Regolamento UE 2016/679 (GDPR) in materia di trattamento dei dati personali e di privacy

VADEMECUM

SUPPORTO ADEMPIMENTI PRIVACY

Via Almese, 25 - 10093 - Collegno (TO) 392 9624402 - fax: 011 4010928 info@thnet.it **www.thnet.it**

PRESENTAZIONE:

Il presente vademecum è stato redatto per aiutarvi a definire le linee guida fondamentali e le regole di comportamento per quanto concerne l'adeguamento al Regolamento UE 2016/679 (GDPR).

Il presente documento rappresenta uno strumento che si propone di supportarti ed aiutare te, il tuo studio/azienda nell'adeguamento al GDPR; suggerisce le linee guida sulle minime operazioni necessarie per adeguarsi al Regolamento, a cui ogni Titolare del Trattamento viene invitato a conformarsi, senza voler sostituire e prevalere sulle Leggi e Normative vigenti.

Si invita inoltre Titolare del Trattamento, nonché eventuali altri soggetti coinvolti (incaricati, Responsabili del Trattamento, ecc.) ad approfondire quanto previsto dal GDPR, attraverso aggiornamenti e formazione continua, per eventuali e successive revisioni, diverse interpretazioni o provvedimenti successivi.

Per approfondimenti: **www.garanteprivacy.it**

INDICE ADEMPIMENTI

1. FORMAZIONE DI TITOLARI/INCARICATI/RESPONSABILI
2. ANALIZZARE IL CONTESTO AZIENDALE/STUDIO
3. VALUTARE L'ORGANIZZAZIONE AZIENDALE/STUDIO
4. MAPPATURA UFFICIO/I
5. INDIVIDUARE I TRATTAMENTI
6. COMPILARE IL REGISTRO DEI TRATTAMENTI
7. NOMINARE I RESPONSABILI/INCARICATI AL TRATTAMENTO
8. IMPLEMENTARE LA DOCUMENTAZIONE
9. INTRODURRE UN CODICE DI CONDOTTA AZIENDALE/STUDIO
10. CREARE UN DOCUMENTO RIGUARDANTE LA SICUREZZA E NOMINA RESPONSABILI
11. CREARE UN REGISTRO DEGLI ACCESSI AGLI ARCHIVI E DELLE VIOLAZIONI (DATA BREACH)
12. INVIARE E PUBBLICARE INFORMATIVA
13. ACQUISIRE I CONSENSI
14. NOMINARE IL DPO (SE NECESSARIO)

GLOSSARIO PRIVACY

OGNI TITOLARE DEL TRATTAMENTO DEVE PROCEDERE A:

1. FORMAZIONE DI TITOLARI/INCARICATI/RESPONSABILI

Formazione continua di incaricati/responsabili/titolari con la presenza di esperti e attraverso circolari informative, partecipazione a convegni, corsi specifici e workshop. Archiviazione della documentazione didattica fornita e degli attestati di frequenza acquisiti.

Come specificato negli artt. 29 e 32 del Regolamento, il Titolare ed il Responsabile del Trattamento devono essere sufficientemente formati per trattare i dati, e devono assicurarsi che chiunque altra figura tratti i dati sia istruito a farlo dal Titolare. In caso di nomina di un DPO, anch'egli deve essere formato adeguatamente per poter ricoprire tale posizione.

Tra le prime verifiche che vengono fatte durante i controlli da parte del Garante e dalla Guardia di Finanza vi sono l'acquisizione del programma formativo, le dispense, i materiali erogati, il test finale nonché i dati relativi alle modalità di accesso e consultazione delle banche dati.

Per essere in regola con la formazione occorre che le figure addette al trattamento dei dati frequentino corsi formativi e facciano test finali per provare le proprie conoscenze. La documentazione relativa alla formazione deve essere conservata e tutto il personale adibito deve poter accedere al materiale. È inoltre necessario sensibilizzare il personale sull'importanza della protezione dei dati personali e sull'uso responsabile dei mezzi aziendali (mail, telefoni, password, ecc.) in cui sono coinvolti i dati.

2. ANALIZZARE IL CONTESTO AZIENDALE/STUDIO

Individuazione del contesto aziendale/studio e definizione dei processi aziendali e delle attività svolte (definizione del contesto interno ed esterno, delle attività che vengono svolte dall'azienda/studio e i processi con cui vengono messe in pratica).

