Camera di Commercio
Pavia

MODELLO ORGANIZZATIVO

INDIVIDUAZIONE DEI RUOLI *PRIVACY* E DEL CONNESSO SISTEMA DI RESPONSABILITÀ;

DISCIPLINARE PER DESIGNATI E AUTORIZZATI

Approvato con Determinazione del Commissario Straordinario n. … del …..

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

SOMMARIO

PREMESSA

OBIETTIVI E CAMPO DI APPLICAZIONE

Si premette che la Camera di Commercio, Industria, Artigianato e Agricoltura di Pavia (di seguito, CCIAA di Pavia o CCIAA) pone da sempre particolare attenzione alla compliance privacy.
A seguito della piena operatività del Regolamento (UE) 2016/679), relativo alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati* - in vigore dal 24 maggio 2016 ed applicabile a partire dal 25 maggio 2018 –– di seguito Regolamento UE o GDPR – e a seguito della modifica del D.lgs. 196/2003 ad opera del D.lgs. 101/2018 entrato in vigore il 19/09/2018 la CCIAA, in sinergia con il sistema camerale lombardo (nell'ambito del gruppo di lavoro "privacy", poi compliance e di relativi progetti di sistema) e nazionale, ha ridisegnato il proprio modello organizzativo, sottoponendosi a un processo di assessment e di adeguamento (come da comunicazione del Presidente alla Giunta Camerale n. 3 del 19 dicembre 2018).

A partire dal 2018, dunque, la CCIAA si è dotata di nuovi strumenti:

- *DPO o RDP* (determinazione d'urgenza del Presidente n. 6 del 24 maggio 2018, ratificata dalla Giunta Camerale con deliberazione n. 41 del 04/06/2018 e successiva);
- predisposizione del *Registro Trattamento Dati Personali*, adozione e implementazione di *REGI*, software fornito gratuitamente da Infocamere al fine di automatizzare il Registro Trattamento Dati e consentirne una più efficiente validazione;
- *Organigramma Privacy (Modello Organizzativo)* e *Disciplinare degli Autorizzati al trattamento* (comunicazioni di servizio numeri 6 del 20.12.2018 e 1 del 5 agosto 2019 ai dipendenti dell'Ente – individuati dal Disciplinare stesso come tutti autorizzati al trattamento, secondo le competenze dell'Organigramma Privacy) – pubblicati sul sito istituzionale www.pv.camcom.it-Amministrazione Trasparente – Atti Generali;
- *procedura Data Breach*, relativo Flusso e Matrice Decisionale (Comunicazione di Servizio del Segretario Generale n. 1 del 5 agosto 2019);
- *Linee Guida per la gestione degli archivi cartacei* (n. 1 del 5 agosto 2019);
- *Procedura per l'esercizio dei diritti degli interessati* e *Registro dei diritti degli interessati* (n. 1 del 5 agosto 2019) - pubblicati sul sito istituzionale www.pv.camcom.it-Amministrazione Trasparente – Atti Generali;
- **nuovo modello di Informativa** da rendere agli interessati, diffusa presso tutti i responsabili. E' stato operato un primo adeguamento di tutte le informative dell'Ente alla normativa vigente ed è in corso un'ulteriore revisione delle medesime.

Scopo del presente documento è, dunque, quello di aggiornare il modello organizzativo per la gestione degli adempimenti "sistemici" in materia di protezione dei dati e degli interessati, avendo come riferimenti i citati GDPR e D.Lgs. n. 196/2003 (come modificato a seguito dell'entrata in vigore del D.Lgs. n. 101/2018) nonché i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali (di seguito anche "Garante Privacy" o "Garante"). Tale aggiornamento si rende necessario a seguito dell'evoluzione dell'organizzazione stessa.
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*;
d) i principi a cui Designati ed Autorizzati al trattamento dei dati personali debbono attenersi nell'organizzazione e/o nello svolgimento delle operazioni di trattamento loro affidate.

