

PRIVACY

**I SERVIZI E I PRODOTTI
PER L'APPLICAZIONE DELLA
NORMATIVA SUL TRATTAMENTO
DEI DATI PERSONALI NELLA P.A.**

GRUPPO

Maggioli

In seguito all'introduzione del Regolamento Europeo 2016/679 o GDPR, dal 25 maggio 2018 i Paesi della UE si sono trovati a dover fare i conti con una normativa complessa e molto garantista per i diritti e le libertà dei propri cittadini.

In Italia il quadro normativo è divenuto definitivo, o quasi, a partire dal 19 settembre 2018, data di entrata in vigore del D.Lgs n. 101/2018 che ha adeguato la previgente normativa in materia (D.Lgs. n. 196/2003 cosiddetto Codice Privacy) alle disposizioni del Regolamento UE 2016/679.

Per raggiungere la *compliance* prevista dal Regolamento europeo, agli enti è richiesto un importante sforzo di analisi, gestione ed attuazione di nuovi pro-

cessi atti a garantire la sicurezza dei dati ed il rispetto della volontà dei cittadini; azioni queste che si riflettono in modo trasversale sull'intera organizzazione. Si tratta di un **radicale cambiamento nell'approccio al trattamento delle informazioni** che richiede una approfondita verifica delle procedure di gestione adottate e da adottare.

In caso di inadempimento gli Enti sono soggetti a sanzioni amministrative e penali nonché a responsabilità civile con relativo risarcimento del danno.

Al fine di affiancare le Amministrazioni nell'attuazione di tutti gli adempimenti, Maggioli offre una vasta e completa gamma di soluzioni di seguito illustrati.

I SERVIZI

1 ASSUNZIONE DEL RUOLO DI RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO) Servizio onsite e online

Ogni Ente è tenuto a nominare obbligatoriamente il Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO). Maggioli offre il servizio di assunzione del ruolo di DPO che prevede lo svolgimento delle seguenti attività (art. 37, 38 e 39 Regolamento UE 2016/679):

- a) **Informare e fornire consulenza** al titolare del trattamento nonché ai dipendenti che eseguono il trattamento sugli obblighi derivanti dal Regolamento UE 2016/679 ovvero da altre disposizioni relative alla protezione dei dati;
- b) **Sorvegliare sull'osservanza del Regolamento** e sulle altre disposizioni relative alla protezione dei dati, nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione della responsabilità, la sensibilizzazione e la formazione del personale che partecipa alla gestione dei dati ed alle connesse attività di controllo;

- c) **Fornire pareri in merito** alla valutazione dell'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- d) **Cooperare** con l'Autorità di controllo;
- e) **Fungere da punto di contatto per l'Autorità di controllo** per questioni connesse al trattamento. L'attività viene svolta mediante visite annuali in occasione delle quali sono redatte specifiche relazioni per documentare le attività svolte.

Considerando il ruolo strategico ricoperto dal DPO, in base alle indicazioni fornite dal Garante per la protezione dei dati personali e secondo i principi dell'*accountability* (ex art. 24 GDPR), **la nomina del DPO dovrebbe essere pluriennale** in modo da consentire una conoscenza approfondita dell'Ente e delle sue peculiarità.

La continuità dell'operato del Responsabile per la protezione dei dati personali è garanzia di stabilità delle scelte dell'Ente e di maggiore efficacia nella gestione degli adempimenti.



Formazione inclusa nel servizio

Corso n. 1 dal titolo: **"Come attuare lo smart working nella PA nel rispetto della Privacy"** - Corso online in diretta - durata n. 2 ore
Vedi il programma del corso a pag. 5.

2

SUPPORTO SPECIALISTICO PER L'ATTUAZIONE DEL NUOVO REGOLAMENTO EUROPEO 2016/679 IN MATERIA DI PRIVACY

Servizio onsite e online

Dopo l'affidamento dell'incarico, il professionista nominato da Maggioli, in accordo con il cliente, realizza sopralluoghi conoscitivi presso l'Ente e riunioni per la creazione del gruppo di lavoro (responsabili della segreteria, del personale, del CED, della Polizia Locale, ecc).

