STUDIO TECNICO
GIACHINO GEOM. GIUSEPPE
PROGETTAZIONE E SERVIZI TECNICI PER L'EDILIZIA
contrada Pirato sn - 94018 Troina (EN) - tel. e fax: 0935 656179 / 339 1499740
codice fiscale: GCH GPP 61D11 L448 V - p.IVA: 0043 277 086 5
www.giachinogiuseppe.it - info@giachinogiuseppe.it - giuseppe.giachino@geopec.it


# *Come raggiungere la compliance con la privacy europea.*

# GDPR

General Data Protection Regulation

Ebook

Studio Tecnico GIACHINO
www.giachinogiuseppe.it

# *Introduzione*

Il Regolamento Generale sulla Protezione dei Dati (**GDPR**, General Data Protection Regulation - Regolamento UE 2016/679) è un regolamento con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea.

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.

Questo Ebook vuole offrire una panoramica delle novità introdotte dal Regolamento e fornire alcuni spunti per raggiungere la compliance con la privacy europea, **arrivando preparati all'appuntamento di maggio 2018**.

# *Contenuti*

# Cosa cambia con il GDPR?

| Ambito di applicazione | |
|---|---|
| Ambiti più estesi | 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.<br>Deve utilizzare un **linguaggio chiaro e semplice**, in particolar modo se rivolta ai minori, senza inutili rimandi alla normativa.<br><br>È proposto l'utilizzo di icone per rendere l'informativa leggibile anche da parte di chi non conosce la lingua.<br><br>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.<br>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".<br>Il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.<br><br>Il consenso dei **minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. |

# Cosa cambia con il GDPR?

| Trattamento dei dati | |
|---|---|
| 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.<br>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.<br>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.<br>Ma non basta: queste attività devono essere specifiche e, soprattutto, dimostrabili in caso di visite ispettive del Garante.<br>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.<br>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".<br><br>Tra le misure di sicurezza applicabili citate dal GDPR ci sono la pseudonimizzazione e la cifratura dei dati personali. |

# Cosa cambia con il GDPR?

| Trattamento dei dati | |
|---|---|
| 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.<br><br>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. |
| Registri 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.<br>Il contenuto dei registri è indicato all’art. 30 del Regolamento. |

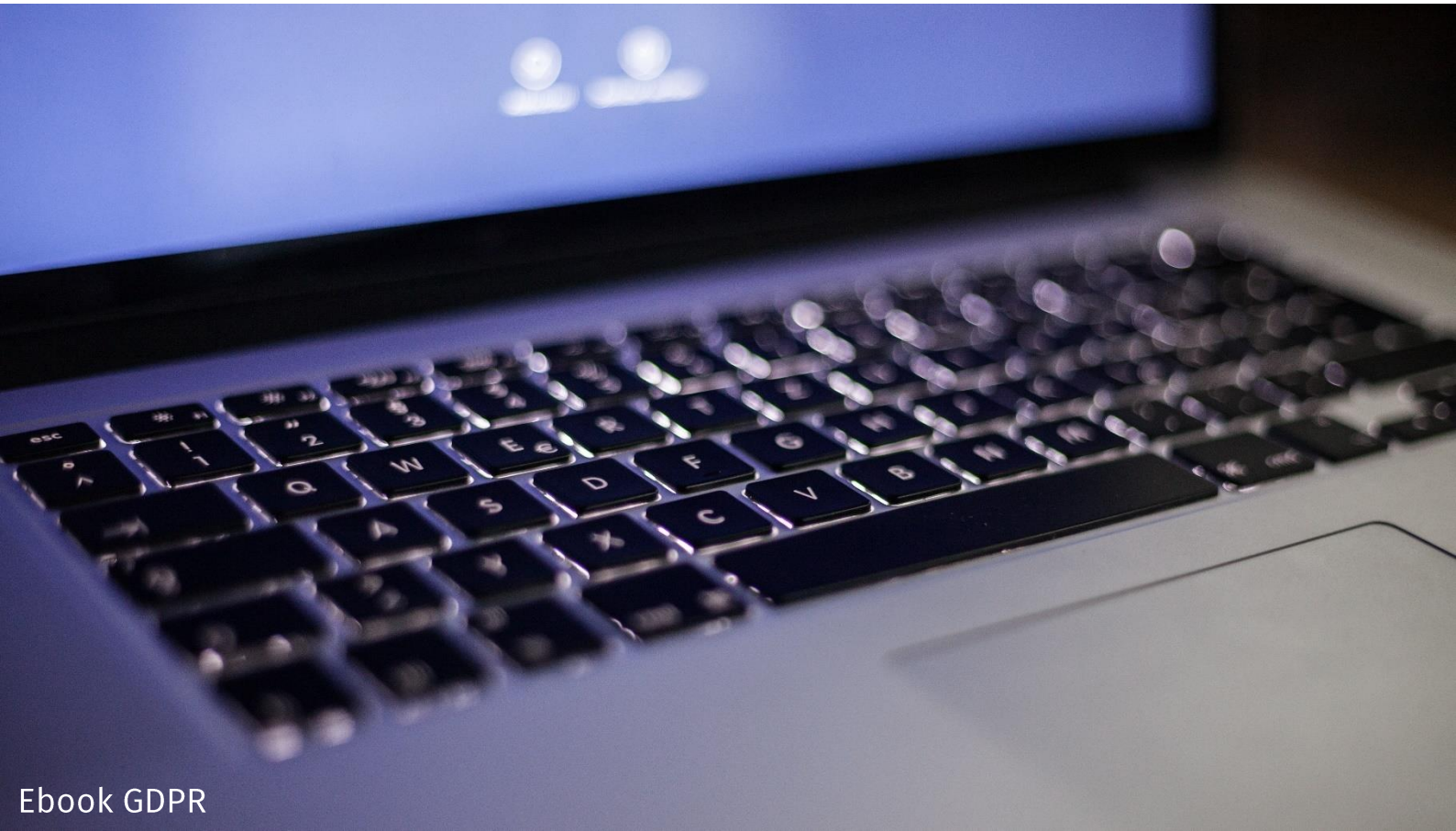
# Cosa cambia con il GDPR?

