



## Proteggere la tua privacy e darti sempre il pieno controllo sui tuoi dati personali: ecco il nostro impegno.

Dal 25 maggio 2018 entrerà in vigore una delle più innovative e importanti normative comunitarie: il **Regolamento EU General Data Protection Regulation (GDPR)** che proteggerà in modo ancora più incisivo i tuoi diritti sulla tutela dei dati personali, armonizzando le norme nei vari Stati dell'Unione, a prescindere da dove vengano elaborati i dati.

Noi di Kiamafacile, da sempre attenti alla tutela e ai diritti dei nostri Clienti e utilizzatori e all'applicazione delle norme già in vigore, attueremo e garantiremo il puntuale rispetto del nuovo regolamento GDPR nei nostri servizi: potrai così controllare meglio e più efficacemente la tua privacy e le modalità con cui tratteremo e proteggeremo i tuoi dati. Potrai accedervi, scaricarli, correggerli direttamente o per nostro tramite in qualsiasi momento e ti potremo rendere disponibili gli aggiornamenti su tutte le nostre piattaforme, in modo integrato.

Rispetto, fiducia e collaborazione sono da sempre al centro dei rapporti tra Kiamafacile e chi utilizza i suoi prodotti e i suoi servizi: l'adequamento al GDPR offre a tutti noi una straordinaria opportunità di stringere e rafforzare ulteriormente questo vitale e proficuo legame.

### CONOSCIAMO INSIEME LE PRINCIPALI CARATTERISTICHE DEL NUOVO REGOLAMENTO EUROPEO



#### **Cos'è il regolamento GDPR?**

GDPR sta per General Data Protection Regulation ed è una nuova legislazione dell'Unione Europea sulla protezione dei dati delle persone fisiche, che andrà a sostituire o integrare le normative nazionali e, per l'Italia, il Codice della Privacy (d.lgs 196/03)



#### **Quando entrerà in vigore il GDPR?**

Il Regolamento entrerà in vigore il 25 maggio 2018



### **Quali nuovi diritti introduce il Regolamento Europeo?**

Il Regolamento si sofferma sul principio di trasparenza nei rapporti con gli utenti. Viene infatti richiesta una informativa chiara, semplice e di immediata comprensione sulle finalità e sulle modalità di trattamento dei dati.

Inoltre, amplia i diritti delle persone (interessati) introducendo il diritto alla limitazione del trattamento ed il diritto alla portabilità dei dati (ovviamente quando tecnicamente applicabile). Viene inoltre confermato con maggiore enfasi il diritto all'oblio ed all'accesso ai propri dati.



### **Quali categorie di dati sono tutelati dal regolamento Europeo**

Il Regolamento chiarisce che la tutela riguarda dati delle sole persone fisiche ed in particolare i dati personali (anche parziale o pseudo anonimi, quali ad esempio codici identificativi), dati sensibili (riguardanti la salute, le abitudini sessuali, gli orientamenti politici e sindacali, religiosi o filosofici), dati biometrici, dati genetici (es. dna) e dati riguardanti precedenti penali o pendenze giudiziarie.



### **Quali nuovi obblighi prevede il Regolamento per i Titolari?**

Il Regolamento introduce una serie di nuovi obblighi per i Titolari, tra cui il principio della **Privacy by design e by default**, il principio di **adeguatezza**, l'obbligo della **valutazione d'impatto**, l'obbligo di nominare un **Responsabile della Protezione dei dati** (Data Protection Officer) e l'obbligo di tenere un **registro dei trattamenti**.



### **Cosa significa Privacy by design?**

Significa valutare e considerare il rispetto della protezione dei dati delle persone, sin dalla progettazione di nuovi trattamenti. Kiamafacile infatti applica questo principio nella realizzazione dei propri prodotti prevedendo la limitazione di trattamenti non strettamente necessari ed adeguate misure di sicurezza.