Nella logica dell'aggiornamento continuo e dell'accountability, dunque, il presente documento sostituisce i precedenti aventi le medesime finalità ("Organigramma Privacy" e "Disciplinare per gli autorizzati al trattamento" dei dati citati) ed è portato a conoscenza di tutti i dipendenti della CCIAA di Pavia. Come avvenuto nel tempo, si procederà anche ad opportune azioni formative.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR / Regolamento	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice *privacy*	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29 / EDPB	Già Article 29 Working Party, Gruppo di lavoro *ex* art. 29, ora EDPB, European Data Protection Board
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Interessato	La persona fisica cui si riferiscono i dati personali
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 del GDPR)
DPO	Data Protection Officer/Responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 28 GDPR
Autorizzato al trattamento	Persona fisica che (nell'organizzazione del Titolare/Responsabile) opera materialmente sui dati personali, svolgendo il trattamento sulla base delle indicazioni fornite dall'Ente di appartenenza e dai Designati, ove presenti
Designato al trattamento	Persona fisica (nell'organizzazione del Titolare/Responsabile) a cui, ai sensi dell'art. 2-*quaterdecies* del Codice *privacy*, l'Ente attribuisce specifici poteri, oltre che compiti e funzioni, ai fini non solo di dare esecuzione ad attività materiali di trattamento, ma anche e soprattutto di contribuire ad assicurare la *compliance* dell'Ente alla normativa in materia di *data protection*

SG	Segretario Generale Camera di Commercio, Industria, Artigianato e Agricoltura di Pavia

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Descrizione
_._._____	Prima versione (sostitutiva dei documenti "*Organigramma privacy*" e "*Disciplinare per gli autorizzati al trattamento dei dati*")

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La CCIAA di Pavia è un ente pubblico dotato di autonomia funzionale che svolge, nell'ambito della circoscrizione territoriale di competenza, funzioni di interesse generale per il sistema delle imprese curandone lo sviluppo nell'ambito dell'economia locale. Le funzioni istituzionali sono definite dalla legislazione nazionale (a partire dalla legge n. 580/1993) nonché da quella regionale.
Lo Statuto camerale approvato con deliberazione del Consiglio Camerale n. 2/2001 e modificato, da ultimo, deliberazione del Consiglio Camerale n. 20/2011, elenca, all'art. 7, gli organi della Camera di Commercio che sono: 1) il Presidente; 2) il Consiglio; 3) la Giunta; 4) il collegio dei Revisori dei Conti. Nell'attuale fase di riorganizzazione territoriale - caratterizzata dal processo di accorpamento con le consorelle di Mantova e Cremona – le funzioni degli organi politici sono svolte da un Commissario Straordinario, nominato con Decreto del Ministro dello Sviluppo Economico del 27.11.2020.
La struttura amministrativa è definita dallo Statuto, dal Regolamento degli Uffici e dei Servizi, da appositi Ordini e Comunicazioni di servizio. La Camera è strutturata in Aree, Servizi ed Uffici (centri di responsabilità primari e secondari). Per l'identificazione della Struttura vigente nel tempo, si rinvia all'**Organigramma camerale** pubblicato nella sezione "Amministrazione Trasparente-Organizzazione-Articolazione degli Uffici" sul sito istituzionale www.pv.camcom.it

Con l'approvazione del presente Modello Organizzativo e del relativo Organigramma Privacy, nell'ambito della più generale *governance* dell'Ente Camerale, è confermata e promossa un'articolazione "a rete" delle funzioni e competenze di gestione e controllo in materia di *privacy compliance*.

Nell'Allegato è riportato l'**Organigramma Privacy della CCIAA di Pavia**.