| Diritto degli interessati | |
|---|---|
| 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. |
| 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. |

# *Impatti sui dati trattati da Studi e Aziende*

Tutte le imprese e gli studi professionali sono costretti a fare i conti con la nuova disciplina, perché ogni giorno trattano una mole considerevole **di dati personali, riferiti ai dipendenti, ai collaboratori, ai clienti e ai fornitori**. Le categorie di dati trattati sono molteplici: dati anagrafici e di contatto dell'interessato, magari corredati della sua fotografia, dati economici e quelli relativi allo stato di salute (definiti "particolari"), e così via.

La protezione dei dati personali da parte del titolare e del responsabile del trattamento deve diventare, sempre di più, uno dei requisiti imprescindibili nella realizzazione e nella fornitura di nuovi prodotti e di nuovi servizi. D'altra parte, la raccolta e l'elaborazione delle informazioni nel rispetto delle regole è la base dei servizi offerti dagli studi professionali e il propellente per generare valore, sia per il professionista che per i suoi clienti.



# *I rischi della non compliance*

I titolari e i responsabili dei trattamenti possono essere colpiti da sanzioni amministrative fino a **20 milioni di euro o fino al 4% del fatturato mondiale** totale annuo.

Ma non esiste soltanto il rischio di sanzioni amministrative o il rischio di danni reputazionali: l'autorità di controllo può anche ordinare la **cancellazione dei dati o la limitazione al trattamento degli stessi,** determinando effetti negativi sul business aziendale.

# *Raccolta del consenso e adeguamento dell'informativa*

Il trattamento dei dati personali è lecito se si fonda, come oggi, su un'idonea base giuridica, che può essere, ad esempio, il consenso rilasciato dall'interessato, o la necessità del titolare di adempiere al contratto di cui l'interessato è parte, oppure la necessità del titolare di adempiere a obblighi di legge.

Per quanto concerne il consenso, questo deve essere libero, specifico, informato e inequivocabile. Non è ammesso, quindi, il consenso tacito o presunto. Nel modulo di raccolta del consenso, la presenza di eventuali caselle precompilate non è ammessa. La richiesta del consenso deve essere chiaramente distinguibile da altre richieste rivolte all'interessato. Quindi, occorre prestare molta attenzione alla modulistica utilizzata.

