Allegato 3

CAMERA DI COMMERCIO
REGGIO CALABRIA

LINEE GUIDA PER LA FORMAZIONE SUL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI

ai sensi del Regolamento UE 679/2016

1 - PREMESSA

1.1. – OBIETTIVI E CAMPO DI APPLICAZIONE

Obiettivi del presente documento è definire le specificità della formazione permanente sul trattamento dei dati personali e le relative misure di sicurezza da parte della Camera di commercio di Reggio Calabria.

A questo riguardo si tenga conto di quanto segue.

Il documento:

a) non costituisce una guida sulle teorie della formazione/apprendimento, né sulle implicazioni della formazione sui cambiamenti dei dipendenti e dell'organizzazione in cui questi operano;

b) si inserisce nell'ordinaria procedura interna per la predisposizione ed erogazione della formazione da parte dell'Ente;

c) presenta una sua specificità con riferimento agli obblighi previsti dal GDPR sulle "istruzioni" che il Titolare è tenuto a fornire ai dipendenti/collaboratori, nonché dei rischi che implica il trattamento dei dati.

d) deve essere approvato dal competente organo previa l'espressione del parere positivo del Responsabile della Protezione dei Dati (RDP/DPO).

1.2. - RIFERIMENTI NORMATIVI PRINCIPALI

Il presente documento risponde ai seguenti requisiti normativi:

1. Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37 e ss. del GDPR);
3. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
4. Artt. 29, 32, 39 del GDPR;
5. Attribuzione di funzioni e compiti a soggetti designati (art. 2-quaterdecies del D.Lgs. n. 196/2003);
6. WP29, parere n. 3/2010, sul principio di responsabilità (00062/10/IT -WP 173), adottato il 13 luglio 2010

1.3. - ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE n. 679/2016 (General Data Protection Regulation)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali"
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati - EDPB)

RPD/DPO	Responsabile della Protezione dei Dati/ *Data Protection Officer*
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate 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

2 – CONTESTO GIURIDICO

2.1. – OBBLIGHI DELL'ISTRUZIONE E DELLA FORMAZIONE

Il complesso delle disposizioni introdotte con il GDPR assume una nuova rilevanza nei processi delle imprese e delle pubbliche amministrazioni laddove la corretta gestione del trattamento dei dati personali è una questione da affrontare sotto il punto di vista giuridico, tecnologico e, soprattutto, organizzativo.

Tutto ciò comporta una "revisione" dei flussi e delle dinamiche organizzative (non è un caso che si parli di "Privacy by design"), apportando quei cambiamenti delle procedure e delle prassi che guidano lo svolgimento delle attività. Questi cambiamenti richiedono necessariamente, a tutti i livelli – a cominciare dalla *governance* –, una rinnovata consapevolezza del diverso quadro di riferimento.

Il GDPR, a questo fine, introduce a carico dei Titolari e dei Responsabili dei trattamenti di dati personali l'obbligo della *formazione a tutti i livelli*.

L'art. 29 del GDPR dispone che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso ai dati personali *non può trattare tali dati se non è istruito in tal senso dal titolare …*"[1].

Non si tratta di una novità. Il WP29, nel parere n. 3/2010, aveva già individuato tra le misure comuni concernenti la responsabilità – e quindi, come si dirà più avanti, parte integrante dell'*accountability* - "*un'adeguata formazione ed istruzione del personale in materia di protezione dei dati. Tale formazione dovrebbe includere tutti i livelli e tutte le figure, anche dirigenziali, di dipendenti o collaboratori che trattano dati personali per conto del Titolare o del Responsabile*".

La centralità della formazione è confermata anche dall'art. 32 del GDPR, in tema di sicurezza del trattamento, il cui par. 4 prevede che *"Il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*". Del tutto evidente il legame con il rischio del trattamento che grava sul Titolare che ne deve assumere ogni responsabilità, non potendo inserire il trattamento nelle "ordinarie" mansioni del lavoratore/collaboratore. Più in particolare, in mancanza di specifiche "istruzioni", non è legittimo trattare dati personali.

