni dei data breach di cui agli artt. 33 e 34 del GDPR secondo quanto previsto nell'apposita procedura gestionale;
f) con riferimento al punto precedente, sovrintendere alla alimentazione ed aggiornamento del "Registro dei data breach" , come previsto dall'apposita procedura gestionale;
g) cooperare con il Garante italiano e con quello di eventuali paesi esteri con cui la Camera dovesse entrare in contatto, e fungere da punto di riferimento per facilitare l'accesso, da parte di questa, ai documenti ed alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal GDPR;
h) fungere da punto di contatto e curare i rapporti con gli interessati, coinvolgendo i Responsabili dei Servizi ed i Responsabili degli Uffici e procedimenti competenti nell'analisi ed evasione di ogni questione[1] che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento;
i) con riferimento al punto precedente, sovrintendere all'aggiornamento del "Registro delle richieste di esercizio dei diritti degli interessati";

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 relaziona direttamente al Titolare del trattamento ai fini della ricognizione e valutazione generale sulla compliance dell'Ente Camerale al GDPR nell'ottica di un miglioramento continuo.
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 del sistema privacy implementato rispetto agli obblighi di cui al GDPR; il DPO potrà farsi coadiuvare da personale interno 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/designati 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;

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

- ✔richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
- ✔esercitare i poteri, come precedentemente esplicitato, anche nei confronti delle società in house del sistema camerale, quando svolgano le funzioni di Responsabili esterni del trattamento.

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.

I dati di contatto del DPO sono resi disponibili, ad esclusione del suo nominativo, sul sito internet istituzionale della Camera di commercio, riportati nelle informative rese agli interessati.

DESIGNATI DEL TITOLARE DEL TRATTAMENTO

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

IL SEGRETARIO GENERALE

Il Segretario Generale, in qualità di organo di vertice dell'amministrazione, sovrintende alla gestione finanziaria, tecnica e amministrativa mediante autonomi poteri di spesa, esercita i poteri di coordinamento, verifica e controllo dell'attività dei Responsabili dei Servizi, degli Uffici e dei procedimenti, 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 le seguenti funzioni:

a) sottoscrizione degli accordi di contitolarità, su delega specifica e previa approvazione della Giunta Camerale;
b) nomina, se necessario, dell'amministratore di sistema interno ed adozione del relativo disciplinare;
c) aggiornamento e manutenzione dei documenti/regolamenti gestionali approvati dalla Giunta Camerale in funzione delle modifiche normative ed organizzative eventualmente intervenute e/o all'emergere di eventuali criticità o necessità di miglioramento gestionale;
d) 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;
e) sottoscrizione delle notifiche dei data breach ed approvazione delle comunicazioni agli interessati, secondo quanto previsto dall'apposita procedura gestionale;
f) 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";
g) dotazione di misure di sicurezza di tipo tecnico-informatico da applicarsi alla Camera di commercio;
h) approvazione di percorsi formativi e strumenti informativi, al fine di definire necessarie istruzioni ai Responsabili dei Servizi, degli Uffici e dei procedimenti, al personale che svolge trattamenti nell'ambito delle unità organizzative dell'Ente Camerale;
i) definizione e sottoscrizione delle clausole contrattuali o atti giuridici analoghi per il conferimento delle responsabilità del trattamento a soggetti esterni (art. 28).

[2] Ove non ricadenti nella specifica responsabilità dei Responsabili dei Servizi/Uffici/procedimenti.

I RESPONSABILI DEI SERVIZI

La micro organizzazione dell'Ente prevede all'interno delle Aree l'individuazione di Servizi, articolati al loro interno, in Uffici in funzione delle competenze attribuite, nonché Unità di staff.