RUOLI E RESPONSABILITÀ

LA CCIAA QUALE TITOLARE DEL TRATTAMENTO

Posto quanto sopra e tenuto altresì in considerazione l'orientamento costante del Garante per la protezione dei dati personali, viene individuata la CCIAA, nel suo complesso, quale – a seconda dei casi – Titolare, Contitolare o Responsabile del trattamento.
Con riferimento specifico ai casi di **Titolarità del trattamento di dati personali**, giova qui richiamare le precisazioni fornite dal Garante al Ministero delle finanze in data 9 dicembre 1997 [doc. web. n. 39785], con cui è stata richiamata l'attenzione sulla necessità di individuare in maniera corretta la figura del Titolare del trattamento con riguardo alle Pubbliche Amministrazioni.
In tale documento, il Garante ha precisato che i principi di cui alla L. n. 675/1996 – i medesimi ad oggi contenuti nel GDPR – impongono che qualora il trattamento sia effettuato nell´ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il Titolare sia "*l'entità nel suo complesso (ad esempio, la società, il ministero, l´ente pubblico, l´associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all´esterno (ad esempio, l´amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)*". Tali persone fisiche "*potrebbero assumere, semmai,*" la qualifica – ad oggi – di Designati del trattamento (ciò in considerazione dell'abrogazione delle norme riferite ai "vecchi" responsabili interni e di cui *infra*).
La definizione di Titolare del trattamento, "*se interpretata in maniera diversa, e cioè ritenendo che la persona giuridica, la pubblica amministrazione o l'ente possano individuare al proprio interno una o più persone fisiche titolari del trattamento, renderebbe illogica la sequenza dei soggetti indicati nella norma medesima*". Ciò comporta che, rispetto all'individuazione del Titolare, la normativa in materia di protezione dei dati personali "*presuppone un approccio assai diverso da quello, ben noto, che deve essere seguito nell´applicazione della legge […] in materia di sicurezza e igiene del lavoro*".
Quanto alla formazione della "volontà" del Titolare, questa è formata "*tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo e dallo statuto*".
Nell'ambito di tale contesto di riferimento, la CCIAA di Pavia, individua nella Giunta Camerale (e nel suo Presidente) il Soggetto a cui compete, ai sensi di legge e dello Statuto, la determinazione delle finalità e delle modalità di trattamento dei dati personali, nei limiti e nelle facoltà di cui alla normativa vigente (tale funzione è oggi rappresentata dal Commissario Straordinario).
Resta dunque in capo a tale organo la responsabilità di determinare finalità e modalità del trattamento nel rispetto della vigente normativa nazionale ed europea in materia di trattamento dei dati personali, in particolare con riferimento ai principi di cui all'art. 5 GDPR e a quelli di *privacy by design* e di *privacy by default*, anche ai fini dell'adozione e della verifica dell'adeguatezza delle misure di sicurezza implementate.
In considerazione di tali funzioni, la Giunta camerale – con il supporto del Responsabile Privacy e del suo management- provvede agli adempimenti qui sotto elencati:

a) scelta e nomina del DPO – Data Protection Officer (RPD – Responsabile della Protezione dei Dati);
b) consultazione periodica del DPO per la verifica della *compliance* privacy dell'Ente;
c) approvazione, rivalutazione e/o verifica periodica dei principali documenti di accountability per il regolare ed efficiente funzionamento del sistema privacy, ovverosia:
   - ✓ il presente modello organizzativo (approvazione e rivalutazione periodica);
   - ✓ il registro dei trattamenti (approvazione e verifica almeno annuale degli aggiornamenti apportati);
   - ✓ la procedura di gestione dei *data breach* (approvazione e rivalutazione della sua adeguatezza);
   - ✓ le valutazioni d'impatto privacy, ove necessario (approvazione e rivalutazione periodica);
   - ✓ le nomine ai Responsabili del trattamento;
   - ✓ gli eventuali patti di contitolarità;
   - ✓ le designazioni e le autorizzazioni al trattamento di dati personali;
   - ✓ le nomine agli Amministratori di Sistema;

- ✓ gli atti relativi all'organizzazione, anche logistica, degli Uffici camerali, aventi potenziali ripercussioni in ottica di privacy by design e by default;
- ✓ lo schema di informativa che i designati dovranno utilizzare al fine di redigere le informative specifiche;
- ✓ i moduli per l'espressione dei consensi da parte degli interessati;
- ✓ le analisi preliminari (rispetto alle eventuali DPIA) del rischio privacy, al fine di determinare se vi è o potrebbe esservi un rischio elevato per gli interessati;
- ✓ i regolamenti interni che hanno un impatto sul trattamento dei dati personali.

Il Titolare può delegare alcuni atti al Responsabile Privacy (Segretario Generale).

DPO – DATA PROTECTION OFFICER

Il DPO viene scelto e nominato dalla Giunta camerale sulla base di una attenta valutazione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti di cui all'articolo 39 del GDPR. Il DPO può essere un dipendente dell'Ente. In ogni caso, l'Ente si assicurerà che eventuali altri compiti e funzioni svolti dal DPO non possa dare adito a conflitti di interesse.
Il DPO viene periodicamente consultato per la verifica, in generale, della *compliance privacy* da parte dell'Ente.
Il DPO riferisce direttamente al vertice gerarchico dell'Ente e, dunque, alla Giunta.

Al DPO spettano i compiti individuati dall'art. 39 GDPR.
L'ambito d'intervento del DPO comprende tutti i trattamenti di dati personali posti in essere dalla Camera, compresa l'attività eventualmente delegata a soggetti esterni (persone fisiche e giuridiche), nonché quelli per i quali la Camera è stata nominata responsabile ai sensi dell'art. 28 GDPR.
Il DPO riferirà direttamente alla *governance* del Titolare del trattamento a seconda delle circostanze e delle prerogative specifiche degli Organi (ad es., decisioni strategiche/operative ovvero caratterizzate da urgenza) anche sulla base della ripartizione dei compiti e delle responsabilità interne alla Camera specificamente definite nel prosieguo del presente documento.