Vale la pena di osservare che il termine "istruzione" non è esplicitato chiaramente nel GDPR e va inteso in due accezioni diverse che si completano vicendevolmente. Sono le "istruzioni" riferite allo svolgimento dell'attività demandata (in questo contesto ci si riferisce al trattamento dei dati personali) e, più in generale, al più ampio ambito – come detto, giuridico, tecnico ed organizzativo – nel quale si inserisce il trattamento dei dati personali.

Le "istruzioni" costituiscono, se si vuole, la parte "esecutiva" della formazione[2].

---

[1] Le "istruzioni" sono dirette anche al Responsabile esterno del trattamento. Ai sensi dell'art. 28, par. 3, lett. a), il Responsabile tratta "(…) i dati personali soltanto su istruzione documentata del titolare del trattamento (…)".

[2] l'istruzione a livello pratico è volta ad evitare che eventuali condotte inconsapevoli od omissioni possano da una parte pregiudicare il funzionamento delle infrastrutture informatiche e dall'altra compromettere la sicurezza delle informazioni. La norma internazionale ISO/IEC 27001:2013 che definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), considera la

La formazione *precede* e *segue* lo svolgimento dell'attività. Una formazione adeguata rappresenta, pertanto:

a) un prerequisito per potere operare all'interno delle organizzazioni, pubbliche o private.

b) un elemento di "qualificazione" necessario per operare in concreto.

Parla esplicitamente di "formazione", l'art. 47, del GDPR, in tema di "Norme vincolanti d'impresa" laddove, al par. 2 prevede che "*Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno: (…) n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali*".

2.2. - FORMAZIONE ED ACCOUNTABILITY

Una formazione adeguata del personale autorizzato ai trattamenti rappresenta, essa stessa, una misura basilare al fine di garantire un livello di sicurezza adeguato a garanzia del Titolare del trattamento sul quale – è bene sottolinearlo – ricade, di regola, ogni responsabilità.

Inoltre, la previsione di programmi formativi diretti al personale e ai collaboratori concretizza il principio di *accountability* ossia di responsabilizzazione del Titolare del trattamento, previsto dal GDPR.

Infatti, il Titolare deve essere in grado di dimostrare che il trattamento dei dati sia non solo lecito, corretto, trasparente, pertinente, adeguato, legittimo, ma anche che vengano rispettati i principi di minimizzazione, di conservazione dei dati e che siano previste (ed osservate) misure di sicurezza adeguate.

I dipendenti e i collaboratori potranno trattare i dati solo se autorizzati ed entro i limiti delle istruzioni impartite dal Titolare, il quale potrà comunque avvalersi, come intermediario, di altro soggetto debitamente autorizzato.

Un adeguato piano formativo rappresenta, pertanto, uno dei tasselli rilevanti del sistema di gestione della privacy delle pubbliche amministrazioni, in grado di concretizzare il '*principio di accountability*' inteso come capacità di dimostrare di avere adottato misure di sicurezza adeguate, che sono anche quelle "culturali" in base alle quali vengono concretamente gestiti i dati.

---

formazione come una misura di sicurezza (v. A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione), alla quale corrispondono i seguenti profili di rischio:

RISCHIO BASSO - L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica con valutazione finale tramite test del livello di apprendimento.

RISCHIO MEDIO - L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati con valutazione finale tramite test del livello di apprendimento.

RISCHIO ALTO - Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti con valutazione finale tramite test del livello di apprendimento.

Secondo questa prospettazione un adeguato e specifico piano/programma di formazione non deve essere considerato un adempimento burocratico quanto, piuttosto, un'opportunità per rendere consapevoli gli operatori dei rischi connessi al trattamento dei dati, nonché uno strumento che contribuisce a migliorare le misure di sicurezza, i processi organizzativi, i servizi erogati, evitare o minimizzare danni d'immagine, ridurre i rischi di sanzioni amministrative.

A tal fine gli organi dell'Ente devono approvare il piano dei programmi di formazione del personale in materia di trattamenti di dati personali, pubblicando il piano ed i relativi materiali formativi in una specifica sezione intranet dell'Ente al fine di costituire un presidio di informazione e aggiornamento a beneficio di tutto il personale.