Il cliente avrà accesso ad una **piattaforma interattiva online** per la gestione degli adempimenti e per lo scambio di informazioni con i professionisti incaricati Maggioli.

Il servizio prevede l'analisi delle misure e delle metodologie tecniche e gestionali che l'Ente adotta nel trattamento dei dati inerenti a:

- > attività istituzionali
- > attività svolte presso sedi operative gestite direttamente dall'Ente (case di riposo, musei, asili, scuole, ecc.)
- > utilizzo sistemi di videosorveglianza
- > verifica adeguatezza del sito web.

Il servizio prevede sia visite presso l'Ente per la rilevazione delle informazioni, che attività svolte in back-office per lo svolgimento delle seguenti attività con la cronologia indicata.

NOVITÀ

Formazione inclusa nel servizio

Corso n. 1 dal titolo: **"Come attuare lo smart working nella PA nel rispetto della Privacy"** - Corso online in diretta - durata n. 2 ore
Vedi il programma del corso a pag. 5.

A) ACQUISIZIONE DELLE INFORMAZIONI

1. **Mappatura degli archivi elettronici** (web e cartacei), individuazione e definizione degli schemi di trattamento dei dati rispetto alle singole unità di archiviazione;
2. **Verifica della liceità dei trattamenti**, delle modalità tecniche e delle misure di protezione adottate;
3. **Individuazione dei soggetti interessati al trattamento** (utenti, cittadini, persone fisiche e referenti delle persone giuridiche, dipendenti/collaboratori, fornitori, etc.);
4. **Individuazione delle figure gerarchiche di responsabilità** quali:
 - > titolare del trattamento;
 - > affidatari esterni (convenzioni con altri Enti) e/o cotitolari;
 - > responsabili esterni del trattamento/clausole per l'affidamento di servizi esternalizzati;

- > amministratori di sistema;
- > soggetti che operano sotto l'autorità del titolare e del responsabile con specifici compiti e funzioni;

B) ELABORAZIONE DEI DOCUMENTI

Il servizio prosegue con la predisposizione e la personalizzazione di procedure e documentazione che saranno pianificate previa consulenza specifica in base alle reali esigenze dell'Ente. Si precisa che le attività saranno svolte in back-office con il coinvolgimento dell'Ente attraverso contatti telefonici e mail ed in occasione delle videoconferenze interattive

1. Redazione delle **informative** per il trattamento dei dati;
2. individuazione dei criteri per la verifica dei requisiti dei **fornitori** di servizi per i quali vi è un trattamento (e/o implementazione di misure di protezione dei dati) e stesura delle clausole contrattuali minime per garantire l'adeguata protezione dei dati;
3. **predisposizione dei registri** delle attività di trattamento;
4. revisione **dell'analisi dei rischi che incombono sui dati**;
5. **individuazione e verifica dei criteri per l'adozione di idonee misure tecnico - organizzative**;
6. verifica implementazione delle misure **"minime di sicurezza informatica** per le Pubbliche Amministrazione" emanate dall'AgID (Direttiva 1/8/2015 e Circolare n 2/2017);
7. definizione delle modalità di gestione degli adempimenti relativi al Provvedimento a carattere generale del Garante per la protezione dei dati personali sulla figura dell'**Amministratore di sistema**;
8. verifica del **sito internet** ed implementazione dei conseguenti adempimenti (indicazioni delle modalità e testi per le informative, cookie law, privacy policy, form di raccolta dati ecc);
9. verifica delle modalità di gestione su trasparenza, regolamenti, geolocalizzazione, dati biometrici, videosorveglianza in ottemperanza al Provvedimento del Garante dell'8 aprile 2010;
10. eventuali integrazioni di aspetti giuslavoristici sull'utilizzo degli strumenti di lavoro aziendali in affidamento al personale dipendente;
11. verifica ed eventuale integrazione del Regolamento per il trattamento dei dati personali in recepimento del GDPR;
12. adempimenti per il trattamento dati nell'ambito dell'erogazione dei servizi socio-sanitari.

Il servizio termina con l'illustrazione e la consegna della documentazione predisposta.