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

a) **potere di autoregolamentazione**. Il DPO potrà programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione sistema privacy implementato rispetto agli obblighi di cui al GDPR; il DPO potrà farsi coadiuvare da personale appartenente alla propria Struttura organizzativa dotato di competenze specifiche nella materia, ferma restando la responsabilità finale dello stesso sugli atti ed indicazioni formalizzate;

b) **poteri ispettivi**: nell'esercizio delle proprie funzioni di controllo, il DPO potrà:
- ✓ utilizzare le risultanze delle attività ispettive interne (ad es., verifiche di I livello dei "delegati del Titolare", audit del Sistema qualità certificato, audit tecnici su sistemi informativi, etc.) ovvero svolgere autonomamente verifiche, anche a sorpresa;
- ✓ accedere liberamente ad ogni documento rilevante per lo svolgimento delle sue funzioni;
- ✓ disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
- ✓ richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
- ✓ Nel rispetto di quanto previsto dall'art. 37 del GDPR, con deliberazione della Giunta Camerale n. 12, del 25.02.2019, la Camera di Commercio ha nominato, quale proprio DPO, l'Avvocato Franco Pozzoli, funzionario di Unioncamere Lombardia. La CCIAA ha provveduto in data 20 marzo 2019

(prot. CCIAA n. 4904 del 20.03.2019) a comunicare formalmente la nomina al Garante per la protezione dei dati personali.

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

Con riferimento agli obblighi gravanti sull'Ente di mettere a disposizione del DPO le risorse a questo necessarie per l'assolvimento dei propri compiti, la CCIAA prevede che il DPO possa avvalersi della collaborazione del Referente Privacy per le sue attività, senza pregiudizio della sua indipendenza (ad esempio per reperimento documentazione e informazioni, organizzazione audit e incontri con la struttura et similia).

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.

SOGGETTI DESIGNATI

Ai seguenti soggetti, ai sensi dell'art. 2-*quaterdecies* del D.Lgs. n. 196/2003 ed in forza dei poteri statutari e delle deleghe gestionali conferite, è assegnata la gestione delle funzioni di seguito descritte.
Ciascun Designato ha, in generale, il compito e la responsabilità di adempiere a tutto quanto necessario per garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza nel trattamento dei dati personali, osservando scrupolosamente le istruzioni e le indicazioni impartite dalla Giunta Camerale.
I soggetti designati redigono le Informative relative alle rispettive aree di competenza – secondo lo schema approvato dalla Giunta Camerale - e le comunicano al Referente Privacy.

A) IL SEGRETARIO GENERALE – RESPONSABILE PRIVACY

Oltre a quanto sopra indicato, al **Segretario Generale** è attribuito il compito di sovrintendere alla gestione complessiva e all'attività amministrativa, esercitando poteri di coordinamento, verifica e controllo delle attività attribuite agli altri Designati.

Con determinazione del Commissario Straordinario n. 30 del 22.06.2022, adottata con i poteri sostitutivi della Giunta Camerale, il Segretario Generale facente funzioni dott. Enrico Ciabatti è stato nominato Responsabile dei Trattamenti dei dati personali per la CCIAA di Pavia (più in breve Responsabile Privacy).

Coerentemente con le competenze statutarie, sotto i profili della protezione e del trattamento dei dati personali, il SG esercita le seguenti funzioni:

a) sottoscrizione degli **accordi di contitolarità,** su delega specifica e previa approvazione della Giunta Camerale;
b) aggiornamento e manutenzione, con propria determinazione, dei **documenti gestionali** approvati dal la Giunta Camerale in funzione delle modifiche normative ed organizzative eventualmente intervenute ed all'emergere di eventuali criticità o necessità di miglioramento gestionale;
c) predisposizione ed approvazione di eventuali **documenti operativi** (es., linee guida, procedure, istruzioni operative, format di informative e consensi, etc.) del sistema di gestione che si rendessero necessari per garantire la più efficace implementazione di quanto previsto dalla normativa *privacy*;
d) **sottoscrizione delle notifiche dei *data breach*** ed approvazione delle comunicazioni agli interessati, secondo quanto previsto da apposita procedura gestionale;
e) gestione degli adempimenti derivanti dall'esercizio dei **diritti degli interessati** (artt. 15 e ss. del GDPR) e/o i **reclami** pervenuti direttamente alla Segreteria Generale ovvero relativi a processi o fasi di