Tali programmi formativi sulla protezione dei dati potranno pianificarsi in modo integrato con altri piani formativi sulla digitalizzazione dei processi, con i codici di comportamento degli enti, con le normative in materia di trasparenza, prevenzione della corruzione.

Nell'ottica di un miglioramento continuo e di una gestione in qualità del sistema privacy, potrebbe essere opportuno anche progettare sessioni informative/formative on line per sensibilizzare tutto il personale sul valore della protezione dei dati personali e sull'utilizzo consapevole e responsabile di Internet.

2.3. - PREVISIONE DELLE RISORSE ED APPROVAZIONE DELLA FORMAZIONE

L'Ente, in coerenza con i propri documenti di programmazione e le risorse disponibili, svolgerà attività di formazione permanente sulla tutela dei dati personali, secondo quanto previsto dal presente documento. In un'ottica di sistema e di coerenza con gli attesi target qualitativi, verrà data priorità all'adesione ai programmi formativi organizzati da Unioncamere nazionale e nell'ambito delle piattaforme nazionali per i dipendenti delle pubbliche amministrazioni (ad es. Syllabus).

2.4. – FORMAZIONE QUALE MISURA DI PREVENZIONE

La rilevanza della formazione è fondamentale quale misura idonea a favorire che lo svolgimento delle attività di competenza avvenga in una documentabile cornice di legalità, nel rispetto delle disposizioni vigenti, la cui inosservanza esporrebbe l'Ente camerale al rischio di sanzioni amministrative. La mancanza di una formazione adeguata e aggiornata espone l'Ente al rischio di non saper gestire i trattamenti con i criteri e modalità imposti dalla normativa e per l'effetto, all'obbligo risarcitorio dei danni conseguenti e all'applicazione di sanzioni amministrative, come previste dal Regolamento UE 679/2016.

2.5. - COMPITI DI CONTROLLO DEL DPO

La rilevanza della formazione è testimoniata anche dall'art. 39, par. 1, lett. b), del GDPR, laddove, tra i compiti del DPO, vi rientra anche sorvegliare l'osservanza delle disposizioni del GDPR da parte del Titolare o del Responsabile del trattamento dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

In relazione alla formazione ed al coinvolgimento del RPD/DPO si fa presente che:

a) il piano di formazione è sottoposto al suo previo parere;

b) gli esiti e gli effetti dell'avvenuta formazione gli sono comunicati ai fini dei suoi compiti di "sorveglianza";

c) può partecipare alla formazione, quale docente, specie per quelle attività/procedimenti di cui può agevolmente illustrare le ricadute giuridiche ed operative in tema di trattamento dei dati personali.

Per la valutazione della formazione (iniziale o di periodico aggiornamento) cui sottoporre i dipendenti del Titolare, il Garante francese (CNIL), nel 2011, ha emanato un provvedimento in cui – sulla scorta della norma UNI ISO 29990:2011 – ha individuato i seguenti ambiti di riferimento: a) la valutazione del corso di formazione rispetto ai contenuti ed alle capacità dei formatori; b) la valutazione della modalità di strutturazione del corso.

In merito alla valutazione del corso rispetto alle competenze necessarie ad erogarlo, si valuteranno le competenze professionali dei docenti e la loro qualificazione anche in relazione alla tipologia di corso ed ai suoi destinatari. Circa le modalità di strutturazione (moduli, webinar, lezione frontale, etc.), sarà verificata se l'organizzazione del corso – quanto alle tipologie e modalità di erogazione/fruizione – sia in grado di consentire ai partecipanti di conseguire gli obiettivi sottesi al corso medesimo.

Le fasi del processo valutativo da parte del DPO sono, esemplificativamente, le seguenti:

a) verifica delle esigenze formative;

b) verifica della struttura del corso;

c) verifica della coerenza tra gli obiettivi, la durata e gli strumenti del corso;

d) verifica del materiale didattico;

e) coerenza di quanto indicato alle precedenti lett. a)-d), con le capacità/esperienza del docente;

f) verifica circa le modalità di svolgimento effettivo del corso, per esempio con schede di valutazione dei partecipanti (ovvero con la presenza dello stesso DPO);

g) verifica dell'efficacia del corso, attraverso dei test, ovvero specifiche schede di valutazione delle competenze acquisite;

h) archiviazione delle attività di formazione in tema di trattamento dei dati personali, affinché sia possibile provare l'accountability del Titolare su questi obblighi.

