Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

Allegato

Checklist di base per

GLI STUDI PROFESSIONALI

Aprile 2018

Indice

Categorie di dati personali ed interessati coinvolti 1°	Specificare tutti gli elementi inclusi nel trattamento per ciascuna categoria 2°	Fonte dei dati personali 3°	Scopo del trattamento dati personali 4°	Base giuridica per ciascun scopo (categorie non speciali di dati personali) 5°	Categorie speciali di dati personali 6°	Base giuridica per il trattamento di categorie speciali di dati personali 7°	Periodo di conservazione 8°	Azioni richieste per la conformità al GDPR 9°
Elencare le categorie di interessati e dati personali raccolti e conservati, ad es. dati relativi al personale attivo di ufficio ed in congedo; dati relativi alla clientela (es. informazioni sui servizi dallo studio, ecc.)	*Elencare ciascun tipo di dati personali inclusi all'interno di ciascuna categoria di dati personali, ad es. nome, indirizzo, eventuali dettagli bancari, cronologia dei servizi acquistati, cronologia di navigazione online, immagini di spese sostenute, atti inerenti la persona, ecc.).* *È importante tracciare anche il flusso dei dati personali trattati.*	*Elencare la (e) fonte (i) dei dati personali e se sono raccolti direttamente o da terze parti*	*All'interno di ciascuna categoria di dati personali, indicare gli scopi per i quali dati vengono raccolti e conservati, ad es. esecuzione del contratto, marketing, miglioramento del servizio, ecc)*	*Per ogni scopo per il quale vengono trattati i dati personali, elencarne la base giuridica su cui si basa* *ad es. consenso, contratto, basi legali (articolo 6 GDPR).*	*Se vengono raccolte e trattati speciali categorie di dati personali,* *specificarne i dettagli sulla natura dei dati, ad es. dati sanitari, genetici, biometrici.*	*Elencare la base giuridica per la quale sono trattati categorie speciali di dati personali, ad es. consenso esplicito, liceità art. 9 GDPR.*	*Per ogni categoria di dati personali, elencare il periodo per il quale i dati saranno conservati.* *Come regola generale, i dati devono essere conservati per un periodo non superiore a quello necessario per lo scopo per il quale sono stati raccolti originariamente*	*Identificare le azioni necessarie per garantire che tutte le operazioni di trattamento dei dati personali siano conformi a GDPR, ad es. cancellazione dei dati laddove non vi siano ragioni in linea con lo scopo originario per conservarle.*

1. Dati Personali trattati

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trattamenti basati sul consenso (Art. 7, 8, 9)	Si sono esaminati i meccanismi di Studio per la raccolta del consenso per garantire che la richiesta di consenso venga presentata in modo chiaramente distinguibile dalle altre materie (es. in una pagina distinta ed a parte del contratto di consulenza), in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro?			
	Se i dati personali che attualmente si trattano in base al consenso non soddisfano quanto richiesto ai sensi del GDPR, lo studio ha proceduto a richiedere nuovamente il consenso dell'interessato per garantire la conformità al GDPR?			
	Esistono procedure di Studio per dimostrare che una persona ha acconsentito al trattamento dei propri dati personali?			
	Esistono procedure per consentire ad una persona di revocare il proprio consenso al trattamento dei propri dati personali?			
Dati personali dei minori (Art. 8)	Qualora vengano forniti servizi online ad un minore, esistono procedure per verificare l'età e ottenere il consenso di un genitore / tutore legale, ove richiesto?			
Trattamenti basati sul legittimo interesse	Se l'interesse legittimo è una base giuridica su cui vengono trattati i dati personali, è stata effettuata un'analisi appropriata per garantire che l'uso di questa base giuridica sia appropriata? Tale analisi deve dimostrare che 1) esiste un valido interesse legittimo, 2) il trattamento dei dati sia strettamente necessario per perseguire l'interesse legittimo, e 3) il trattamento non sia pregiudizievole ovvero non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento.			