attività nella propria diretta competenza, provvedendo a far alimentare il "Registro delle richieste di esercizio dei diritti degli interessati";

f) approvazione 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 della Giunta - svolgono trattamenti nell'ambito delle Aree, Servizi ed Uffici dell'Ente Camerale;

g) definizione e sottoscrizione – ove rientrante nelle proprie competenze, deleghe e poteri di spesa – delle **clausole contrattali o atti giuridici analoghi** per il conferimento della nomina a Responsabile del trattamento a soggetti esterni, ai sensi dell'art. 28 GDPR;

h) gestione dei **flussi informativi** al DPO e al Referente *privacy* (cfr. infra) di propria competenza e, più in generale, comunicazione al Referente *privacy* di ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati,

i) atti delegati dal Titolare.

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

B) I RESPONSABILI DI UFFICI/SERVIZI

Ai Responsabili degli Uffici/Servizi indicati nell'Organigramma Privacy – Allegato ("Uffici di Staff", "Risorse e Patrimonio", "Servizi Istituzionali" e "Servizi Promozionali") spetta la gestione finanziaria, tecnica e amministrativa, mediante autonomi poteri di spesa, di organizzazione delle risorse umane e strumentali nonché di controllo. Detti soggetti sono altresì responsabili della gestione delle funzioni loro assegnate e dei relativi risultati.

In coerenza con il Regolamento degli Uffici e dei Servizi, a tali Designati sono attribuite le seguenti funzioni:

a) **applicano -** nel contesto della specifica mission dell'Area di riferimento **- la normativa e le istruzioni** definite dalla Giunta e dal Segretario Generale attraverso i documenti gestionali del sistema *privacy*; sono altresì 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 od aggiornamento dei documenti gestionali predisposti, ad esempio evidenziando al Referente *privacy* 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 esempio, acquisizione di applicativi informatici per la gestione di determinate attività rientranti nella propria autonomia gestionale);

c) rilevano e segnalano al Referente *privacy* le eventuali e specifiche **esigenze formative o di approfondimento** da far valutare al SG, anche quale Responsabile della Privacy, ai fini della progettazione e programmazione dei percorsi formativi interni;

d) adottano ordinariamente, ovvero in caso di criticità e problematiche sopravvenute, **tutte le misure preventive e correttive[2] a tutela dei dati personali che le competenze connesse al ruolo consentano di assumere** (rientranti nell'ambito delle funzioni e budget attribuite), rappresentando al SG specifiche esigenze cui non possono far fronte ordinariamente;

---

[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.

e) 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 (ove strettamente necessario) l'acquisizione del **consenso** dagli interessati;

f) effettuano, nell'ambito delle funzioni istruttorie connesse alla proposta dei relativi atti e con il supporto del Referente *privacy*, l'istruttoria necessaria per la definizione degli **accordi di contitolarità** da sottoporre alla firma del SG;

g) in caso di affidamento di servizi ed incarichi professionali a **soggetti esterni** all'Ente, che comportino il trattamento di dati personali, provvedono in qualità di **proponente** (o di concerto con il) **responsabile unico del procedimento**, con la collaborazione del Referente *privacy*:
   - alla individuazione degli elementi di esperienza ed 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;

   in qualità di (ovvero di concerto con il) **Responsabile/Direttore dell'esecuzione del contratto/Referente contrattuale**, verificano il rispetto delle regole definite contrattualmente;

h) garantiscono che la **comunicazione** e la **diffusione** dei dati personali 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;

i) si attivano - in collaborazione con il Referente *privacy* - 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; ai attivano altresì per la conduzione della **valutazione preliminare del rischio** su ciascun trattamento e, ove necessario, provvedono ad eseguire la **valutazione d'impatto sulla protezione dei dati** e a supportare la Giunta nell'attivazione della consultazione preventiva del Garante ove ritenuta necessaria;

j) gestiscono i **flussi informativi** verso il DPO e il Referente *privacy* (cfr. infra) di propria competenza e, più in generale, la comunicano al Referente *privacy* di ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati.

C) IL REFERENTE INTERNO PRIVACY

Con la già menzionata comunicazione di servizio n. 1/2019, l'Ente ha attribuito l'incarico di Referente *privacy* alla D.ssa Chiara Scuvera, Responsabile del Servizio Affari Generali.