Per rispondere al meglio alle esigenze dell'Ente, tutto il materiale verrà integrato ed aggiornato anche in base a modifiche intervenute al dettato normativo di riferimento.

3

LAVORO AGILE (o SMART WORKING) Supporto specialistico per la gestione degli adempimenti in materia di Privacy Servizio online



L'introduzione di norme d'emergenza per il contenimento ed il contrasto della pandemia di COVID-19, ha comportato importanti ricadute anche in ambito di protezione dei dati poiché gli Enti hanno dovuto implementare nuove misure organizzative e tecniche al fine di rendere i trattamenti di dati, anche di tipo sanitario, conformi al Regolamento Europeo 2016/679.

L'utilizzo delle modalità di **lavoro agile/smart working** rende necessaria la verifica del rispetto delle regole sulla protezione dei dati poiché comportano l'introduzione di nuove minacce sulla sicurezza dei dati personali, derivanti sia dal luogo di lavoro domestico, che dalle nuove modalità tecniche di connessione.

Il Regolamento UE 2016/679 (GDPR) prescrive l'adozione di adeguate misure di sicurezza tecniche organizzative (dette anche "contromisure") in grado di ridurre ad un livello accettabile il nuovo scenario di "rischio" derivante dalle nuove modalità di lavoro agile così come previsto dall'art. 25 e dall'art. 32 GDPR.

Il servizio offerto:

Dopo l'affidamento dell'incarico, il consulente incaricato Maggioli, in collaborazione con il cliente, raccoglierà i dati nonché eventuali informazioni e materiale necessario per impostare la documentazione oggetto del servizio. La raccolta di informazioni potrà avvenire mediante contatti telefonici, compilazione di check list, accesso ai documenti pubblicati sul sito dell'ente, materiale inviato via mail ecc.

Il cliente avrà accesso ad una piattaforma online riservata interattiva per la gestione online degli adempimenti previsti e per lo scambio di informazioni con i consulenti incaricati Maggioli.

Il servizio prevede sia **incontri online** per la rilevazione delle informazioni sia **attività svolte in back-office** per l'elaborazione dei documenti e per la successiva pubblicazione dei documenti sulla piattaforma online.

LE FASI DEL SERVIZIO

Il servizio prevede lo svolgimento delle seguenti attività:

1. Adozione misure organizzative

- › Adozione di politiche adeguate per lo smart working (personalizzate in base alle reali esigenze del cliente ed alle modalità di lavoro adottate) (art. 24 GDPR);
- › Istruzioni integrative per il trattamento dati rivolte al personale dipendente e collaboratori (art. 29 GDPR, art. 2 quaterdecies D.Lgs. n. 196/2003;

- › Check list per la realizzazione di audit, revisione e rafforzamento delle clausole con i fornitori di servizi di informatica/webmaster (art. 28 GDPR);
- › Integrazione delle informazioni sul trattamento dati fornite ai dipendenti a fronte delle modalità di smart working (art. 13 GDPR);
- › Revisione della valutazione del rischio e misure di sicurezza - privacy by design, limitatamente per i trattamenti dati relativi al servizio in oggetto (art. 25 e art 32 GDPR);
- › Aggiornamento del registro delle attività del trattamento, limitatamente ai trattamenti dati relativi al servizio in oggetto (art. 30 GDPR);
- › Eventuale revisione della valutazione di impatto per utilizzo nuove tecnologie per lo smart working (Art. 35 GDPR);
- › Se predisposte, revisione delle procedure per le violazioni dei dati personali - data breach limitatamente ai trattamenti dati relativi al servizio in oggetto (art. 33 e 34 GDPR);
- › Informazioni sul trattamento dei dati e designazioni in caso di utilizzo di piattaforme per la gestione di videoconferenze.

Formazione

Corso n. 1 dal titolo: **"Come attuare lo smart working nella Pa nel rispetto della Privacy"** - Corso online in diretta - durata n. 2 ore

Il corso è rivolto a tutti i dipendenti di qualsiasi mansione che operano o dovranno operare in smart working.

Vedi il programma del corso a pag. 5.

