CAMERA DI COMMERCIO
SONDRIO

DISCIPLINARE PER IL PERSONALE CAMERALE AUTORIZZATO AL TRATTAMENTO DI DATI

1. Premessa

Con il regolamento (UE) n. 679/2016, di seguito anche GDPR, di fondamentale importanza è diventata l'organizzazione dei ruoli e dei rispettivi compiti in materia di trattamento dei dati e riservatezza. In particolare, con la definizione di un Organigramma della Privacy è possibile procedere alla individuazione e nomina del Titolare, dei Referenti interni, dei Responsabili esterni e, ancorchè non espressamente previsto dal GDPR, anche degli Autorizzati al trattamento dei dati personali (ex incaricati al trattamento) per conto del Titolare o dei Responsabili.

A tale riguardo si ricorda che per il GDPR "titolare del trattamento" è: 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.

Titolare del trattamento per tutti i dati trattati dai dipendenti camerali nell'ambito di attività/servizi/procedimenti camerali è la Camera di commercio di Sondrio, che esercita tale ruolo attraverso il Segretario Generale, in ottemperanza alle disposizioni normative di cui al D.lgs. 165/2001 e, in particolare, in attuazione del principio di separazione di competenza fra organi di governo e dirigenza di cui all'articolo 4 del predetto decreto.

Per responsabile del trattamento il GDPR intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. La Camera di commercio, in qualità di titolare del trattamento, ha proceduto a nominare responsabili del trattamento diversi soggetti esterni, tra cui Infocamere.

2. Linee operative

A prescindere dai diversi ruoli aziendali in materia di Privacy (di cui all'Organigramma Privacy) si evidenzia che, come codificato sia nei provvedimenti in materia di privacy assunti negli anni pregressi (determinazione n. 201/SG/2008) che nel Manuale di gestione documentale aggiornato, da ultimo nel 2022, tutti i dipendenti dell'Ente risultano autorizzati al trattamento dei dati afferenti alle attività/servizi/procedimenti di competenza dell'unità operativa e/o Area di appartenenza.

Il personale autorizzato ad un trattamento di dati personali deve operare in modo tale che vengano rispettate le normative vigenti per la riservatezza dei dati e la sicurezza del trattamento e deve seguire le disposizioni particolari fissate dal proprio Referente.

Le norme di comportamento standard adottate dall'ente per i trattamenti di dati personali sono riportate, oltre che nel presente disciplinare, nelle linee guida sulla "Social media policy della Camera di commercio di Sondrio" di cui alla determinazione del Segretario generale n. 169/2017.

Di seguito sono descritte le modalità con cui i dati devono essere trattati al fine di essere allineati con la normativa dettata dal GDPR, modalità che variano a seconda della tipologia di dati trattati: solo dati comuni, dati particolari (ex dati sensibili) e dati giudiziari.

Si rammenta che per "dato personale" il GDPR intende 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. Pertanto i dati riferiti ad una persona giuridica (denominazione, ragione sociale, CF, partita IVA) non sono mai dati personali. Nel caso di impresa individuale sono dati personali quelli riferibili alla persona fisica titolare dell'impresa (quali CF o ditta dell'impresa).

Per "trattamento" il GDPR intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

2.1. Trattamento di dati personali comuni (artt. 5 e seguenti GDPR)

L'autorizzato opera in modo tale che i dati personali comuni (es. nome, cognome, CF, residenza) oggetto di trattamento siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *("liceità, correttezza e trasparenza");*
b) raccolti e registrati per scopi documentati e determinati, espliciti e legittimi, ed utilizzati in altri trattamenti correlati in modo compatibile con gli scopi per cui sono stati raccolti *("limitazione delle finalità");*
c) esatti e, se necessario, aggiornati; devono inoltre essere adottate tutte le ragionevoli misure per la cancellazione o la rettifica tempestiva dei dati inesatti, rispetto alle finalità del trattamento

("esattezza");

d) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati *("minimizzazione dei dati");*

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati personali possono comunque essere conservati per periodi di tempo più lungo, a condizione che siano trattati esclusivamente a fini archivistici di pubblico interesse, ricerca scientifica o storica o per fini statistici *("limitazione della conservazione");*

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali – compresa la protezione mediante misure tecniche ed organizzative adeguate – da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale *("integrità e riservatezza").*

Ai sensi degli artt. 32 e seguenti del GDRPR, le attività di trattamento devono seguire le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, quali:

- la pseudoanonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare – su base permanente – riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali, in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza nel trattamento.

In attuazione delle previsioni di legge gli autorizzati devono:

g) utilizzare l'autenticazione informatica, custodendo con la massima riservatezza la credenziale di accesso (user-id) e la password; le credenziali non possono essere comunicate a terzi e non possono essere custodite in chiaro; le password devono essere cambiate almeno ogni sei mesi;

h) attivare la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

i) seguire le indicazioni del proprio Referente fornite sulla base della documentazione presente;

j) seguire le procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Nel caso in cui il trattamento sia effettuato con supporti cartacei si deve prevedere:

k) idonea custodia di atti e documenti affidati agli autorizzati per lo svolgimento dei relativi compiti;

l) conservazione di determinati atti in archivi ad accesso selezionato.