Il Referente *privacy*:

a) rappresenta il punto di riferimento interno per tutti gli Uffici e, in particolare, per gli altri Designati per le questioni che attengono, in generale, la *data protection* e la *compliance* dell'Ente lato *privacy*;

b) coordina le attività delle singole Aree / Uffici / Servizi per l'adeguamento dell'Ente alla normativa in materia di protezione dei dati personali;

c) fornisce supporto agli altri Designati in relazione agli adempimenti relativi alla *compliance privacy* dell'Ente e, ove necessario, interpella direttamente il DPO;

d) monitora costantemente l'applicazione e l'implementazione del sistema di gestione della *privacy* all'interno dell'Ente, segnalando al competente Responsabile di funzione e, se del caso, al SG, eventuali criticità riscontrate o necessità di adeguamento alla normativa;

[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.

e) rileva le esigenze di integrazione /modifica / aggiornamento dei documenti gestionali predisposti, con particolare riferimento alla necessità di modifica/integrazione del registro dei trattamenti di cui all'art. 30 del Regolamento;
f) rileva le eventuali e specifiche esigenze formative o di approfondimento e le sottopone al SG ai fini della progettazione e programmazione dei percorsi formativi interni;
g) in caso di *data breach*, ha specifici compiti individuati nella apposita procedura di gestione *data breach*;
h) collabora con il Titolare e con il DPO per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
i) offre supporto al DPO per l'espletamento dei propri compiti e funzioni come sopra delineati, garantendo la tempestività e la completezza dei flussi informativi;
j) svolge in collaborazione con i Responsabili di funzione coinvolti le valutazioni d'impatto secondo quanto previsto dagli artt. 35 e 36 del Regolamento e dalle indicazioni dell'EDPB e del Garante italiano;
k) gestisce i flussi informativi al DPO (cfr. infra) di propria competenza

SOGGETTI AUTORIZZATI AL TRATTAMENTO

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

Tutti i dipendenti dell'Ente sono Autorizzati al Trattamento, nei Servizi e negli Uffici in cui operano, come indicato nell'**Organigramma Privacy** (Allegato).

Gli Autorizzati possono visionare i singoli trattamenti assegnati sul **Registro dei Trattamenti dei Dati Personali approvato, disponibile sulla Intranet camerale**.

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

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

Oltre alle procedure e alle istruzioni tecniche che disciplinano le singole attività, ciascuna persona autorizzata al trattamento è altresì obbligata a conoscere e a rispettare le seguenti ulteriori procedure: *Disciplinare degli Autorizzati al trattamento*; *Procedura Data Breach*; *Linee Guida per la gestione degli archivi cartacei*; *Procedura per l'esercizio dei diritti degli interessati*.
Il personale autorizzato rimane soggetto al potere di vigilanza e controllo dei soggetti individuati nei paragrafi precedenti.

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

AMMINISTRATORI DI SISTEMA

Il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i. definisce l'amministratore di sistema come la *«figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i*

sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali».

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

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

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

FORMAZIONE ED INFORMAZIONE INTERNA

Al fine di ottemperare alle previsioni di cui all’art. 29 GDPR secondo le quali chiunque agisce sotto la diretta autorità Titolare del trattamento e “*abbia accesso a dati personali non può trattare tali dati se non è istruito*” nonché al fine di promuovere la diffusione della cultura della protezione dei dati personali, la CCIAA provvede a:

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

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

I dipendenti e collaboratori dell’Ente Camerale possono inoltre fare riferimento direttamente al Referente *privacy*.

STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA

REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI

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

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

- ❖ controllo di I livello, ad opera del SG e dei Responsabili di servizio/Ufficio nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di II livello (interno) svolto dal Responsabile Privacy (Segretario Generale) coadiuvato dal Referente interno Privacy nell'ambito della propria attività di monitoraggio continuo
- ❖ controllo di II livello (esterno) affidato al DPO.

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

PERIODICITÀ	DESCRIZIONE FLUSSO INFORMATIVO	RESPONSABILE FLUSSO
Tempestiva	Copia delle richieste di informazioni da parte di organi di Polizia Giudiziaria (ad es., Carabinieri, Polizia, Guardia di Finanza, etc.) o dal 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	Referente *privacy*
Tempestiva	Rilevazione incidenti di sicurezza (cfr. procedura *data breach*)	*Come da procedura*
Tempestiva	Richieste di esercizio dei propri diritti avanzate degli interessati, laddove richiedano espressamente un intervento del DPO (cfr. procedura diritti)	*Come da procedura*
Quadrimestrale	Verbali di analisi degli incidenti (cfr. procedura di *data breach*)	*Come da procedura*
Quadrimestrale	Risposte agli interessati in caso di reclami/esercizio diritti gestiti senza il coinvolgimento del DPO	Referente *privacy*
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile del trattamento	Referente *privacy*

PRIVACY AUDIT

La realizzazione di verifiche ed audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite è funzione affidata – nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al Referente Interno Privacy e al DPO.