Oltre all'attività formativa è prevista l'illustrazione delle procedure e dei documenti progettati che saranno caricati sul portale costituenti l'oggetto del servizio, tale illustrazione è rivolta unicamente al personale che collaborerà al reperimento delle informazioni e gestirà le attività successive.

L'attività formativa sarà realizzata in occasione delle videoconferenze contrattualizzate per l'espletamento del servizio.

2. Applicazione delle misure tecniche organizzative di sicurezza sulla base di linee guida nazionali ed europee

- › WP 29 - "Opinion 2/2017 on data processing at work", adottato l'8 giugno 2017
- › Raccomandazioni Cert-PA - AgID del 17/03/2020 "Vademecum per lavorare online in sicurezza", n. 11 raccomandazioni per aiutare i dipendenti pubblici a utilizzare in maniera sicura pc, tablet e smartphone personali quando lavorano da casa.
- › Linee guida ENISA del 02/6/2020 per la sicurezza informatica e lo smart-working durante il COVID (Agenzia dell'Unione Europea per la Cybersecurity)

3. Cybersecurity Test

- › Test sulla sicurezza informatica dell'indirizzo IP pubblico utilizzato per le connessioni dall'esterno della rete informatica dell'Amministrazione. Risultato del test mediante report tecnico.

4

SUPPORTO SPECIALISTICO PER I TRATTAMENTI DEI DATI RELATIVI ALLO SVOLGIMENTO DELLE ATTIVITÀ DI VIDEOSORVEGLIANZA DELLA POLIZIA LOCALE

Servizio onsite e online

In seguito all'introduzione della Direttiva n. 680/2016 e all'entrata in vigore del D.Lgs. n. 51/2018, dall'8 giugno 2018 è a regime la normativa in materia di trattamento dei dati personali per le **attività di indagine di polizia giudiziaria** svolte con l'ausilio degli strumenti di videosorveglianza urbana (telecamere, videotrappole, bodycam, autovelox, ZTL, ecc). Il servizio, che potrà essere svolto on site o da remoto, prevede la **predisposizione del regolamento** specifico e la **valutazione dei rischi** in riferimento all'articolo 25 del GDPR, nonché la **valutazione d'impatto** in riferimento all'articolo 35 del GDPR.

Il servizio include l'accesso ad una **piattaforma online interattiva** per la gestione degli adempimenti e per lo scambio di informazioni con i consulenti incaricati Maggioli.

Sono previste le seguenti attività:

- › Predisposizione di **informative** brevi (cartelli) ed informative complete ai sensi dell'articolo 13 e 26 del GDPR;
- › **Individuazione dei compiti**, funzioni, istruzioni e predisposizione di specifici accordi di riservatezza rivolti ai soggetti autorizzati al trattamento dati;

5

SERVIZI SPECIALISTICI AGGIUNTIVI

Servizio onsite e online

È possibile richiedere i seguenti servizi aggiuntivi con preventivi su richiesta:

- › **Organizzazione di corsi per la formazione obbligatoria** (di base e/o specifici) presso l'Ente per gli addetti autorizzati al trattamento dati, con rilascio di attestato di partecipazione valido ai fini di legge;
- › **Organizzazione di corsi per la formazione dedicata alle figure apicali** o loro referenti con analisi delle tematiche afferenti alla privacy, con particolare riferimento alle responsabilità del **Sindaco, del Segretario Comunale e delle Posizioni Organizzative**;
- › **Organizzazione di incontri formativi-operativi**, finalizzati a garantire il confronto fra i referenti/coordinatori di più Enti logisticamente vicini e con problematiche simili nella gestione materiale della documentazione e del trattamento dati. I laboratori avranno un taglio fortemente tecnico-operativo con la risoluzione di casi pratici.
- › **Privacy check documentale**: il servizio a distanza si rivolge agli Enti che necessitano di una verifica della documentazione utilizzata e delle procedure adottate nel rispetto del Regolamento UE 2016/679.