3. VALUTARE L'ORGANIZZAZIONE AZIENDALE/STUDIO

Raccolta delle informazioni sull'organizzazione aziendale/studio (com'è strutturata l'azienda/studio, che ruolo hanno le figure che ci lavorano, di quali mansioni si occupano, ecc.).

4. MAPPATURA UFFICIO/I

Si consiglia di redigere una mappa di ogni ufficio, tenendo in particolare considerazione ciò che viene utilizzato per la conservazione di documenti contenenti dati personali (ad es. pc, armadi, raccoglitori, ecc.).

5. INDIVIDUARE I TRATTAMENTI

Verifica della situazione attuale rispetto al trattamento dei dati personali.
Occorre individuare:
-la tipologia dei trattamenti che viene eseguito in ogni ufficio,
-le tipologie di dati trattati (personali semplici o sensibili/giudiziari),
-le finalità del trattamento (ovvero il motivo per cui viene trattato tale dato),
-i soggetti che trattano i dati,
-le persone/interessati i cui dati vengono trattati,
-il tipo di conservazione dei dati (informatico o cartaceo),
-la durata dei trattamenti,
-la base giuridica del trattamento (ad es. esecuzione di un contratto),
- il livello di gravità in caso di violazione del dato,
- i nominativi degli incaricati al trattamento,
- l'eventuale trasmissione dei dati al di fuori dell'UE,
- le misure di sicurezza adottate per la protezione dei dati.

6. COMPILARE IL REGISTRO DEI TRATTAMENTI

Creazione del registro dei trattamenti e compilazione con i dati raccolti al punto precedente. Il registro è obbligatorio per le aziende dai 250 dipendenti in su, ma è definito utile dal Garante se utilizzato come strumento per tenere traccia di tutto ciò che riguarda il trattamento dei dati personali.

7. NOMINARE I RESPONSABILI/ INCARICATI AL TRATTAMENTO

Individuazione dei ruoli e delle responsabilità dei responsabili/incaricati al trattamento dei dati, sia interni (ad es. dipendenti, collaboratori, ecc.) sia esterni (ad es. commercialista, avvocato, consulenti, ecc.) procedendo alla nomina con relativo atto scritto e lettera di nomina.

8. IMPLEMENTARE LA DOCUMENTAZIONE

Implementazione della documentazione secondo la nuova normativa in relazione a provvedimenti successivi e/o a completamento in caso di carenza nell'attuale documentazione.

9. INTRODURRE UN CODICE DI CONDOTTA AZIENDALE/STUDIO

Elaborazione di un codice di condotta aziendale o adozione di uno di categoria, da far poi sottoscrivere a tutti gli incaricati.

10. CREARE UN DOCUMENTO RIGUARDANTE LA SICUREZZA E NOMINA RESPONSABILI

Creazione di un documento sulle misure di sicurezza aziendali e sulla valutazione dei rischi in seguito all'adeguamento al Regolamento. Occorre inoltre nominare i responsabili relativi alla sicurezza (responsabile sistema informatico, responsabile gestionale, responsabile videosorveglianza, custode password/chiavi/accesso archivi, amministratore di sistema).

11. CREARE UN REGISTRO DEGLI ACCESSI AGLI ARCHIVI E DELLE VIOLAZIONI (DATA BREACH)

Creare un registro relativo agli accessi agli archivi contenenti dati personali e uno relativo alla notifica delle violazioni, anche di livello basso. In caso di violazioni più gravi è necessario notificare al Garante entro 72 ore l'avvenuta violazione e procedere in base alla gravità della violazione stessa.

12. INVIARE E PUBBLICARE L'INFORMATIVA

È necessario inviare l'informativa a dipendenti, clienti e fornitori preferibilmente a mezzo PEC o raccomandata per tenerne traccia; pubblicarla sul sito ed inserire il link in calce alle mail/comunicazioni/fatture/ordini. In caso di trattamento di dati particolari/giudiziari o di raccolta di dati per finalità diverse dal legittimo interesse del titolare o dell'interessato (come ad esempio il "marketing massivo"), è necessaria la firma del consenso.

13. ACQUISIRE I CONSENSI

È necessario richiedere e acquisire il consenso dell'interessato nel caso in cui i dati vengano raccolti per finalità diverse dal legittimo interesse del titolare o dell'interessato stesso, o nel caso di trattamento di dati particolari o giudiziari. La richiesta di consenso deve essere presentata in modo distinto da altre richieste, essere comprensibile e facilmente accessibile e avere un linguaggio semplice e chiaro. Il titolare deve inoltre essere in grado di dimostrare che il consenso sia stato effettivamente prestato.

