Linee guida essenziali per il GDPR

Principi di riferimento

Il GDPR si applica a tutti coloro che trattino dati personali di persone fisiche e che effettuino attività di monitoraggio, sempre di persone fisiche, entro la UE; i principi base del regolamento sono:

- la liceità, correttezza e trasparenza nel trattamento, l'adeguatezza e pertinenza dell'utilizzo dei dati
- l'esattezza, la conservazione per un periodo di tempo limitato,
- l'integrità e la riservatezza dei dati conservati.

L'applicazione di tali principi mira al fine di salvaguardare i diritti della persona fisica titolare dei dati. Tali principi responsabilizzano fortemente le aziende che acquisiscono e trattano tali dati e che sono quindi soggette a sanzioni anche molto rilevanti.

Cosa sono i dati personali

Un dato personale è ogni informazione che possa in qualche modo identificare, direttamente o indirettamente, una persona fisica: nome, cognome, indirizzo, la mail, il numero di telefono, informazioni sulla salute, la scelta politica, le preferenze sessuali, le immagini e simili.
Quindi il campo è molto ampio e soggetto a interpretazione.

Le figure responsabili del trattamento dati

Il GDPR prevede tre diverse figure principali legate al trattamento dei dati personali,

1. il **titolare del trattamento**, che decide le finalità di trattamento, impartisce istruzioni e direttive e svolge funzioni di controllo.

   Il titolare, in caso di persona giuridica o di studio associato, è l'azienda o lo studio stesso, mentre in caso di azienda individuale o professionista è la persona fisica. Non servono atti di nomina, si identifica con il legale rappresentante dell'azienda, in una parola il capo.

2. il **responsabile del trattamento**, preposto dal titolare al trattamento dei dati personali.

   Il responsabile del trattamento può essere interno, un dipendente responsabile di una attività, o esterno. Un esterno può essere una persona fisica o giuridica e lavora per l'azienda in base ad un contratto.

3. l'**incaricato del trattamento**, ruolo che può essere ricoperto da una o più persone.

L'incaricato del trattamento, chiunque esso sia, deve essere obbligatoriamente istruito dal titolare o dal responsabile del trattamento ed è autorizzato ad operare sui dati. Può essere ad esempio, un impiegato addetto all'amministrazione o alla gestione del personale..

Vi sono poi altre due figure importanti.

1. l'**amministratore di sistema;** un tecnico che si occupa della gestione di un sistema informatico e/o alla manutenzione dei suoi componenti

2. il **responsabile della protezione dei dati** (Data Protection Officer); è la persona assegnata ad affiancare il titolare e il responsabile del trattamento dati, può essere un dipendente o un soggetto esterno. È il garante del rispetto del GDPR e della privacy in generale; la sua nomina è richiesta in alcuni casi specifici:
    - Se il trattamento dei dati è effettuato da un'autorità pubblica o da un organismo pubblico
    - Quando le attività principali del titolare del trattamento o del responsabile del trattamento prevedano raccolta e gestione di dati su vasta scala (es. E-Commerce, Blog ecc.)
    - Quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali (ad esempio dati sanitari) o di dati relativi a condanne penali.

    I compiti del DPO sono di **verifica e controllo** sull'attuazione e applicazione del regolamento, inoltre il DPO cura la sorveglianza sul trattamento dei dati, informazione e consulenza circa gli obblighi del regolamento.

Conservazione e trattamento dei dati

Il titolare ha l'obbligo di:

- ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati;
- ridurre al minimo i rischi di accesso non autorizzato alle banche dati, cartacee o elettroniche;
- assicurare che il trattamento sia lecito e rimanga sempre conforme alle finalità della raccolta;
- assicurare che i dati siano conservati per il periodo strettamente necessario.

Il diretto interessato deve poter accedere in ogni momento ai dati conservati per conoscere:

- la finalità del trattamento,
- le categorie dei dati personali in questione,
- i destinatari o le categorie di destinatari cui i dati sono stati o saranno comunicati,
- il periodo o i criteri di conservazione,
- il diritto di proporre reclamo a un'autorità di controllo,
- le informazioni sull'origine dei dati qualora questi non siano stati raccolti dal titolare,
- l'esistenza di un processo decisionale automatizzato quale la profilazione.

Su richiesta, il titolare del trattamento fornisce all'interessato le informazioni richieste entro un tempo stabilito e a titolo gratuito. Una volta ricevute le informazioni, il soggetto che le ha richieste può chiedere la rettifica dei dati, la limitazione del trattamento in caso di dati inesatti o, ancora, la loro cancellazione se è esaurita la finalità di trattamento o se è stato revocato il consenso, è stata fatta opposizione al trattamento o se ci sia stata di violazione di legge.