Se il consenso è già stato raccolto e rispetta i requisiti del Regolamento (deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile") non occorre procedere con una ulteriore richiesta.
Per quanto concerne l'informativa, il Regolamento specifica le caratteristiche: deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; deve utilizzare un linguaggio chiaro e semplice, soprattutto se rivolta ai minori.
L'informativa è data, in linea generale, per iscritto e "*preferibilmente in formato elettronico [...], attraverso un sito web*".

In caso di raccolta presso l'interessato dei dati che lo riguardano, il titolare è tenuto a fornire all'interessato determinate informazioni.

# Raccolta del consenso e adeguamento dell'informativa

## La tua informativa è adeguata? Controlla la presenza di questi elementi.

1. Identità e i dati di contatto del titolare del trattamento
2. Dati di contatto del DPO, ove esistente
3. Finalità e base giuridica del trattamento
4. Se il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi
5. Eventuali destinatari dei dati personali o le eventuali categorie di destinatari
6. 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)
7. Periodo di conservazione dei dati o i criteri per stabilire tale periodo
8. Esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento dei dati che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati
9. Esistenza del diritto di revocare il consenso in qualsiasi momento
10. Diritto di presentare un reclamo all'autorità di controllo
11. 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
12. 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

# *Violazione dei dati: casi pratici e rimedi*

Cos'è la **violazione dei dati (o 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 ai 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.**

La violazione non deve essere tenuta nascosta perché, oltre a esporre il titolare a gravi sanzioni pecuniarie, non consente di scongiurare o limitare i danni per gli interessati.

## Esempi di violazioni di dati personali

- L'invio di una e-mail contenente dati personali alla persona sbagliata
- Un ex-impiegato che accede ai sistemi aziendali con le sue credenziali, non ancora disabilitate
- Una chiavetta USB, contenente i dati personali dei Clienti (in chiaro), persa o dimenticata
- Dimenticare documenti contenenti dati personali alla stampante
- Il furto del portatile (o dello smartphone) aziendale

# *Violazione dei dati: casi pratici e rimedi*

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 dell'impresa o dello studio siano consapevoli dei rischi** e si comportino costantemente in modo diligente e rispettoso delle istruzioni che sono state impartite loro.


Shift
Enter

# La check list sulla privacy

Di seguito si propone una check-list per valutare, senza pretesa di esaustività, il livello di "maturità" dell'impresa o dello studio in relazione alle nuove disposizioni.

| Quesito | Si | No | Annotazioni |
|---|---|---|---|
| **Dati personali e trattamento effettuati** | | | |
| È disponibile una descrizione di tutte le categorie di dati personali che vengono trattati? | | | |
| I dati sensibili sono individuati separatamente rispetto agli altri dati? Così anche i dati relativi a condanne penali e reati? | | | |
| **Finalità e basi giuridiche del trattamento** | | | |
| Sono state individuate e esplicitate le finalità della raccolta e del trattamento dei dati personali? | | | |
| Il trattamento si fonda su un'idonea base giuridica (es. consenso dell'interessato, esecuzione di un contratto, adempimento di un obbligo legale)? | | | |
| Qualora un trattamento sia effettuato per conto del titolare, questo è disciplinato da un contratto o da altro atto giuridico? Il contratto (o altro atto giuridico) disciplina la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento? | | | |

# La check list sulla privacy

| Quesito | Si | No | Annotazioni |
|---|---|---|---|
| **Consenso e informativa** | | | |
| Se il trattamento si fonda sul consenso, è possibile dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali? | | | |
| Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro? | | | |
| L'informativa utilizzata è concisa, trasparente, intelligibile e facilmente accessibile? Utilizza un linguaggio semplice e chiaro, in particolare se destinata al minore? | | | |
| L'informativa fornita agli interessati contiene tutti gli elementi previsti dal Regolamento? | | | |
| **Periodo di conservazione dei dati** | | | |
| Per ciascun trattamento, il periodo di conservazione dei dati è determinato o determinabile? | | | |
| Sono disponibili procedure per eseguire la cancellazione sicura dei dati al termine del periodo di conservazione, ovunque essi si trovino? | | | |