2. Diritti degli interessati

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Diritto di accesso ai dati personali (Art. 15)	Esiste una politica / procedura documentata per la gestione delle richieste di accesso ai propri dati personali da parte dell'interessato?			
	Lo Studio è organizzato a rispondere entro un mese?			
Portabilità dei dati (Art. 20)	Esistono procedure per fornire agli interessati i loro dati personali in un formato strutturato, comunemente usato e leggibile da un dispositivo?			
Diritto di rettifica e di cancellazione (Art. 16 e 17)	Esistono controlli e procedure per consentire la cancellazione (oblio) o la rettifica dei dati personali (ove applicabile)?			
Diritto alla limitazione di trattamento (Art. 18)	Esistono controlli e procedure per cessare il trattamento dei dati personali laddove un interessato abbia, per motivi validi, richiesto la limitazione del trattamento?			
Diritto di opposizione (Art. 21)	Gli interessati al trattamento sono informati del loro diritto di opporsi all'effettuazione di determinati tipi di trattamento (come per il marketing diretto)?			
	Esistono controlli e procedure per cessare il trattamento dei dati personali quando l'interessato si è opposto al trattamento?			
Profilazione e processi automatizzati (Art. 22)	Se lo studio utilizza un processo decisionale automatizzato, che ha un impatto legale o significativo per l'interessato, il trattamento è basato sul consenso, ed è stato raccolto con un consenso esplicito?			
	Quando viene presa una decisione automatizzata che è necessaria per stipulare o eseguire un contratto, o in base al consenso esplicito di un dell'interessato, esistono procedure per facilitare il diritto dell'interessato ad ottenere l'intervento umano e di poter contestare la decisione?			

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Limitazioni (Art. 23)	Sono stati chiariti all'interessato le ipotesi di limitazioni ai propri diritti e libertà fondamentali previste dall'art. 23 GDPR (es. prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica)?			

3. Accuratezza e conservazione

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Scopo limitato	I dati personali vengono utilizzati solo per gli scopi per i quali sono stati originariamente raccolti?			
Minimizzazione del dato	I dati personali raccolti sono limitati a quanto necessario per gli scopi per cui sono trattati?			
Accuratezza	Sono in atto procedure per garantire che i dati personali siano aggiornati e precisi e dove è necessaria una correzione, le modifiche necessarie sono apportate senza ritardi?			
Conservazione	Sono in atto politiche e procedure di conservazione per garantire che i dati personali siano conservati per un periodo non superiore a quello necessario per gli scopi per cui sono stati raccolti?			
	Lo studio è soggetto ad altre regole che richiedono un periodo minimo di conservazione (ad esempio documenti fiscali da mantenere per i dieci anni civilisticamente previsti: quantificare con il cliente anche i relativi costi di conservazione e la reale necessità di mantenerli in archivio di studio o se possibile di restituirli al cliente ed in che modalità)?			
	Sono attuate procedure per garantire che i dati personali vengano distrutti in modo sicuro, in conformità con le politiche di conservazione?			
Duplicazione delle informazioni	Esistono procedure per garantire che non vi siano duplicazioni inutili o non regolamentate dei dati personali raccolti e trattati?			

4. Requisiti di trasparenza

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trasparenza verso clienti e dipendenti (Art. 12, 13 e 14)	I dipendenti ed i collaboratori di studio ed i clienti sono pienamente informati sul come si utilizzino i propri dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile utilizzando un linguaggio chiaro e trasparente?			
	Esistono policy di studio chiare sull'utilizzo degli strumenti informatici utilizzati?			
	Laddove i dati personali siano raccolti direttamente presso l'interessato, sono in atto procedure per fornire le informazioni elencate all'art. 13 del GDPR (il personale di studio è all'uopo istruito)?			
	Se i dati personali non sono raccolti direttamente dall'interessato ma da una terza parte (ad esempio da un altro Professionista) sono in atto procedure per fornire le informazioni elencate all'Art. 14 del GDPR?			
	Quando si interagisce con gli interessati, ad esempio quando si fornisce un servizio personalizzato derivante da profilazione o si utilizza un Sistema di videosorveglianza, esistono procedure per informare proattivamente gli interessati dei loro diritti conformemente al GDPR?			
	L'interessato ha avuto ed ha disponibilità di capire come poter esercitare i propri diritti GDPR nei confronti dello studio con informativa in un formato facilmente accessibile e leggibile?			

