

GUIDA OPERATIVA REGOLAMENTO PRIVACY

Questo documento vuole essere uno strumento a disposizione degli iscritti per applicare nella realtà dello studio professionale il nuovo Regolamento Europeo sulla protezione dei dati, conosciuto anche come GDPR.

INTRODUZIONE

Il Regolamento generale sulla protezione dei dati è l'innovazione più significativa apportata negli ultimi anni in materia di protezione dei dati personali, non solo a livello dell'Unione Europea ma a livello globale. Qualsiasi organizzazione che gestisca le informazioni personali dei residenti nell'UE, a partire dal 25 maggio 2018, dovrà adattarsi alla nuova normativa in materia di trattamento dei dati, personali, sicurezza delle informazioni, processi di conformità e relazioni contrattuali.

Le organizzazioni hanno poco tempo per conformarsi al nuovo regolamento.

Ignorare il nuovo regolamento o commettere errori nella sua applicazione può avere conseguenze costose: infatti, alcune violazioni del regolamento sono punibili con sanzioni pecuniarie fino al 4% del fatturato totale annuo dell'azienda o fino ad un massimo di 20 milioni di euro e danneggiare così la reputazione aziendale.

Il regolamento generale sulla protezione dei dati (RGPD), offre un quadro di riferimento in termini di Compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (accountability).

In base al RGPD, alcuni titolari e responsabili del trattamento sono tenuti a nominare un RPD in via obbligatoria. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).

Gli obiettivi principali della Commissione sono quelli di restituire ai cittadini il controllo dei propri dati personali e di semplificare il contesto normativo che riguarda gli affari internazionali, unificando i regolamenti entro l'UE.

Nella tabella qui di seguito si riportano schematicamente le novità del GDPR.

AMBITO DI APPLICAZIONE	
Ambito di applicazione	Il Regolamento si applica a titolari e responsabili stabiliti con le proprie attività nell'Unione Europea o stabiliti al di fuori della UE, ma con attività di trattamento dei dati personali di interessati che si trovano nell'UE
TRATTAMENTO DEI DATI	
Informativa sulla privacy	Deve essere concisa, trasparente, facilmente comprensibile e accessibile per l'interessato. Deve utilizzare un linguaggio chiaro e semplice, in particolar modo se rivolta ai minori, senza inutili rimandi alla normativa. Gli interessati devono sapere se i loro dati sono trasmessi al di fuori dell'UE e con quali garanzie, e che possono esercitare molteplici diritti (es. revoca del consenso per determinati trattamenti, come il marketing diretto).
Consenso	Per i dati sensibili il consenso deve essere "esplicito", così come per il consenso a decisioni basate su trattamenti automatizzati, profilazione compresa. Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è la modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito".
Valutazione d'impatto sulla protezione dei dati	I titolari dovranno effettuare una valutazione degli impatti privacy (Privacy Impact Assessment-PIA) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati. L'assessment privacy è obbligatorio in casi specifici, quali: l'analisi sistematica ed estesa di aspetti personali di individui basata su un trattamento automatizzato, profilazione inclusa, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo significativo sugli individui; il trattamento, su larga scala, di dati sensibili o giudiziari; la sorveglianza sistematica, su larga scala, di una zona accessibile al pubblico. La PIA sostituisce la notifica al Garante per particolari finalità (es. trattamento di dati genetici e biometrici).
Privacy by design e by default	Prima di procedere al trattamento dei dati occorre prevedere le garanzie indispensabili per tutelare i diritti degli interessati, tenendo conto del contesto in cui si colloca il trattamento e dei rischi per i diritti e le libertà degli interessati. Ma non basta: queste attività devono essere specifiche e, soprattutto, dimostrabili in caso di visite ispettive del Garante. Anche la tenuta e l'aggiornamento dei registri dei trattamenti e la valutazione preliminare degli impatti privacy rientrano in questa filosofia.



Misure di Sicurezza	Si passa dal concetto di misure "minime" di sicurezza al concetto di misure "adeguate", quindi molto è lasciato alla responsabilità e alla sensibilità del titolare del trattamento. Lo sforzo tecnico-organizzativo per la messa in sicurezza dei trattamenti deve, comunque, essere proporzionato allo "stato dell'arte" della tecnologia e ai "costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento". Tra le misure di sicurezza applicabili citate dal GDPR ci sono la pseudonimizzazione e la cifratura dei dati personali.
Violazione dei dati	Si estende a tutti la regola della notifica del "data breach" al Garante e, se necessario, all'interessato
Data Protection Officer	La designazione di questa nuova figura è obbligatoria negli enti pubblici e nelle imprese, se impegnate in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, o in trattamenti su larga scala di dati particolari e relativi a condanne penali e reati. Le attribuzioni del DPO vanno da quelle di consulenza a quelle di supervisione. È un interlocutore privilegiato per gli interessati e le autorità di controllo
Registro dei trattamenti	I titolari e responsabili che occupano almeno 250 dipendenti, o che effettuano trattamenti rischiosi per i diritti e le libertà degli interessati, o che trattano dati particolari o dati relativi a condanne penali e reati, sono tenuti ad approntare questi registri. Il contenuto dei registri è indicato all'art. 30 del Regolamento.
DIRITTI DELL'INTERESSATO	
Portabilità dei dati	L'interessato ha la possibilità di ottenere la restituzione dei dati forniti a una azienda o a un servizio online (es. un social network, piattaforme online di vendita di beni e servizi) in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un diverso titolare, se fattibile tecnicamente.
Diritto all'oblio	L'interessato ha il diritto di chiedere di essere completamente "dimenticato" da chi ha raccolto i dati.
SANZIONI	
Sanzioni Amministrative e Penali	È inasprito il regime sanzionatorio amministrativo in caso di violazioni dei dati (fino a € 20 mln e al 4% del fatturato globale), con possibilità di sanzioni penali lasciate ai singoli Stati membri.