Il registro dei trattamenti

Il regolamento prevede l'istituzione del **registro dei trattamenti**, non obbligatorio se ci sono meno di 250 dipendenti. Il registro è sempre obbligatorio se il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, che non sia occasionale o che gestisca dati particolarmente critici.

Analisi dei rischi

Il GDPR prevede che periodicamente sia fatta una analisi dei rischi generale a cui è soggetta l'azienda con particolare riferimento ai sistemi, informatico o manuali, che trattano dati personali.

Notifica al Garante

In caso di **violazione dei dati personali** (Data breach notification) ovvero perdita, distruzione o diffusione indebita degli stessi, si deve notificare il fatto al Garante dei dati personali, l'autorità pubblica che regola la privacy, indicando le misure di contrasto adottate. In alcuni casi è necessario comunicare il fatto anche all'interessato titolare dei dati.

Valutazione di impatto

In particolari casi è richiesta anche una **valutazione di impatto sul trattamento dei dati**, ad esempio qualora i trattamenti dei dati riguardino dati molto delicati o siano trattati in grossa quantità (vasta scala) come nei casi di profilazione ai fini di marketing. In questo caso è necessario valutare i possibili impatti (danni) causabili ai titolari dei dati in caso di perdita, manomissione, danneggiamento dei dati stessi.

Informativa privacy

È la dichiarazione che il titolare fa all'interessato sull'esistenza del trattamento e delle sue finalità. L'informativa deve essere immediata, chiara, in linguaggio non tecnico, e che contenga le informazioni che permettano di contattare il titolare del trattamento dei dati personali. Se i dati personali sono raccolti direttamente dall'interessato, l'informativa è rilasciata prima della raccolta dei dati e dovrebbe includere una richiesta di consenso al trattamento. L'informativa deve contenere:

- l'identità del titolare del trattamento e, dove applicabile, del suo rappresentante; i dati di contatto del responsabile della protezione dei dati,
- le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento,
- gli eventuali destinatari o le categorie di destinatari dei dati.

Il titolare deve fornire all'interessato:

- le informazioni sul periodo di conservazione dei dati, la lista dei diritti dell'interessato
- comunicare l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione dell'utente.
- Le eventuali altre fonti dati utilizzate

Consenso al trattamento dati

Oltre all'informativa, è necessario ottenere il **consenso** al trattamento che deve arrivare mediante dichiarazione o azione inequivocabile dell'interessato. Il consenso conferma che i dati personali sono oggetto di trattamento autorizzato. In alcuni casi il consenso non è obbligatorio.

Le sanzioni previste

La mancata osservanza delle norme comporta delle pesanti **sanzioni**:

- da 6mila a 36mila euro per l'omessa o inidonea informativa;
- da 20mila a 120mila euro per l'omessa o incompleta notificazione.

Le sanzioni pecuniarie per la violazione degli obblighi del regolamento europeo sono commisurate alla gravità dei fatti. La sanzione può arrivare fino a 20 milioni di euro e al 4 per cento del fatturato.

Regole minime da seguire

1. Disporre di una buona informativa da comunicare e far sempre firmare a clienti e fornitori
2. Disporre di una buona informativa per i propri siti WEB se esistenti
3. Dotarsi di un set di documenti che dimostrino la corretta gestione della privacy. Tali documenti devono essere rivisti o aggiornati almeno annualmente
4. In caso di dubbi rivolgersi ad esperti e/o al proprio commercialista
5. Tenersi aggiornati sulle principali novità in materia di privacy
6. Richiedere il consenso al trattamento dei dati ove obbligatorio
7. Proteggere l'acceso ai propri PC (firewall, antivirus, salvaschermo) cambiando periodicamente le password di accesso, la password non va comunicata a nessuno
8. Gestire correttamente i tempi di conservazione dei dati
9. Non lasciare mai il PC o il telefonino accessibili ad altri se non con voi presenti
10. Proteggere i dati cartacei chiudendoli in luoghi ed armadi protetti
11. Proteggere i dati elettronici utilizzando se necessario modalità di cifratura
12. Eseguire copie periodiche dei dati elettronici (back-up)
13. Controllare gli accessi ad internet e accedere con prudenza a siti non conosciuti
14. Non scaricare dati o programmi da internet se non da siti noti e controllati
15. Non accedere a siti pericolosi
16. Gestire con prudenza le mail provenienti dall'esterno
17. Siglare accordi precisi che prevedano garanzie relative alla privacy con i fornitori soprattutto di servizi (es. commercialista)
18. Assicurarsi di non avere sistemi di video sorveglianza che controllino i dipendenti al lavoro