5. Altri obblighi del titolare

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Accordi con i fornitori (Art. 27 a 29)	Sono stati esaminati accordi con fornitori e altre terze parti che trattano dati personali per conto dello Studio al fine di garantire che siano inseriti tutti i requisiti di protezione dei dati in modo adeguato?			
Data Protection Officer (DPO) – Responsabile della protezione dei dati personali (Art. 37 a 39)	Si è valutato se si è obbligati o meno come Studio a nominare un DPO (ex Art. 37 GDPR)? Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala (che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato) qualora riguardi dati personali di clienti da parte di un singolo professionista.			
	Se si decide che un DPO non è obbligatorio per lo studio, si è proceduto ad archiviarne i motivi?			
	Se si decide che un DPO vada nominato, è prevista una procedura per il reporting al dominus di Studio? Queste procedure sono documentate?			
	Sono stati resi noti i dettagli di contatto del DPO di Studio affinché clienti, dipendenti e collaborator, possano prendere agevolmente contatto con lui?			
Data Protection Impact Assessment (DPIA) (Art. 35) o valutazione di impatto	Se il trattamento dei dati personali è considerato ad alto rischio, esiste in studio un processo per identificare la necessità di effettuare una valutazione di impatto? Queste procedure sono documentate?			

6. Sicurezza del trattamento

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Adeguate misure di sicurezza tecniche ed organizzative (Art. 32) Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e	Lo studio ha valutato i rischi associati al trattamento dei dati personali effettuati e messo in atto misure adeguate per mitigarli? Ne ha messo anche da parte la relative documentazione?			
	Esiste un programma di sicurezza documentato che specifichi le misure tecniche, organizzative e logiche per un trattamento dei dati personali conforme al GDPR?			
	Dipendenti e collaboratori di studio sono stati adeguatamente formati sui rischi generali e specifici dei trattamenti di dati, sulle misure organizzative, tecniche ed informatiche adottate in studio, nonché sulle responsabilità e sulle sanzioni?			
	Esiste un processo documentato per la risoluzione di reclami e di problemi relativi alla sicurezza?			
	Esiste una persona di Studio che sia designata quale responsabile della prevenzione e delle indagini sulle violazioni della sicurezza (c.d data breach)? È stata valutato questo ruolo?			
	Sono utilizzate per trasferire, archiviare e ricevere informazioni personali riservate degli interessati tecnologie crittografiche?			
	Quando non è più necessaria la conservazione dei dati personali trattati, gli stessi, vengono distrutti, cancellate o anonimizzati? Gli interessati ne sono consapevoli?			
	L'accesso ai dati personali può essere ripristinato tempestivamente in caso di incidente fisico o tecnico?			

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.				

7. Data breaches (violazione dei dati personali)

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Obblighi di risposta alla violazione dei dati personali (Art. 33 e 34)	Lo studio ha un piano di risposta agli incidenti sulla sicurezza e sulla privacy che sia documentabile?			
	Questi piani e relative procedure vengono riesaminate in modo periodico?			
	Esistono procedure per notificare al Garante Privacy una violazione dei dati?			
	Esistono procedure per notificare agli interessati (qualora ne ricorrano i presupposti) una violazione dei dati?			
	Esiste piena documentazione di tutte le violazioni subite?			
	Esistono procedure di cooperazione tra i titolari del trattamento dei dati in ufficio, i fornitori ed altri partner per far fronte alle violazioni dei dati?			

8. Trasferimento dati personali (Extra europeo) – qualora applicabile

	QUESITO	SÌ	NO	COMMENTI/AZIONI DI RIMEDIO
Trasferimenti internazionali di dati personali (Art. 44 a 50)	I dati personali sono trasferiti al di fuori dell'Europa, ad es. negli Stati Uniti o in altri paesi?			
	Il trasferimento include percaso anche particolari categorie di dati (es. dati sensibili)?			
	A che scopo viene effettuato il trasferimento?			
	A quale soggetto sono trasferiti tali dati personali?			
	Esiste un elenco complete di tutti i trasferimenti eventualmente effettuati? comprese le risposte ai quesiti precedenti (ad esempio, la natura dei dati, lo scopo del trattamento, da quale Paese i dati vengono esportati e quale Paese riceve i dati e chi è il destinatario del trasferimento?)			
Trasferimenti internazionali leciti	Esiste una base legale per il trasferimento? (ad es. Decisione sull'adeguatezza della Commissione europea; clausole contrattuali standard). Queste basi sono documentate?			
Trasparenza	Gli interessati sono pienamente informati di eventuali trasferimenti internazionali previsti dei loro dati personali?			