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

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

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

RIESAME ED AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di *compliance* alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate

sia "*testata regolarmente*" (art. 32, par. 1, lett. d), del GDPR), il **Sistema di Gestione della Privacy** dovrà essere sottoposto a riesame / aggiornamento, almeno in occasione:

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

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

In caso, invece, si tratti di mero aggiornamento dei documenti del Sistema di Gestione della Privacy, lo stesso potrà essere attuato dal Segretario Generale.

DISCIPLINARE PER DESIGNATI E AUTORIZZATI

Le indicazioni che seguono costituiscono la disciplina che ciascun Autorizzato e/o Designato deve seguire nello svolgimento dei trattamenti di dati personali affidatigli, in ragione delle proprie mansioni.

Fermi restando i profili di responsabilità personale, sia di carattere disciplinare che di altra natura previsti per legge, il mancato rispetto delle istruzioni in materia di trattamento e protezione dei dati personali potrebbe comportare la violazione delle disposizioni normative nazionali ed europee in materia privacy nonché delle regole interne previste per la protezione dei dati personali, con conseguenziale esposizione della CCIAA a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e penale.

PRINCIPI FONDAMENTALI

Ogni trattamento di dati personali deve avvenire nel rispetto primario dei seguenti principi di ordine generale, fissati dall'art. 5 del GDPR.

I dati devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principi di «liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità (principio di «limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di «minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di «esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di «limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'Interessato, ovverosia di colui al quale i dati si riferiscono.

Ove l'Autorizzato o il Designato riscontri o sospetti che il trattamento dei dati personali è operato dall'Ente in violazione dei summenzionati principi, ne dà immediato avviso al Referente *privacy*.

REGOLE GENERALI DI COMPORTAMENTO

Gli autorizzati e i Designati sono tenuti a conoscere e ad attenersi scrupolosamente alle istruzioni loro fornite da Titolare, dal Segretario Generale e dal Responsabile di servizio/ufficio di riferimento.

Autorizzati e Designati sono altresì tenuti a prendere parte attiva alla formazione obbligatoria in materia di protezione dei dati personali.

Laddove l'Autorizzato o il Designato riscontri o sospetti essere intervenuta una violazione di sicurezza sui dati personali, tale da comprometterne la riservatezza (accesso abusivo), l'integrità (alterazione indebita) o la disponibilità (perdita, definitiva o provvisoria, per cancellazione, eliminazione o distruzione), ne dà immediato avviso al proprio Designato di riferimento (ove presente) e al Referente *privacy*, attenendosi a quanto indicato nell'ambito della procedura di gestione *Data Breach* e restando a disposizione dell'Ente per la raccolta di informazioni relative all'evento nonché – ove necessario – per porre in essere le strategie di contenimento dei rischi e le eventuali azioni di *remediation* (azioni correttive) decise dalla CCIAA.

Ove all'Autorizzato pervenga una richiesta di esercizio dei diritti in materia di protezione dei dati personali, ne dà immediato avviso al proprio Designato di riferimento, attenendosi a quanto previsto nell'apposita procedura interna.

Ciascun Autorizzato/Designato è tenuto a:

1) accedere ai soli dati personali per i quali si è autorizzati in ragione delle proprie mansioni;

2) operare esclusivamente i trattamenti connessi e necessari allo svolgimento dei propri compiti;

3) non utilizzare, diffondere o comunicare per fini personali o per altri finalità diverse da quelle fissate dal Titolare e/o al di fuori dei casi consentiti dalla normativa i dati personali di cui viene a conoscenza nell'esecuzione dei propri compiti/mansioni/attività, mantenendo il più assoluto riserbo in relazione ai dati e alle informazioni in qualunque forma appresi (per iscritto o oralmente, anche attraverso l'ascolto accidentale di colloqui, conversazioni, etc.);