14. NOMINARE IL DPO (SE NECESSARIO)

Il Data Protection Officer (DPO) è la figura che si occupa di valutare e organizzare la gestione del trattamento di dati personali all'interno dell'azienda. La nomina di un DPO è obbligatoria per chi tratta in modo sistematico dati personali su larga scala, dati sensibili o giudiziari.

GLOSSARIO

LA PRIVACY CON IL GDPR 2016/679

Il GDPR (General Data Protection Regulation) disciplina la protezione dei dati personali nell'UE.

Alcune cose da sapere:

L'INFORMATIVA

Si tratta delle informazioni destinate all'interessato. Illustra in modo chiaro e sintetico i suoi obblighi e diritti e gli scopi e le modalità del trattamento. Deve essere chiara, semplice e facilmente accessibile e deve avere una forma concisa, trasparente, intelligibile. Viene consegnata per iscritto o in formato elettronico.

COSA SONO I DATI PERSONALI?

I dati personali sono quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, relazioni personali, abitudini, stile di vita e situazione economica, ecc.

E I DATI PERSONALI PARTICOLARI?

Sono quei dati personali che rientrano in particolari categorie e sono definiti «*dati sensibili*», cioè che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, politiche, l'appartenenza sindacale, relativi alla salute, alla vita, all'orientamento sessuale e i dati genetici e biometrici.

COSA SI INTENDE PER TRATTAMENTO DEI DATI PERSONALI?

S'intende l'operazione o l'insieme di operazioni applicate ai dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, l'utilizzo, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

PERCHÉ SI PARLA DI CONSENSO?

. Per consenso si intende qualsiasi manifestazione di volontà libera, specifica, informata, preventiva e inequivocabile dell'interessato con cui egli manifesta il proprio assenso, mediante dichiarazione o azione positiva, che i suoi dati personali siano oggetto di trattamento. Non deve essere necessariamente documentato per iscritto o avere forma scritta e può essere implicito ma NON tacito o presunto (come nel caso di caselle pre-spuntate sui moduli). Nel caso invece di dati sensibili o processi decisionali automatizzati occorre un consenso esplicito

COSA SIGNIFICA IL TERMINE ACCOUNTABILITY?

Indica la responsabilizzazione di Titolari e Responsabili del trattamento nell'adottare comportamenti proattivi tali da dimostrare l'adozione di misure concrete per assicurare l'applicazione del GDPR.

E L'ESPRESSIONE "PRIVACY BY DESIGN E BY DEFAULT"?

È il principio che implica la predisposizione di misure preventive volte alla protezione dei dati basandosi non solo su modelli standard (privacy by default), ma anche su procedure specifiche per la propria realtà (privacy by design) da parte del Titolare del trattamento.

CHI È L'INTERESSATO?

L'interessato è la persona fisica identificata o identificabile cui si riferiscono i dati personali.

CHI È LA FIGURA DEL DPO?

Il Data Protection Officer (Responsabile della protezione dei dati) è la figura che valuta e organizza la gestione del trattamento dei dati personali nel rispetto delle normative privacy. Ha inoltre la funzione di intermediario tra il Garante e l'interessato. Le amministrazioni, gli enti pubblici, i soggetti la cui attività principale consiste in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala e i soggetti la cui attività principale consiste nel trattamento su larga scala di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari o biometrici; hanno l'obbligo di nominare un DPO.

COS'È IL REGISTRO DEI TRATTAMENTI?

Si tratta del documento interno che contiene tutte le informazioni relative al trattamento, esiste in duplice copia (per il Titolare e per il Responsabile del trattamento).

CHI È IL TITOLARE DEL TRATTAMENTO?

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento.

CHI È IL RESPONSABILE DEL TRATTAMENTO?

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

CHE RUOLO HA IL DESTINATARIO?

Si tratta della persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali (che si tratti o meno di terzi).

COSA SI INTENDE PER DATA BREACH?

Si parla di data breach quando vi è una violazione di sicurezza nella quale i dati sensibili vengono consultati, copiati, trasmessi, rubati, persi, distrutti o utilizzati da un soggetto non autorizzato. In caso di violazioni, queste ultime devono essere segnalate al Garante e all'interessato entro 72 ore dalla violazione stessa.

A QUALI SANZIONI SI PUÒ ANDARE INCONTRO?

L'inosservanza delle disposizioni in tema di privacy può portare a sanzioni sino a un massimo di euro 20.000.000,00 o al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

Garante per la protezione dei dati personali: www.garanteprivacy.it