# GDPR - Codice di Condotta e Norme di Comportamento per il trattamento dei Dati Personali

## Principi generali

**Definizioni**

- Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile
- Trattamento: qualsiasi operazione o insieme di operazioni, compiuto con o senza l'ausilio di processi automatizzati e applicati a dati personali o insieme di dati personali
- Interessato o Utente: persona fisica i cui dati personali sono raccolti e/o elaborati
- Titolare: persona giuridica, azienda, ente o associazione che raccoglie e/o elabora i dati personali degli Utenti per scopi correlati alla propria attività
- Soggetto autorizzato o Incaricato: dipendente o collaboratore del Titolare, autorizzato al trattamento dei dati personali
- Responsabile esterno: un soggetto, distinto dal "titolare", che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

**I fondamenti**

La protezione dei dati personali è un dovere per tutti. Dipendenti e collaboratori sono obbligati a gestire i dati personali degli utenti in maniera responsabile. I dati personali degli utenti appartengono agli utenti i quali determinano liberamente lo scopo per il quale devono essere utilizzati i propri dati.

**Finalità del Codice**

Il presente Codice di Condotta (di seguito "Codice") è volto a fornire informazioni di base per agire in conformità ai princìpi generali della normativa vigente in materia di protezione dei dati personali.

Tra le finalità del Codice, vi sono anche quella di contribuire a migliorare la trasparenza dei trattamenti dei dati personali e favorire un clima di fiducia per gli utenti che fruiscono dei servizi sia gratuiti che a pagamento erogati dal Titolare.

**Tutela dei rapporti con gli utenti**

Ogni incaricato si impegna a mantenere un comportamento improntato alla correttezza, liceità e rispetto degli utenti in ogni attività che comporta il trattamento dei loro dati personali.

Nell'ambito dello svolgimento delle proprie attività, l'incaricato deve sempre comportarsi in modo trasparente con l'utente, in conformità con le disposizioni vigenti in materia di protezione dei dati personali e in linea con i princìpi etici contenuti nel presente Codice.

**Pratiche e omissioni ingannevoli**

E' considerata ingannevole una pratica che comporta l'omissione di informazioni rilevanti o la comunicazione di informazioni non veritiere, o che, seppure di fatto corrette, sono in grado di indurre in errore l'utente riguardo all'assunzione di decisioni, che altrimenti non avrebbe preso, di fornire i propri dati personali o prestare liberamente il proprio consenso al trattamento.

Sono in ogni caso considerate ingannevoli le pratiche che si basino palesemente sull'inganno o che risultino significativamente riduttive e che rendano difficoltoso per l'utente essere dovutamente informato o prestare consapevolmente il proprio consenso al trattamento dei suoi dati personali, nonché l'utilizzo di sistemi mirati a forzare l'ottenimento del consenso dell'utente mediante checkbox preselezionate o altri espedienti che pregiudichino l'effettiva possibilità di esprimere liberamente il proprio consenso.

**Rispetto obbligo di informare gli utenti**
Ogni titolare o incaricato è tenuto ad adottare le misure appropriate per fornire all'utente tutte le informazioni riguardanti il trattamento dei suoi dati personali in conformità alla normativa vigente.

Tali informazioni devono essere fornite all'utente in modo conciso, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
Una delle lingue utilizzate deve essere quella ufficiale o prevalente dell'area geografica di pertinenza, oppure l'inglese se il servizio è rivolto a un pubblico internazionale di utenti.

**Rispetto della norma sul consenso dell'utente**
In tutti i casi in cui il trattamento dei dati personali richiede consenso, il titolare deve essere in grado di dimostrare che l'utente, possa liberamente prestare il proprio consenso in conformità con le prescrizioni di legge vigenti.

Il titolare è tenuto altresì a rispettare il diritto dell'utente di revocare il proprio consenso in qualsiasi momento con la stessa facilità con cui è stato precedentemente accordato, salvo obblighi di legge che lo impediscano.

**Rispetto dei diritti degli utenti**
Ogni incaricato si impegna a rispettare tutti i diritti dell'utente in materia di protezione dei dati personali.

**Divieto di trattamento di informazioni sensibili**
A meno che l'utente non abbia prestato il proprio consenso esplicito e specifico, o che sussistano specifiche deroghe previste dalla legge, è vietato il trattamento di informazioni di carattere sensibile, quali i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

# Norme di comportamento

## Norme di comportamento generiche

- Il trattamento di dati personali non autorizzato da una norma o dal consenso esplicito dell'interessato, è vietato.
- L'uso dei dati per scopi diversi da quelli previsti inizialmente è vietato.
- Il titolare del trattamento è responsabile per le violazioni della protezione dei dati e per le violazioni della legge.
- Incaricati e responsabili hanno gli stessi obblighi dei titolari e devono garantire agli utenti gli stessi diritti. Titolari e incaricati devono anche poter dimostrare di rispettare la normativa del GDPR e tutti gli obblighi previsti da essa.
- L'incaricato controlla sempre se la procedura per la gestione dei dati dell'utente è regolare o anomala; nel caso rilevi anomalie informa immediatamente il titolare,
- L'utente può richiedere accesso ai propri dati. Gli incaricati devono rispettare tale richiesta senza ritardi.
- Gli incidenti riguardo la protezione dei dati devono essere segnalati immediatamente al titolare e riportati all'utente entro 48 ore. E' obbligatorio informare riguardo a: causa dell'evento, quantità di dati interessati, come sono stati compromessi, quali possono essere le conseguenze e quali contromisure sono previste.
- In caso di incidenti riguardo la protezione dei dati, la mitigazione dell'incidente deve essere iniziata immediatamente.