2.6. - LA FORMAZIONE DEL DPO

Allo stato attuale della disciplina non esistono Albi o certificazioni che siano necessarie al DPO per poter svolgere il suo incarico[3]. La nomina del DPO si basa, in particolare, sul criterio della "sostanziale" esperienza e conoscenza della normativa e della giurisprudenza in materia di trattamento di dati personali, nonché la specifica situazione in cui opera il Titolare

[3] Come ribadito a più riprese dall'autorità, allo stato attuale non esistono titoli abilitanti o attestati formali che determinano l'idoneità di un Responsabile della Protezione dei Dati. Tuttavia, eventuali certificazioni delle competenze professionali, specialmente quando sono rilasciate da enti indipendenti di terza parte, costituiscono un valido strumento ai fini della verifica del possesso di un certo livello di conoscenza della disciplina. Come ha chiarito il Garante, con la nota del 27 marzo 2018, n. 9530/2018, le certificazioni sono sempre volontarie, e non sono mai obbligatorie per svolgere il ruolo di *Data Protection Officer*, sia che siano basate su schemi proprietari che su norme tecniche pubbliche (come la UNI 11697:2017).

(nel nostro caso: il DPO deve avere una conoscenza significativa del sistema camerale e delle procedure che si svolgono al suo interno). La dimostrazione di dette conoscenze è rimessa al Titolare che può accertarla come meglio ritenga (valutazione del curriculum, colloquio, etc.).

Proprio al fine del mantenimento di un adeguato livello di conoscenza, il Titolare (cioè il "datore di lavoro" del DPO)[4] deve consentirgli di mantenere la propria competenza specialistica.

Tra le norme specifiche riferite ai profili professionali sul trattamento dei dati personali vi è la UNI 11697:2017 che, oltre al rilascio della certificazione per i diversi profili previsti, prevede anche le modalità per il mantenimento della certificazione. Nell'ambito di ogni anno di vigenza della certificazione conseguita il DPO deve dimostrare di aver partecipato a corsi di formazione, docenze, ovvero gruppi di lavoro e/o attività relative al trattamento dei dati personali nel contesto in cui opera.

3 - PROFILI E MODALITA' DELLA FORMAZIONE

3.1. – GENERALITA'

La formazione, per essere efficace, non può essere "universale" ma deve essere "coerente" con le esigenze dei singoli profili di coloro che la ricevono. Nell'ambito dei singoli profili, inoltre, deve essere progettata una "successione" di interventi basati su un progressivo innalzamento del livello di approfondimento, previa verifica dell'acquisizione (e possibilmente utilizzo) di quanto ricevuto.

Con riferimento ai "profili", con tutta evidenza, la formazione deve essere differenziata rispetto all'inquadramento ed al ruolo dei dipendenti, si avrà così la formazione destinata: agli "amministratori", al segretario generale, ai dirigenti, ai titolari di incarico di elevata qualificazione, al RDP/DPO, etc.

Con riferimento al livello di approfondimento si avrà, per es., oltre alla formazione "di base", quella "superiore" e quella "avanzata", con crescenti livelli di qualificazione.

La formazione specializzata può riguardare anche le specificità di Aree/Uffici/Servizi. Si pensi, per fare un facile esempio, le esigenze conoscitive/operative dei trattamenti di dati personali dell'Ufficio del personale.

Quanto alle modalità della formazione, nell'ambito della singola progettazione degli interventi, saranno verificate le molteplici tipologie/forme/strumenti disponibili al fine di comporre il "mix" ritenuto idoneo al caso specifico.

---

[4] Questa specificazione appare necessaria. Mentre se il DPO è un dipendente del Titolare, spetta a questi mantenere lo stato delle conoscenze del DPO attraverso gli opportuni interventi formativi periodici, qualora questi non sia un dipendente del Titolare (si pensi al caso il cui il DPO sia un avvocato di uno studio professionale), spetta al soggetto che è il suo "datore di lavoro" provvedere a questo obbligo. Qualora il DPO, quale soggetto 'esterno', si trovi ad operare in un contesto particolare, si ritiene che il Titolare debba comunque rendere disponibili le informazioni e le cognizioni, proprie del suo ambito, ai fini del perfezionamento delle competenze del DPO, come, ad esempio, sentenze specifiche riguardanti detto ambito che possano essere di ausilio all'inquadramento dei temi del trattamento dei dati personali proprie di quest'ambito.