# La check list sulla privacy

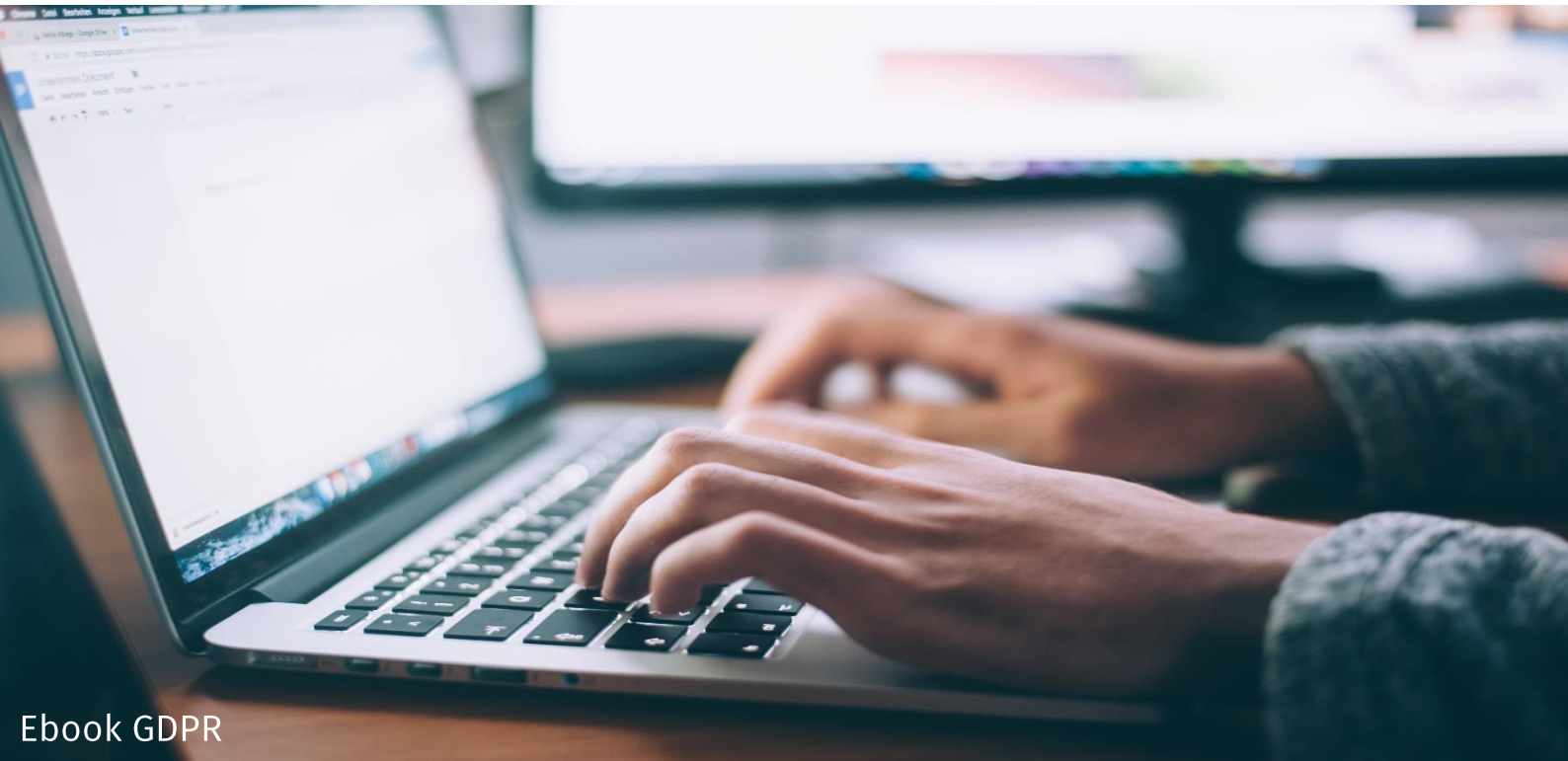
| Quesito | Si | No | Annotazioni |
|---|---|---|---|
| **Diritti degli interessati** | | | |
| Sono disponibili procedure che illustrano dettagliatamente le modalità con le quali un interessato può esercitare il diritto di accesso ai dati personali? | | | |
| Sono disponibili procedure che illustrano dettagliatamente le modalità con le quali un interessato può esercitare il diritto di rettifica e di cancellazione dei dati personali? | | | |
| Sono disponibili procedure che illustrano le modalità con le quali l'interessato ha il diritto a ottenere la limitazione di trattamento dei dati personali? | | | |
| Sono disponibili procedure che descrivono le modalità con le quali l'interessato può esercitare il diritto alla portabilità dei dati? | | | |
| Esiste una procedura che consente ad un interessato di negare l'utilizzo dei suoi dati per finalità di marketing diretto? | | | |
| Esiste una procedura che consente all'interessato di esercitare il diritto di non essere sottoposto a processi decisionali automatizzati, compresa la profilazione? | | | |