Per attuare idonea custodia agli uffici e agli archivi si possono adottare le seguenti semplici

precauzioni:

m) chiudere a chiave la porta dell'ufficio in assenza del personale preposto;
n) mantenere la documentazione cartacea negli armadi e chiudere a chiave gli armadi al termine della giornata di lavoro;
o) mantenere la massima riservatezza con gli estranei e prestare la massima attenzione affinché persone non autorizzate al trattamento non possano, neppure incidentalmente, venire a conoscenza di documenti contenenti dati personali.

Nel valutare l'adeguato livello di sicurezza si deve, in particolar modo, tenere conto dei rischi presentati dal trattamento dei dati, soprattutto dalla loro distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso – in modo accidentale e/o illegale – ai dati personali trasmessi, conservati o trattati.

In caso di violazione delle normative e delle regole, l'autorizzato deve informare tempestivamente il proprio Referente e seguire le eventuali indicazioni che egli darà per minimizzare le ricadute sull'Ente.

Va ricordato che, ai sensi dell'art. 32 e seguenti del GDPR, in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di Controllo competente senza ingiustificato ritardo e, se possibile, entro le 72 ore dalla venuta a conoscenza. Inoltre quando la violazione dei dati personali è suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ritardo ingiustificato.

Per la valutazione del rischio e le modalità operative in caso di violazione si rinvia alla procedura di gestione del data breach approvata dall'Ente.

2.2. Trattamento di dati personali particolari - ex dati sensibili D.lgs. 196/2003 - (artt. 9 e seguenti GDPR)

Il GDPR sancisce il divieto di trattamento di dati *"personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

Il generale divieto di trattamento di detti dati non opera in determinati casi tra cui si evidenziano quelli di potenziale interesse camerale:

- L'interessato abbia prestato il proprio consenso esplicito al trattamento dei dati personali, per una o più finalità specifiche;
- Il trattamento sia necessario per assolvere gli obblighi ed esercitare diritti specifici del titolare del

trattamento o dell'interessato in materia di diritto del lavoro, sicurezza sociale e protezione sociale e gli interessi dell'interessato;

- Il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato stesso;
- Il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- Il trattamento sia necessario per motivi di pubblico interesse rilevante, che deve essere proporzionato rispetto alla finalità perseguita;
- Il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, gestione dei sistemi e servizi sanitari o sociali, fatti salvi i casi in cui i dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di riservatezza;
- Il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'individuo.

L'Autorizzato al trattamento dei dati personali particolari opererà nelle seguenti modalità:

a) nel momento in cui i dati particolari sono (come nella maggioranza dei casi) relativi ai dipendenti dell'Ente e, quindi, legati alla gestione del personale, ove si trattino dati storici compresi eventuali file di pertinenza dell'interessato, devono essere conservati in un archivio riservato dell'ufficio competente alla gestione del personale, tali file devono inoltre essere archiviati su supporto permanente;
b) nel caso in cui il trattamento sia effettuato con supporti cartacei o richieda supporti cartacei si deve attuare idonea custodia tramite conservazione di quei determinati documenti o atti contenenti dati particolari in archivi ad accesso selezionato, possibilmente chiusi a chiave.

Tenuto conto dei particolari limiti e garanzie il GDPR prevede, l'autorizzato è tenuto al compimento delle attività di trattamento nel pieno rispetto della normativa vigente e soprattutto delle peculiarità previste, ai sensi dell'art. 9 del GDPR, per i dati personali particolari.

2.3. Trattamento di dati personali relativi a condanne penali e reati

Con specifico riguardo al trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, ai sensi dell'art. 10 del GDPR, esso *"deve avvenire soltanto sotto il controllo dell'Autorità Pubblica o se il trattamento è autorizzato dal diritto dell'Unione e dagli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali*

deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica".

Il trattamento di tali dati può quindi avvenire solamente se espressamente previsto da una norma di legge. Per la natura dei dati trattati di tipo giudiziario, l'attenzione da prestare sul trattamento degli stessi deve essere molto puntuale, mantenendo la massima riservatezza nello svolgimento delle attività e nella custodia delle informazioni, siano esse in forma elettronica che cartacea.

2.4. Comunicazione e diffusione di dati personali

La comunicazione e la diffusione dei dati personali "comuni", quindi non particolari (ex sensibili) e/o giudiziari, è permessa esclusivamente nei casi indicati dall'art. 2 ter del D.Lgs. 196/2003 e deve essere preventivamente autorizzata dal proprio referente.

2.5. Indicazioni per la gestione di dati personali trattati senza l'ausilio di strumenti elettronici

Le presenti indicazioni sono rivolte a tutto il personale camerale e hanno ad oggetto il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici.

Nell'ipotesi di trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è fatto espresso obbligo di osservanza delle seguenti disposizioni:

- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso in cui ciò avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, gli stessi non dovranno essere lasciati incustoditi;
- è fatto obbligo di controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;
- al termine dell'orario di lavoro, tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici devono essere riportati nei locali individuati per la loro conservazione;
- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi nelle postazioni di lavoro;

- si deve adottare ogni idonea cautela affinché altre persone non vengano a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici;
- per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro dipendente debitamente autorizzato;
- i documenti contenenti dati personali di cui agli articoli 9 e 10 del Regolamento (UE)[1] o dati che, per una qualunque ragione, siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura in armadi chiusi a chiave;
- è tassativamente proibito utilizzare copie fotostatiche di documenti (anche parziali o non integralmente leggibili) all'esterno del luogo di lavoro.

[1] **Art. 9 Regolamento (UE) ha ad oggetto i** dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Art. 10 Regolamento (UE) ha ad oggetto i dati personali relativi a condanne penali e reati