Tra le tipologie, che possono essere distinte – unicamente in termini esplicativi e non esaustivi – tra "in presenza" e "da remoto", troviamo la "lezione", il "seminario", il "workshop", la "pillola", con o senza la presenza di esercitazioni pratiche[5]. Seguono, o dovrebbero seguire, i relativi test di valutazione (autovalutazione) dell'apprendimento conseguito.

Altre scelte riguardano gli strumenti didattici: volumi, dispense ed altri documenti cartacei, e-book, slides, "presentazioni", testi informatici e telematici iperlinkati[6], siti web, etc.

Ulteriori decisioni concernono il/i formatore/i, il livello e lo "stile" della formazione: docente/professionista; "collega" interno/esterno, etc.

Infine, occorre predisporre gli opportuni strumenti per la rilevazione ed il monitoraggio dell'attività formativa svolta.

3.2. - I PROGRAMMI FORMATIVI

Un adeguato piano formativo dovrebbe, alla luce del GDPR, presentare un taglio interdisciplinare (con adeguati programmi che prevedano nozioni non solo giuridiche ma anche tecnico-informatiche di livello adeguato nonché sui profili organizzativi dell'Ente o dell'organismo Titolare) e pratico (come si evince dal termine "istruito" previsto all'art 29 e 32 del GDPR) e riguardare tutti i soggetti.

Un piano formativo adeguato deve quindi essere finalizzato ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

---

[5] Le esercitazioni sono caldamente consigliate. La dimostrazione di un'idonea preparazione si comprova attraverso l'effettivo esercizio delle attività sulla base delle "istruzioni" ricevute ed acquisite. In caso di controlli, infatti, il verificatore con ogni probabilità potrebbe coinvolgere degli operatori e chiedere di eseguire certe operazioni correlate al trattamento analizzato, anche con domande specifiche e dirette, al fine di comprendere se il personale coinvolto è consapevole dei trattamenti che sta effettuando, e se ad esempio abbia chiaro il ruolo della propria organizzazione per quel trattamento e delle relative conseguenze. Le prove pratiche possono essere realizzate anche con il supporto del RDP/DPO.

[6] Un esempio di testo *iperlinkato* è costituito dal "Manuale del sistema di gestione della protezione dati personali" della Camera di commercio di Milano, Monza-Brianza e Lodi (revisionato nel 2021).
Le finalità del Manuale sono le seguenti:
"• rappresentare l'assetto complessivo delle misure tecniche ed organizzative che la Camera mette in campo per garantire - ed essere in grado di dimostrare - la conformità al Regolamento delle attività di trattamento dei dati personali che effettua nello svolgimento dei compiti istituzionali di propria competenza e delle connesse attività amministrative;
• documentare le politiche adottate (con particolare riferimento a quelle di sicurezza e secondo valutazioni di adeguatezza correlata al rischio) per contenere i rischi di violazione del diritto fondamentale dell'individuo alla protezione dei dati personali, sancito dalla Carta dei diritti fondamentali dell'Unione europea (art. 8);
• raccogliere in un quadro organico e coordinato degli strumenti (mappa) utilizzati dall'organizzazione per perseguire la piena conformità dei propri comportamenti ai principi e alle disposizioni della norma e descrivere la metodologia adottata dall'Ente;
• favorire una sostanziale compliance dell'organizzazione promuovendo consapevolezza e comportamenti responsabili e corretti da parte di tutto il personale".

La formazione prevede anche l'analisi specifica dei documenti che costituiscono il Sistema di gestione dei dati personali dell'Ente camerale.

Ad ogni buon conto, i contenuti dei piani formativi saranno, di volta in volta, determinati dal Titolare in collaborazione con il RPD dell'Ente, stabilite le priorità di intervento in ragione dello stato di consapevolezza dei soggetti autorizzati e l'evolversi del contesto normativo vigente.