# La check list sulla privacy

| Quesito | Si | No | Annotazioni |
|---|---|---|---|
| **Formazione del personale** | | | |
| Il personale ha ricevuto dettagliate istruzioni per il trattamento dei dati personali nel rispetto delle disposizioni regolamentari? | | | |
| Sono previste periodiche sessioni di aggiornamento per tutto il personale incaricato al trattamento dei dati? | | | |
| **Sicurezza dei trattamenti** | | | |
| Sono state valutate le misure di sicurezza tecniche e organizzative suggerite dal Regolamento? (es. pseudonimizzazione e cifratura dei dati personali, procedure per valutare regolarmente l'efficacia delle misure tecniche e organizzative) | | | |
| Le misure adottate garantiscono un livello di sicurezza adeguato al rischio? | | | |
| **Registro dei trattamenti** | | | |
| L'impresa o l'organizzazione ha un numero di dipendenti pari o superiore a 250? | | | |
| Il trattamento effettuato può presentare un rischio per i diritti e le libertà delle persone, non è occasionale o include dati particolari e dati personali giudiziari? | | | |
| In caso di risposta affermativa ad almeno uno dei due quesiti precedenti, è stato istituito il registro dei trattamenti? | | | |

# La check list sulla privacy

| Quesito | Si | No | Annotazioni |
|---|---|---|---|
| **Valutazione di impatto sulla protezione dei dati** | | | |
| 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? | | | |
| In caso di risposta affermativa, è stata eseguita, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali? | | | |
| **Gestione del data breach** | | | |
| È stato definito un protocollo per l'individuazione e la gestione di eventuali violazioni dei dati? | | | |
| In caso di violazione dei dati, sono definite le modalità di comunicazione del "data breach" all'autorità garante e agli interessati, se necessario? | | | |



# Piena operatività delle disposizioni

Il Regolamento è entrato in vigore il 24 maggio 2016 e sarà applicato, dopo un periodo di transizione di due anni, **a partire dal 25 maggio 2018**. Pertanto, da tale data sono obbligati al rispetto delle disposizioni i titolari o i responsabili del trattamento che sono stabiliti con le proprie attività nell'Unione.

Il Regolamento è, inoltre, operante quando le **attività di trattamento riguardano dati personali di interessati che si trovano nell'Unione**, indipendentemente dal fatto che titolare o il responsabile del trattamento siano stabiliti nell'Unione.

L'operatività di quest'ultima disposizione è condizionata al fatto che le attività di trattamento riguardino l'offerta di beni o la prestazione di servizi agli interessati o il monitoraggio del loro comportamento all'interno dell'UE.

# Cose da fare per arrivare pronti all'appuntamento col GDPR

## Consapevolezza

l'azienda o lo Studio deve essere consapevole, a tutti i livelli, che il GDPR impone dei cambiamenti e che avrà impatto sulle attività quotidiane. Vanno istituiti momenti di formazione e informazione.

## Organizzazione

è necessario definire in modo chiaro le responsabilità e gli ambiti di intervento di ciascuno. Deve essere valutato l'obbligo (o l'opportunità) di nomina del DPO.

## Censimento

dei dati trattati e dei processi di trattamento

occorre censire tutte le tipologie di dati trattati, la natura e le finalità dei trattamenti. Ciò consente al titolare di capire se è necessario procedere con una valutazione di impatto sulla protezione di dati.

## Fondamenti legali

per il trattamento dei dati personali:

dopo aver individuato i dati trattati, occorre individuare quali sono i fondamenti legali del trattamento (es. esecuzione di un contratto, consenso, obbligo legale).