- › **Individuazione di eventuali ruoli di cotitolarità** (articolo 26 GDPR) desumibili da convenzioni stipulate con altri Enti o organi dello Stato;
- › Designazione e redazione di idonee istruzioni ai soggetti responsabili del trattamento;
- › **Redazione di una procedura** e creazione di un modello organizzativo per l'utilizzo dell'impianto di videosorveglianza (articolo 24 del GDPR);
- › **Redazione di un piano di audit** per la verifica della corretta applicazione delle procedure che prevede un riesame periodico;
- › Implementazione di una procedura specifica per la **registrazione degli incidenti di sicurezza** nonché per la gestione di una violazione di dati personali (**data breach**);
- › **Redazione di un piano di formazione** per gli addetti al trattamento dati;
- › Integrazione dello specifico trattamento dati derivante dall'impianto di videosorveglianza all'interno del registro delle attività del trattamento in capo al Titolare del trattamento (art. 30 GDPR);
- › Integrazione dello specifico trattamento dati derivante dall'impianto di videosorveglianza all'interno del registro delle attività del trattamento in capo all'Ente in qualità di Responsabile del trattamento (art. 30 GDPR);
- › Verifica e/o **stesura di convenzioni** stipulate con altri Enti o organi dello Stato nonché per eventuali connessioni con soggetti privati.

Il servizio termina con l'illustrazione e la consegna della documentazione predisposta.

- › **Audit periodici di verifica dell'adozione delle misure predisposte in ottemperanza al GDPR.**

L'attività ha l'obiettivo di misurare la conformità di determinati sistemi, processi o documenti alle norme e verificarne l'effettiva applicazione. Gli audit potranno essere di tre tipi:

- **interni di prima parte** - verifiche effettuate sulle procedure adottate dall'Ente
- **esterni di seconda parte** - verifiche eseguite sui partner dell'Ente (fornitori) quali i responsabili del trattamento
- **audit di terza parte** realizzati in collaborazione con Enti di certificazione accreditati.

Per tutti i servizi sopra indicati verrà rilasciata una relazione scritta contenente le risultanze dell'audit, le osservazioni, le non conformità insieme agli spunti/suggerimenti di miglioramento.

- › **Affiancamento all'Ente in sede di verifiche o ispezioni da parte delle Autorità di controllo** (Garante della Privacy).
- › **Servizio Data Entry dati privacy**. Il servizio è pensato per gli Enti che necessitano di un supporto operativo per l'inserimento dei dati afferenti alla normativa privacy all'interno di gestionali, applicativi o portali.

Il servizio viene svolto mediante personale esperto nell'utilizzo di strumenti hardware e software e oltre, a garantire la verifica dei dati forniti nonché l'esattezza dei documenti personalizzati, consente di ottimizzare il lavoro delle risorse interne che potranno così concentrarsi sulle loro quotidiane attività.

LA FORMAZIONE Corsi di formazione online in diretta

1 COME ATTUARE LO SMART WORKING NELLA PA NEL RISPETTO DELLA PRIVACY Corso online in diretta durata n. 2 ore

L'emergenza COVID 19 ha introdotto nuove modalità lavorative per tutti i dipendenti della Pubblica Amministrazione. La direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica, nonché i successivi DPCM emanati a seguito dell'emergenza COVID-19 prevedono l'utilizzo dello smart working, ed in particolare che il dipendente pubblico possa utilizzare propri dispositivi per svolgere la prestazione lavorativa, purché siano garantiti adeguati livelli di sicurezza e protezione della rete secondo le esigenze e le modalità definite dalle singole pubbliche amministrazioni. La formazione ricopre un ruolo fondamentale per istruire i dipendenti sui nuovi scenari operativi, a fronte dei rischi privacy che incombono per effetto delle nuove tecnologie. Il Reg. UE 2016/679 GDPR qualifica la formazione come "strumento" per la sicurezza dei trattamenti dati di cui all'art. 32 del GDPR, pertanto la rende obbligatoria.