COSA DEVO FARE

1. A CHI SI APPLICA?

Ad oggi non ci sono esclusioni. Tutti gli studi professionali, indipendentemente dalle loro dimensioni, sono obbligati ad applicare il GDPR. Tutti gli studi indipendentemente dal target di riferimento, azienda o persona fisica, gestiscono dati personali di almeno tre soggetti:

- _ clienti: referente commerciale, titolare, referente di progetto, amministratore, etc.
- _ fornitori: referente ufficio acquisti, titolare, etc.
- _ dipendenti, se presenti

I dati possono essere semplicemente dati personali (la classica anagrafica), oppure dati giudiziari o sensibili. In base alle tipologie di dati devono essere definite modalità di gestione dei dati più stringenti (armadiature chiuse a chiave, password di accesso a cartelle di rete, ecc.)

2. COSA DEVO FARE?

2.1 INVENTARIO DEI DATI TRATTATI

È necessario creare un documento in cui vengono elencati le tipologie di dati trattati. In particolare:

- _ tipologia dei dati (personale, sensibili, giudiziari)
- _ finalità del trattamento (per fini legali, contrattuali, ecc.)
- _ le modalità di gestione (informatico, cartaceo e con quali strumenti)
- _ chi li gestisce (risorse interne o esterne)
- _ tempi di conservazione

Un semplice foglio Excel può essere lo strumento più idoneo a gestire questo elenco.

2.2 ANALISI DEL RISCHIO DEI TRATTAMENTI

Se il trattamento dei dati prevede l'uso di nuove tecnologie o può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il nuovo regolamento prevede l'effettuazione di una analisi dei rischi utile alla definizione di action necessarie alla riduzione del rischio individuato.

Nell'ipotesi di una gestione ordinaria dei dati da parte di uno studio professionale si reputa non necessaria la valutazione.

Si ritiene utile nel documento dei trattamenti, illustrato precedentemente, riportare una nota a giustificazione della non presenza di rischi che porta alla non redazione della valutazione stessa.

2.3 INFORMATIVA (Già obbligatoria)

Ogni studio deve rivedere l'informativa, già obbligatoria, verso i tre soggetti sopra individuati. L'informativa deve avere almeno queste informazioni:

1. Identità e i dati di contatto del titolare del trattamento. Il Titolare del trattamento può essere lo studio professionale stesso.
2. Dati di contatto del DPO, ove esistente. Per gli studi, in linea di massima, non è obbligatorio nominare questa nuova figura
3. Finalità e base giuridica del trattamento. Normalmente la finalità è l'esecuzione dell'incarico verso il cliente, finalità amministrative contabili verso il fornitore, gestione del rapporto di lavoro verso il dipendente.
4. Eventuali destinatari dei dati personali o le eventuali categorie di destinatari. Se i dati vengono forniti a soggetti terzi vanno indicati. Es. consulente del lavoro, avvocati, ecc.
5. Eventuale trasferimento dei dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (ad esempio, se si tratta di un Paese terzo giudicato adeguato dalla Commissione europea)
6. Periodo di conservazione dei dati o i criteri per stabilire tale periodo.
7. Indicazione dei diritti dell'interessato previsti dal Regolamento.
8. Se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati
9. Se il trattamento comporta processi decisionali automatizzati, compresa la profilazione, e in questi casi le informazioni circa la logica di tali processi decisionali e le conseguenze previste per l'interessato

In allegato un esempio di informativa verso i clienti e i fornitori (ALL-01).

L'informativa può essere un documento separato, integrato nel format contrattuale o in altro documento utilizzato dallo studio.

N.B. Se i dati personali sono trattati a fini contrattuali o per obbligo di legge e sono solo dati personali, NON È NECESSARIO RACCOGLIERE IL CONSENSO e quindi l'informativa può non essere firmata dal soggetto interessato. È invece obbligatorio dimostrare di aver informato i soggetti interessati (mantenere le e.mail di invio delle informative).