I Responsabili dei Servizi sono responsabili della gestione dei Servizi assegnati e dei relativi risultati, rispondendo al Segretario Generale. In coerenza con le funzioni statutarie e con il nuovo modello organizzativo, ai Responsabili dei Servizi, con il supporto dei Responsabili degli Uffici e procedimenti, sono assegnate le seguenti funzioni nell'ambito dei Servizi di competenza:

a) applicano la normativa e le istruzioni definite attraverso i documenti gestionali/regolamenti del sistema privacy; 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;
b) verificano le esigenze di integrazione od aggiornamento dei documenti gestionali predisposti e le eventuali necessità di modifica/integrazione del registro dei trattamenti di cui all'art. 30 del GDPR, 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'ambito di competenza del Servizio/Ufficio che comportino diverse modalità di gestione dei trattamenti di dati, anche ai fini dell'analisi dei rischi (ad es., acquisizione di applicativi informatici per la gestione di determinate attività rientranti nella propria autonomia gestionale);

c) rilevano e segnalano le eventuali e specifiche esigenze formative o di approfondimento da considerare ai fini della progettazione e programmazione dei percorsi formativi interni;
d) propongono, in caso di criticità e problematiche sopravvenute, le misure preventive e correttive[3] a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere;
e) garantiscono, in relazione alle necessità di volta in volta emergenti, il rilascio dell'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) istruiscono le richieste di esercizio dei diritti degli interessati (artt. 15 e ss. del GDPR) e/o i reclami pervenuti 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;
j) gestiscono – secondo quanto definito da apposita procedura gestionale - il coordinamento del processo di analisi, gestione e risposta alle violazioni di dati verificatesi; acquisiscono gli elementi informativi utili a valutare la necessità/obbligo di notifica dei data breach al Garante ed agli interessati;
h) garantiscono che la diffusione dei dati personali (diversi da quelli particolari 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.);
i) si attivano 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 dell'EDPB (ex WP29) e del Garante, provvedono a collaborare ai fini della valutazione d'impatto sulla protezione dei dati e supportare l'attivazione della consultazione preventiva del Garante ove ritenuta necessaria;
j) gestiscono i flussi informativi, come definiti nell'apposito paragrafo del presente documento, con riferimento ad ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati.

I responsabili delle Unità di staff, per le attività di competenza interessate dal sistema privacy, svolgono le funzioni di cui al presente paragrafo.

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

R.U.P.

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, i R.U.P. provvedono a:

- verificare gli elementi di esperienza ed affidabilità che costituiscono il presupposto per l'affidamento dell'incarico di trattamento[4];
- definire gli adempimenti 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;
- verificare il rispetto delle regole definite contrattualmente.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

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

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

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

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

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

- ✔ garantire la massima riservatezza su qualsiasi informazione e dato personale di cui vengano a conoscenza nell'esercizio delle proprie funzioni, in conformità a quanto previsto normativamente in tema di segreto d'ufficio e di segreto d'impresa;
- ✔ fare riferimento alla specifica scheda analitica del registro dei trattamenti per l'individuazione degli elementi fondamentali dei trattamenti che si è autorizzati ad effettuare;
- ✔ partecipare ai percorsi formativi che saranno organizzati dall'Ente;
- ✔ rispettare le disposizioni impartite dal Titolare o dal Delegato del Titolare competente attraverso la documentazione rilevante a fini privacy, nonché tutte le ulteriori istruzioni che possono essere formalizzate dai soggetti di cui ai paragrafi precedenti;

[4] "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.

- ✔ 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 Disciplinare per l'utilizzo degli strumenti informatici e delle misure di sicurezza;
- ✔ comunicare al DPO 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 DPO, del verificarsi di eventuali violazioni dei dati personali che possano esporre a rischio le libertà ed i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati (data breach);
- ✔ collaborare più in generale con il DPO provvedendo a fornire ogni informazione da questi richiesta.

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

AMMINISTRATORE DI 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 sistema (ad es., addetti alla gestione e manutenzione di un impianto di elaborazione o di sue componenti; amministratori di basi di dati; amministratori di reti e di apparati di sicurezza, amministratori di applicativi complessi):

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

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

In attuazione di tale provvedimento, l'Ente Camerale ha proceduto ad attribuire le funzioni di Amministratore di Sistema alla società InfoCamere s.c.p.a, società in house del sistema camerale e partecipata dalla Camera di Commercio di Reggio Calabria, i cui compiti, specificatamente e limitatamente a tale contesto, consistono nelle disposizioni indicate negli accordi contrattuali in essere.

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 Reggio Calabria – ed in generale a tutti i soggetti che a vario titolo siano chiamati ad effettuare trattamenti di dati personali per conto della Camera di commercio a valere su rapporti formalizzati (personale somministrato, dipendenti dell'Azienda speciale, etc.) e che si trovino ad utilizzare strutture ed infrastrutture di pertinenza dell'Ente - sono adottate le seguenti misure:

- tutta la documentazione relativa al Sistema di Gestione della Privacy è resa disponibile mediante condivisione in apposita cartella;
- il funzionamento del Sistema di Gestione è comunicato a tutti i Designati del Titolare al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste;

- sono realizzati, ove ritenuto necessario, progetti formativi specifici per tutti i soggetti autorizzati al trattamento.