A chi è rivolto:

a tutti i dipendenti di qualsiasi mansione che operano o che dovranno operare in smart working

Argomenti trattati:

- > I principi fondamentali del GDPR, dall'accountability alla sicurezza del trattamento dei dati
- > Le indicazioni dell'AGID per uno smart working sicuro
- > Istruzioni e modalità organizzative dell'amministrazione per l'utilizzo degli strumenti di smart working
- > Utilizzo consapevole delle piattaforme per effettuare video conferenze

2 FORMAZIONE DI BASE SUGLI ADEMPIMENTI DEL REGOLAMENTO UE 2016/679 PER L'INDIVIDUAZIONE ED ASSEGNAZIONE DEI RUOLI DI RESPONSABILITÀ ALL'INTERNO DELL'ENTE LA COSTITUZIONE DI UN "PRIVACY TEAM" Corso online in diretta durata n. 2 ore

Il concetto di consapevolezza e di responsabilizzazione di cui all'art. 24 del GDPR, è ancora il primo principio che purtroppo nella Pubblica Amministrazione non viene applicato così come si rileva anche nei recenti provvedimenti sanzionatori emessi dal Garante della Protezione dei dati personali.

Il corso di formazione ha come obiettivo la costruzione del sistema delle responsabilità in merito ai trattamenti dati a partire dalle funzioni apicali, fino ai dipendenti che svolgono le loro mansioni.

Il corso prevede il rilascio di modelli organizzativi e bozze di documenti per la costruzione di un gruppo di lavoro generalmente chiamato "Privacy Team", oltre alla metodica per condurre gli audit interni.

A chi è rivolto:

ai dirigenti, posizioni organizzative e dipendenti con incarichi specifici in qualità di "referenti privacy", CED, amministratori di sistema e tutti i dipendenti che

l'amministrazione ritiene debbano essere edotti sulle responsabilità in merito al trattamento dei dati.

Argomenti trattati:

- > I principi fondamentali del Reg. (UE) 2016/679 (GDPR) in merito alla responsabilizzazione e la predisposizione di politiche adeguate per dimostrare la compliance al regolamento,
- > Come effettuare la progettazione dei compiti, funzioni ed istruzioni adeguate per ciascun ruolo all'interno della PA, al fine di assegnare le dovute responsabilità,
- > Costituzione del gruppo di lavoro per la conduzione degli adempimenti e delle relative verifiche di applicazione del GDPR.
- > Esempi di casi pratici.

3 INDICAZIONI ED ISTRUZIONI OPERATIVE PER LE PUBBLICAZIONI DA EFFETTUARE NELL'AREA "AMMINISTRAZIONE TRASPARENTE" DEL SITO INTERNET DELL'ENTE LOCALE (EX D.LGS. N. 33/2013) NEL RISPETTO DELLA PRIVACY Corso online in diretta durata n. 2 ore

Il corso formativo ha come obiettivo la comprensione del "bilanciamento fra trasparenza amministrativa e rispetto dei diritti e libertà delle persone" al fine di acquisire le modalità corrette per la pubblicazione dei contenuti sul sito web dell'Ente. I recenti provvedimenti sanzionatori emanati da parte dell'Autorità Garante per la protezione dei dati personali a carico degli Enti locali a seguito della pubblicazione errata di atti, documenti ed informazioni ha messo in evidenza l'esigenza di formare tutti i dipendenti, a partire dalle posizioni apicali fino ai dipendenti che snello svolgimento della propria mansione sono abilitati alla pubblicazione dei documenti nell'area trasparenza del sito web dell'Ente. Durante il corso saranno esaminate le linee guida per la corretta pubblicazione, saranno analizzati dei casi pratici e verificati in diretta i contenuti presenti sul sito dell'ente.

A chi è rivolto:

ai dirigenti, alle posizioni organizzative, ai dipendenti con incarichi specifici in qualità di "referenti privacy", CED, amministratori di sistema e tutti i dipendenti che l'amministrazione ritiene debbano essere edotti sulle responsabilità in merito alla pubblicazione dei dati in area trasparenza.

Argomenti trattati:

- > I principi fondamentali del Reg. (UE) 2016/679 (GDPR) e del Codice D.Lgs. n. 196/2003 così come modificato dal D.Lgs. n. 101/2018 che disciplinano i trattamenti dati per la trasparenza amministrativa.
- > Le linee guida sulla trasparenza amministrativa.
- > Metodologie di analisi, procedure e documenti utili per la gestione delle pubblicazioni a norma di legge.
- > Esempi di casi pratici.