4) conoscere e adottare con diligenza le misure di sicurezza previste dal Titolare, segnalando al proprio Designato di riferimento (ove presente) e al Referente *privacy* eventuali carenze sotto il profilo della protezione dei dati, in modo da ridurre al minimo i rischi, anche accidentali, di accesso non autorizzato ai dati, di impiego dei dati non consentito o non conforme alle finalità dichiarate agli Interessati, di modifica, alterazione o cancellazione/distruzione indesiderate dei dati;

5) informare immediatamente il proprio Designato di riferimento (o, per il Segretario Generale, il Vertice dell'Ente) qualora per le operazioni di trattamento sorga la necessità di compiere attività ulteriori o assumere decisioni non contemplate proprio incarico;

6) adottare ogni possibile cura ed attenzione nello svolgimento delle operazioni di trattamento dei dati personali, tenendo conto che la eventuale creazione di copie, in locale, in rete ovvero cartacee di documenti/archivi esistenti e contenenti dati personali, aumenta il livello di rischio per i diritti e le libertà degli interessati;

7) mantenere riservate le proprie credenziali di accesso ai sistemi informativi impiegati per ragioni lavorative, non comunicandole, diffondendole o condividendole con altri soggetti (compresi i colleghi di lavoro) e non trascrivendole (a titolo esemplificativo) in appunti, *post-it*, agende, prediligendo invece gestionali di *password* dotati di crittografia forte e protetti con *password* complessa;

8) custodire con cura e diligenza le chiavi fisiche (comprese le tessere/badge di accesso) che consentono l'apertura di armadi o l'accesso ad archivi e locali, evitando – salvo nei casi in ciò sia espressamente autorizzato – di effettuare copie, calchi o fotografie delle stesse e/o di consegnarle o prestarle ad altri soggetti (compresi i colleghi di lavoro, se non espressamente autorizzati a riceverle);

9) non comunicare e/o diffondere (a titolo meramente esemplificativo, a mezzo *social network* o sistemi di messaggistica personali) fotografie o dati, anche parziali, del proprio tesserino di riconoscimento e/o badge rilasciato dall'Ente;

10) non lasciare in alcun modo incustoditi o accessibili documenti e strumenti di lavoro (compreso – a titolo esemplificativo – il computer o laptop impiegato per lo svolgimento delle proprie mansioni) al termine della sessione lavorativa, nonché in ogni occasione di allontanamento (anche se di brevissima durata) dalla propria postazione;

11) fornire assistenza e collaborazione al DPO e al Referente *privacy* in relazione a loro possibili richieste di informazioni o allo svolgimento di *audit*;

12) al termine del proprio rapporto di lavoro con l'Ente, provvedere alla restituzione delle chiavi fisiche e di tutto il materiale (cartaceo ed elettronico) contenente dati di carattere personale, cancellandone/distruggendone ogni eventuale copia.

REGOLE AGGIUNTIVE PER I DESIGNATI

Per quanto attiene, in particolare, alla figura dei Designati, questi devono:

i) individuare, nel proprio ambito camerale di competenza, tutte le persone le cui mansioni lavorative implicano il trattamento di dati personali;

ii) assicurarsi che le autorizzazioni ad accedere, modificare o cancellare/distruggere i dati, assegnate a ciascun Autorizzato, siano esclusivamente quelle minime e strettamente necessarie rispetto alle mansioni lavorative che l'Autorizzato è chiamato a svolgere;

iii) assicurarsi che gli autorizzati operino nel rispetto delle istruzioni loro impartite, in relazione al trattamento e alla protezione dei dati personali;

iv) adoperarsi al fine di rendere effettiva la tutela della riservatezza, dell'integrità e della disponibilità dei dati, nonché e l'osservanza da parte degli Autorizzati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

v) stabilire modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati, come le modalità di trasmissione dei dati da parte degli stessi, avendo cura di adottare preventivamente le più opportune misure organizzative;

vi) stabilire delle modalità di accesso all'archiviazione dei dati che riduca il rischio di impatto sui dati, facendo in modo che l'accesso alle informazioni sia garantito esclusivamente agli autorizzati che ne hanno effettivo bisogno per lo svolgimento delle proprie mansioni lavorative e nei limiti delle stesse;

vii) organizzare le modalità di lavoro al fine di ridurre il rischio di impatto sui dati;

viii) comunicare periodicamente al DPO l'elenco aggiornato dei nominativi con i relativi profili autorizzativi per l'accesso alle banche dati di pertinenza;

ix) comunicare al DPO eventuali problematiche e qualsiasi variazione ai profili autorizzativi o organizzativi.