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

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[5] e 32 del GDPR[6].

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

- ❖ controllo di I° livello (c.d. "controllo di linea"), posto in essere nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza, in ragione del ruolo e delle responsabilità, come descritte nel presente documento;
- ❖ controllo di II° livello (c.d. "controllo di compliance") affidato al DPO come descritto nell'apposito paragrafo del presente documento.

Gli specifici strumenti messi a disposizione sono i seguenti:

a) Registro dei Data Breach: il registro consente la registrazione e tracciamento degli eventi (anche non sfociate in un incidente), degli incidenti e quasi-incidenti (situazioni anomale o incidenti di sicurezza) nonché dei veri e propri data breach, a prescindere se l'evento abbia dato luogo alla notifica al Garante e/o alla comunicazione agli interessati di cui agli artt. 33 e 34. Così configurato, il Registro consente di identificare e circoscrivere (per "tipologia di eventi" ovvero per asset/trattamento) gli ambiti di criticità maggiormente impattanti - in termini organizzativi, operativi e di compliance - sull'organizzazione ed eventualmente sugli interessati, al fine di poter evidenziare i principali o più critici ambiti di intervento da gestire mediante azioni correttive;

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

La tenuta dei Registri e l'alimentazione degli stessi sono regolamentate da apposite istruzioni e procedure e garantite dai seguenti flussi informativi.

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

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

[5] "… 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".

[6] "… 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".

- ✔ audit report e relazioni periodiche formalizzate dal DPO 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 DPO da parte dei Designati del titolare del trattamento:

PERIODICITÀ	DESCRIZIONE FLUSSO INFORMATIVO
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
Tempestiva	Sanzioni comminate da Pubbliche autorità in materia di privacy
Tempestiva	Copia relazioni / verbali redatti in sede di audit di I° livello in cui si evidenzino criticità lato privacy
Quadrimestrale	Schede di rilevazione eventi (cfr. procedura data breach)
Quadrimestrale	Verbali di analisi degli incidenti (cfr. procedura di data breach)
Quadrimestrale	Risposte agli interessati in caso di reclami/esercizio diritti
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile del trattamento

INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY

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

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO (nell'anno)	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	> 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	> 1	Flussi informativi al DPO
	Numero di sanzioni comminate in materia da pubbliche autorità	> 0	
	Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento	> 2	
CONTROLLO E MIGLIORAMENTO CONTINUO	% di Non Conformità (NC) riscontrate (n. NC / n. audit) nelle privacy audit effettuate	≥ 20%	Verbali/relazioni di audit/ Relazioni agli Organi
SICUREZZA E	Numero di segnalazioni di incidenti inserite	≥ 3	Registro data breach

DISPONIBILITÀ DEI DATI	nel Registro dei Data Breach		
	Numero di violazioni di dati personali notificate al Garante Privacy ex art. 33 GDPR	> 1	
	Numero di data breach notificati al Garante oltre i termini previsti dal GDPR (72h)	> 1	
	Numero di violazioni di dati personali comunicate agli interessati ex art. 34 GDPR	> 1	
	Tempi medi di risoluzione incidenti e problematiche di sicurezza (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 7	Sistema ticketing interno / fornitori esterni
	Tempi medi di risoluzione incidenti bloccanti (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 2	

PRIVACY AUDIT

La realizzazione di verifiche ed audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite è funzione affidata - nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al DPO coadiuvato dai Responsabili dei Servizi, per quanto di rispettiva competenza.

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, sono alimentati gli indicatori di cui al paragrafo precedente.

RIESAME ED AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY

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

- dell'emanazione di nuove disposizioni normative, di pronunce giurisprudenziali, ovvero in relazione ad eventuali provvedimenti del Garante per la Protezione dei Dati di carattere cogente e/o interpretativo che abbiano un impatto sulla disciplina della protezione dei dati rilevante per l'Ente Camerale;
- di cambiamenti significativi della struttura organizzativa o aree 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.