## Raccolta del consenso informato

occorre verificare puntualmente l'attuale informativa sulla privacy e la raccolta dei consensi per il trattamento dei dati. È necessario impostare un piano di intervento preciso, perché è un lavoro che richiede del tempo.

## Sicurezza dei trattamenti

è necessario implementare nuove misure di sicurezza dei dati (anche cartacei) oppure le misure adottate sono già adeguate?

# Cose da fare per arrivare pronti all'appuntamento col GDPR


## Diritti personali

tutti i processi sono rispettosi dei diritti degli interessati? Verificare la presenza di un protocollo di gestione delle richieste di accesso secondo le nuove tempistiche.

## Fornitori

è stata valutata l'affidabilità dei fornitori, anche nell'ambito del trattamento dei dati personali?

## Privacy by Design

in caso di implementazione di nuovi prodotti e servizi, è buona regola definire linee guida e template utili alla valutazione dell'impatto privacy.

## Registri delle attività di trattamento

hai valutato l'obbligo di istituire i registri dei trattamenti?

## Data breach

definisci le procedure per rilevare e notificare una eventuale violazione dei dati.

# *Conclusioni*

Il GDPR costringe le aziende e gli studi a guardare alla gestione dei dati personali, in particolare quelli dei clienti, con occhi nuovi e con una nuova consapevolezza.
Nel caso di aziende medio-grandi e strutturate, raggiungere la compliance è un lavoro impegnativo che coinvolge molteplici settori, dal dipartimento affari legali all'IT.

Anche se il tempo stringe, non è mai troppo tardi per cominciare il processo di adeguamento.

Il 25 maggio 2018 non va inteso come punto di arrivo, ma rappresenta un nuovo punto di partenza rispetto al Codice privacy italiano.

# Glossario

**G.D.P.R.**

General Data Protection Regulation.
Introduce regole più chiare su informativa e consenso; definisce i limiti al trattamento automatizzato dei dati personali; pone le basi per l'esercizio di nuovi diritti; stabilisce criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue; fissa norme rigorose per i casi di violazione dei dati (data breach).

**Informativa privacy**

Testo da fornire in modo obbligatorio, fondamentale per il trattamento dei dati personali

**Compliance**

Correttezza delle procedure e del rispetto delle norme previste dalla normativa sulla privacy allo scopo di non incorrere in sanzioni

**D.P.O.**

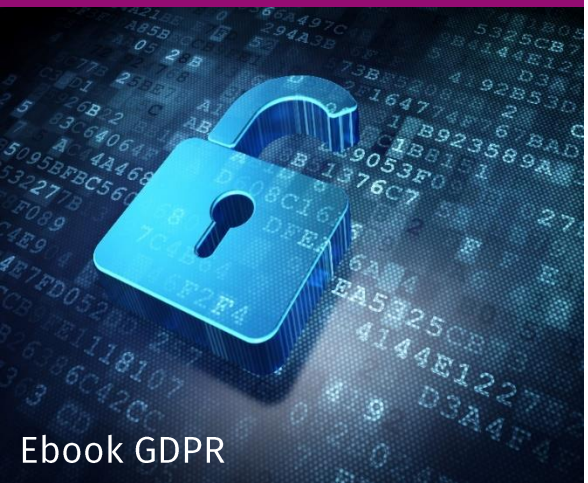
Data Privacy Officer, responsabile di attività di consulenza e supervisione all'interno dell'Azienda o dello Studio

**Data breach**

Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trattati.

**Oblio**

È il diritto alla cancellazione dei propri dati personali in forma rafforzata.
Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad es. pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".




# *Come raggiungere la compliance con la privacy europea.*

Per maggiori informazioni visita: www.giachinogiuseppe.it

STUDIO TECNICO
GIACHINO GEOM. GIUSEPPE
PROGETTAZIONE E SERVIZI TECNICI PER L'EDILIZIA

*contrada Pirato sn - 94018 Troina (EN) - tel. e fax: 0935 656179 / 339 1499740*
*codice fiscale: GCH GPP 61D11 L448 V - p.IVA: 0043 277 086 5*
*www.giachinogiuseppe.it - info@giachinogiuseppe.it - giuseppe.giachino@geopec.it*