## Norme di comportamento base per il trattamento di dati in formato cartaceo

- I documenti cartacei che contengono dati personali devono essere custoditi in luoghi inaccessibili alle persone non autorizzate e protetti da eventi che potrebbero danneggiarli o distruggerli.
- E' vietato lasciare documenti cartacei incustoditi o esposti al pubblico; al termine dell'utilizzo devono essere riposti nel loro archivio.
- In caso di alienazione di documenti cartacei contenenti informazioni personali, assicurarsi che non siano leggibili a chi ne dovesse eventualmente venire in possesso; utilizzare gli appositi distruggi-documenti oppure cancellare in modo sicuro le informazioni personali.
- E' vietato cedere documenti a terzi senza autorizzazione; in ogni caso non cedere documenti originali a terzi senza aver preventivamente verificato la disponibilità di copie dei dati.

**Norme di comportamento per il trattamento di documenti personali dell'interessato** (es. carte di identità, carte di credito, certificati, etc...)

- Trattenere i documenti solo per il tempo indispensabile allo scopo del trattamento (es. rilevazione dati, operazioni di pagamento, …), quindi restituire immediatamente il documento al proprietario.
- Non è permesso fotografare o riprodurre in copia i documenti se non previsto esplicitamente dalla procedura di trattamento; in tal caso accertarsi che la procedura di trattamento preveda adeguati sistemi di protezione delle copie effettuate.
- Ove possibile eseguire le operazioni di trattamento "a vista", in presenza dell'utente, in modo che non perda mai il contatto visivo con i suoi documenti; in nessun caso allontanare dalla vista dell'utente carte credito o di pagamento.
- Nel caso si debbano trattenere documenti per il loro trattamento, occorre custodirli in luogo sicuro, protetto almeno da serratura a chiave in dotazione esclusivamente alle persone autorizzate al trattamento.
- In caso di furto o smarrimento dei documenti, informare immediatamente il titolare del trattamento, l'utente e le autorità di sicurezza, per avviare le opportune procedure di blocco di sicurezza di documenti d'identità, carte di pagamento, titoli di credito, etc

**Norme di comportamento per il trattamento di carte di credito o simili**

- Evitare di trattenere dati relativi a carte di credito o altri strumenti di pagamento che, in caso di furto, smarrimento o utilizzo fraudolento potrebbero causare danno economico all'utente.
- Nel caso sia necessario ricevere dall'utente tali dati, scomporne l'invio tramite strumenti diversi (es. una parte via email e un altra parte via sms); quindi cancellarne ogni traccia dai veicoli trasmissivi (email, sms, etc…)
- Nel caso sia necessario memorizzare tali dati, scomporre i dati e memorizzarli su supporti differenti (almeno 2) ognuno protetto da password forti e adeguati sistemi di protezione fisica e logica; preferibilmente crittografare i dati prima di memorizzarli.
- Trattenere i dati esclusivamente per il tempo necessario alla finalità perseguita e cancellarne immediatamente tutte le tracce appena possibile.

**Norme di comportamento base per il trattamento di dati in formato elettronico**

- Le credenziali di accesso sono personali e segrete; conservarle in modo che non siano accessibili ad estranei.
- Bloccare lo schermo del computer con la schermata di richiesta password, prima di allontanarsi dalla postazione di lavoro
- Impostare password forti per l'accesso a server, personal computer, smartphone, email, cloud ed ogni altro dispositivo o software dove vengono memorizzati e/o trattati

dati personali (la password deve essere composta da almeno 8 cifre e contenere almeno una lettera maiuscola, un numero e un carattere speciale).
- Proteggere gli smartphone tramite PIN e segno di sblocco; impostare, se disponibile, la procedura di localizzazione e reset remoto del dispositivo,
- In caso di furto o smarrimento di dispositivi o supporti su cui sono memorizzate credenziali di accesso, cambiarle immediatamente e bloccare l'accesso ai servizi compromessi; informare immediatamente il titolare del trattamento e il responsabile dei sistemi se si sospettano accessi fraudolenti o compromissione dei sistemi di sicurezza.
- Nel caso si utilizzino procedure di accesso remoto ai sistemi (Desktop remoto, Teamviewer, Anydesk, etc…), non utilizzare le funzioni di salvataggio password disponibili sui software di accesso remoto.

- Verificare sempre che i dati immessi (digitati, scannerizzati, importati, etc…) siano stati acquisiti correttamente dal sistema di memorizzazione.
- Eseguire sempre le procedure di backup e verificarne la corretta esecuzione
- Attenersi alle procedure di sicurezza antivirus ed informare immediatamente il titolare qualora si sospetti infezione o tentativo di accesso ai sistemi
- L'utilizzo di dispositivi portatili quali "penne" o hard-disk usb deve essere autorizzato dal titolare; tali dispositivi devono essere custoditi in luogo inaccessibile ad estranei; prevedere funzioni di crittografia.
- In caso di alienazione di dispositivi con memoria di massa, (pc, server, nas, hard-disk, smartphone, etc…), effettuarne la preventiva cancellazione sicura con sistemi logici o fisici (formattazione a basso livello o distruzione meccanica) per evitare che siano leggibili da estranei.

**Norme di comportamento base per il trattamento di dati sensibili**

- Il trattamento di dati sensibili, qualora necessario e autorizzato, deve essere oggetto di attenzioni particolari volte ad evitarne qualsiasi diffusione o utilizzo non previsto.
- E' vietato inviare dati personali sensibili tramite social di qualsiasi tipo, anche se sussiste base giuridica per il trattamento o consenso dell'interessato.
- I dati personali sensibili devono essere sempre custoditi sotto chiave o tramite password forti.
- In caso di trasferimento a mezzo web (email, dropbox, etc...), devono essere anonimizzati, pseudonimizzati o crittografati.