Nel caso lo studio invece invii periodiche e.mail di natura commerciale/marketing allora deve essere richiesto **ESPLICITO CONSENSO** predisponendo specifica informativa (ALL.02). L'esempio riportato integra al suo interno anche l'informativa precedente in modo da inviarne una sola ai clienti e l'altra, senza consenso, ai fornitori.

In allegato una informativa per i dipendenti da utilizzare dagli studi che hanno dipendenti nel proprio studio (dipendenti / collaboratori) (ALL.03)

2.4 NOMINE INTERNE (solo per studi con dipendenti con qualsiasi contratto lavorativo). Già obbligatoria

Lo studio deve informare - formare le persone che gestiscono dati personali sulle modalità di TRATTAMENTO DEI DATI. Si possono fare nomine specifiche, come era con il vecchio Codice Privacy, o semplice informazione-formazione. Si allega un esempio di Istruzioni Operative al trattamento dei dati (ALL.04)

2.5 NOMINE ESTERNE. GIÀ OBBLIGATORIE

I soggetti che per motivi contrattuali gestiscono dati personali dei clienti/fornitori/dipendenti dello studio devono essere nominati **RESPONSABILI ESTERNI AL TRATTAMENTO DEI DATI**. Es. consulente del lavoro, collaboratore esterno, software house, ecc.

Per i piccoli studi probabilmente non ci saranno nomine esterne da effettuare.

2.6 NOMINA AMMINISTRATORE DI SISTEMA. GIÀ OBBLIGATORIO

Questa figura, già obbligatoria normalmente viene affidata alla società che esegue l'assistenza sui sistemi informatici. In alternativa può essere lo stesso titolare dello studio o un suo delegato

2.7 SICUREZZA INFORMATICA. GIÀ OBBLIGATORIA

Gli studi devono munirsi di strumenti basici di sicurezza informatica (ANTIVIRUS, SOFTWARE PER LA NAVIGAZIONE IN INTERNET, STRUMENTI DI BACK UP, ECC). In caso di utilizzo di cloud è necessario richiedere informazioni sulla sicurezza informatica al gestore.

In tal senso in allegato (ALL.06) un foglio Excel che permette allo studio di effettuare una analisi sulla sicurezza sia fisica che informatica. Lo strumento fornisce una scala di rischio. Se il rischio risulta rosso lo studio deve fare delle azioni di mitigazione (es. mettere password nelle cartelle dirette, fare back up periodici, fare aggiornamenti software, comprare un antivirus, ecc)

2.8 REGOLE

E' necessario definire una regola su come gestire:

1 data breach: È la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a i dati personali trasmessi, conservati o comunque trattati.

Si tratta di un evento che deve essere affrontato immediatamente e nel modo corretto, perché è necessario evitare qualsiasi danno fisico, materiale e immateriale agli interessati coinvolti: la perdita del controllo dei dati personali o la limitazione dei diritti, la discriminazione, il furto d'identità, danni finanziari, pregiudizi alla reputazione delle persone, la violazione del segreto professionale e simili. In caso di violazione dei dati personali, il responsabile del trattamento è tenuto ad informare il titolare, senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato non è richiesta quando, ad esempio, sono state disposte misure tecniche e organizzative di protezione adeguate (es. cifratura dei dati). Fortunatamente, non tutte le violazioni devono essere notificate all'autorità garante: l'obbligo di notifica scatta se la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone.

Quindi, è bene che i dipendenti e i collaboratori dello studio siano consapevoli dei rischi e si comportino costantemente in modo diligente.

È opportuno quindi redigere una procedura su come comportarsi in caso di violazione dei dati.

2 richiesta per esercitare i diritti degli interessati: i diritti dell'interessati sono stati ampliati rispetto alla vecchia norma. È opportuno definire una regola per la gestione di questi diritti, partendo dalla fattibilità della richiesta, alla gestione e alla comunicazione allo stesso.

Più lo studio è strutturato, più è necessario definire regole, procedure, necessarie a regolare il trattamento dei dati e la loro sicurezza. (Es. regole su come gestire i documenti, regole su come gestire gli strumenti informatici e le cartelle di rete).

2.9 FORMAZIONE E INFORMAZIONE

È obbligatorio formare e informare le risorse interessate alla gestione dei dati (dipendenti).

in tal senso si allega la guida all'applicazione del Modello in materia di Privacy pubblicata dal garante utile come strumento informativo e formativo. (ALL.05)

ALLEGATI

ALL.01 ESEMPIO DI INFORMATIVA

ALL.02 ESEMPIO INFORMATIVA CON CONSENSO

ALL.03 ESEMPIO INFORMATIVA AI DIPENDENTI (per studi che hanno dipendenti)

ALL.04 ESEMPIO ISTRUZIONI OPERATIVE 8per studi che hanno dipendenti)

ALL.05 LINEE GUIDA DEL GARANTE

ALL.06 ANALISI RISCHIO (FOGLIO EXCEL)