### **Cosa significa adeguatezza?**

Significa prevedere ed applicare misure tecniche, organizzative e procedurali adeguate ai rischi effettivi per i dati delle persone.



### **Cosa significa Valutazione di Impatto?**

Significa valutare per ogni nuovo trattamento o prodotto che implichi trattamento di dati, i rischi per i dati delle persone e le misure necessarie a proteggerli. È un obbligo strettamente collegato al principio della *Privacy by design e della adeguatezza*.



### **Si ha sempre l'obbligo di nominare un DPO?**

No. Solo nei casi espressamente previsti dal regolamento europeo (Pubbliche Amministrazioni, Organizzazioni che trattano dati particolari, tra cui i dati sensibili – salute, abitudini sessuali, orientamenti politici – e organizzazioni che trattano dati personali su larga scala)



### **Tutti devono avere un registro dei trattamenti?**

No. Ma solo le aziende con più di 250 dipendenti o quelle che eseguano trattamenti di dati sensibili, particolari o penali, o quelle che effettuano trattamenti che possano comportare un rischio per i diritti delle persone.



### **Se si profilano i Clienti sulla base dei cookies sul proprio sito, il GDPR è applicabile?**

La raccolta di dati tramite cookie e l'uso degli strumenti pubblicitari implica solitamente il trattamento dei dati personali; di conseguenza dovranno essere rispettate da parte dei Titolari le norme del Regolamento.



## **Ma quali basi legali autorizzano il trattamento dei dati?**

### *Necessità contrattuale*

I dati trattati vengono trattati perché necessari per la fornitura del servizio e devono essere chiaramente definiti nel contratto stipulato con l'utente.

### *Interessi legittimi*

Si tratta di un bilanciamento di interessi tra quello di un'azienda che deve sviluppare i servizi specifici del settore in cui opera (es. informazioni commerciali per la prevenzione delle frodi o erogazione di pubblicità) rispetto ai diritti degli interessati.

In ogni caso il trattamento dei dati deve essere sospeso se un utente solleva un'obiezione o espressamente chiede che i suoi dati non vengano più trattati. Ma unico obbligo iniziale per il Titolare del Trattamento è specificare nell'informativa la base legale del trattamento.

### *Far valere un diritto in giudizio o esercitare un proprio diritto*

Il trattamento è possibile quando è finalizzato ad una eventuale controversia giudiziaria.

### *Obbligo giuridico*

Quando il trattamento è previsto da un obbligo di legge (es. adempimenti antiriciclaggio)

### *Consenso*

Il trattamento è sempre consentito quanto vi è consenso non ambiguo, consapevole, specifico e libero da parte dell'utente mediante azione informativa chiara.

Le persone hanno il diritto di ritirare il proprio consenso e questa possibilità deve essere sottoposta alla loro attenzione e chiaramente dichiarata nell'informativa

Il consenso deve arrivare da una persona che abbia superato la maggiore età o deve essere dato o autorizzato da un genitore/tutore.

Per alcuni trattamenti (ad es. categorie dati sensibili), è necessario un consenso esplicito.



**IL PERCORSO DI ADEGUAMENTO DI ITALIAONLINE:  
PASSO DOPO PASSO....**

Il cuore delle attività di Kiamafacile è il trattamento di dati. Noi tutti interagiamo con persone, Clienti, fornitori, partner, utenti: per questo, abbiamo avviato, sin dallo scorso anno, un percorso di adeguamento al nuovo GDPR, il Regolamento Europeo sulla protezione dei dati personali.

Vediamo insieme lo stato di avanzamento delle attività, ossia quanto già fatto e quanto si andrà a fare entro il 25 maggio 2018, data di entrata in vigore della nuova normativa.

### **Cosa abbiamo fatto ad oggi:**

- Nell'ambito della Direzione Affari Legali e Societari, è stato nominato un Data Protection Officer di Gruppo a cui sono stati conferiti dal Consiglio di Amministrazione adeguati poteri ed un supporto di un Comitato Privacy (composto dal Direttore Audit & Compliance, dal Chief Technology Officer e dal Direttore Affari Legali e Societari).
- È stato nominato, quale consulente esperto (Advisor), un primario studio legale internazionale.
- È stato nominato un gruppo di lavoro (Steering Committee), con rappresentanti delle diverse Direzioni e Società del Gruppo, dedicato al presidio e al monitoraggio continuo di tutte le fasi del percorso.
- Come previsto dal Regolamento:
  - è stato adottato un applicativo per la gestione del registro dei trattamenti e per la gestione di tutta la documentazione Privacy;
  - è stato eseguito un censimento aggiornato di tutti i trattamenti in essere;
  - è stato realizzato un inventario dei sistemi e dei dati relativi.
- È stata disegnata la struttura organizzativa per la tutela della Privacy, con l'identificazione in ogni Direzione e Società Controllata, di un Privacy Officer, responsabile dell'utilizzo dell'applicativo adottato;
- È stata completata la analisi dei rischi, con il supporto dell'Advisor legale, e definito il piano di interventi ai fini dell'adeguamento mentre è in fase di completamento un ulteriore percorso di valutazione, di carattere più tecnologico, per identificare gli eventuali possibili miglioramenti della struttura tecnica.

### **Cosa sarà completato entro il 25 maggio**

- Una completa revisione e ottimizzazione delle informative sulla privacy, con particolare attenzione alla corretta e completa informazione degli utenti dei portali e delle piattaforme informative, sui loro diritti e sulle modalità per esercitarli e tutelarli.
- Una completa revisione e ottimizzazione delle informative sulla privacy dedicata ai fornitori ed ai Clienti, delle loro informazioni presenti sui portali e per i siti custom realizzati per loro da Kiamafacile.
- Una accurata revisione e adeguamento delle clausole contrattuali standard sulla privacy adottate per le diverse macro categorie.
- La stesura e/o la revisione delle procedure e delle policy per i diversi ulteriori adempimenti privacy (diritto all'oblio, portabilità del dato, conservazione, etc.) previsti dal GDPR
- La definizione e adozione di una struttura organizzativa a presidio della Tutela Privacy e le relative necessarie nomine interne di delegati, privacy officer, autorizzati al trattamento dei dati (ex "incaricati del trattamento") e di responsabili esterni e contitolari.

- La predisposizione di un articolato piano di sensibilizzazione e formazione di dipendenti e agenti sulla cultura della protezione dei dati, sulle policy e sulle normative di sicurezza a presidio e tutela dei dati delle persone
- La valutazione dell'eventuale necessità di un ulteriore successivo piano di interventi tecnici.
- L'adozione e la regolarizzazione di un nuovo PIA (Privacy Impact Assessment), di un processo cioè codificato e strutturato in fasi – un vero strumento operativo - che supporterà l'organizzazione aziendale nel monitoraggio sistematico, per individuare e ridurre tempestivamente i rischi di violazione dei dati.

**Tutto questo fa parte di un percorso di coinvolgimento, di collaborazione e di trasparenza che Kiamafacile propone quotidianamente a tutti i suoi Clienti e a chiunque si trovi coinvolto, direttamente o indirettamente, nell'attività della più grande internet company italiana: per arrivare a costruire e sottoscrivere un vero patto di fiducia, un bene prezioso da conquistare e ancor più da mantenere, per generare il massimo valore reciproco.**

**RESTA IN CONTATTO PER CONOSCERE TUTTI GLI AGGIORNAMENTI!**

The logo for KIAMAFACILE features a large, stylized letter 'K' on the left. Inside the negative space of the 'K', there is a small globe icon. To the right of the 'K', the word 'IAMAFACILE' is written in a large, grey, serif font. The 'I' is slightly smaller than the other letters.