EU's General Data Protection Regulation
Directive 679/16

ROAD MAP: a simple overview

KIBStudio - Via XIII martiri, n° 88 - 30027 - San Donà di Piave (VE)

Sommario:

Introduzione……3

Violare il GDPRE: sanzioni amministrative e penali……4

Gestire i dati: tipologia e rilevanza……5

I protagonisti del GDPR……7

Data Protection Officer: la nuova figura di supporto al trattamento dei dati……8

Applicare il GDPR……9

Lasciare una traccia: il registro dei trattamenti……10

L'elenco di controllo……10

Introduzione

Dal 25 Maggio 2018 è in vigore, in tutti i Paesi dell'Unione Europea, il Regolamento Generale sulla protezione dei dati (cd. GDPR dall'inglese General Data Protection Regulation).

La norma in particolare:

- Detta gli obblighi riguardanti i il trattamento dei dati dei cittadini europei;
- Contiene i principi sulla protezione delle persone fisiche relativamente al trattamento dei dati personali;
- Elenca i presupposti per la libera circolazione dei dati personali.

Il Codice Privacy (D. Lgs. 196/2003) risulta armonizzato al GDPR attraverso il D. Lgs 101/2018, il quale lascia invariati una parte dei precedenti obblighi aggiungendone altresì di nuovi caratterizzati da logiche completamente rivisitate e orientate:

- Alla comprensione del rischio potenziale, insito nel trattamento dei dati;
- All'accountability (responsabilità) sulle proprie azioni in relazione alle misure adottate per il trattamento dei dati.

È fondamentale, per qualsiasi azienda, cogliere l'importanza delle novità introdotte dal GDPR che non deve essere inteso semplicemente come "nuova norma" ma come uno dei più grossi e discussi cambiamenti del XXI secolo.

Lo scopo[1] è dunque non solo fare chiarezza sul contenuto del Regolamento, illustrare i cambiamenti che esso comporta per le organizzazioni e fornire un breve vademecum su come devono essere gestiti correttamente i dati personali. Questo E-Book intende far riflettere sulla necessità di salvaguardare le figure coinvolte nella gestione del trattamento dalle possibili conseguenze derivanti dal non rispetto della normativa.

> *"La privacy non è qualcosa di separato dal rispetto e dalla dignità umana.*
>
> *Tim Cook"*

[1] **Dichiarazione di limitazione di responsabilità:**
Il contenuto di questo documento è da considerarsi puramente illustrativo, non esaustivo, ed assolutamente non paragonabile ad una consulenza legale sull'applicazione del GDPR. Pur rispettando i suggerimenti contenuti all'interno non si garantisce in alcun modo il pieno rispetto della privacy secondo i principi impartiti dal Regolamento UE.

Violare il GDPR: sanzioni amministrative e penali

Il sistema sanzionatorio ricopre sicuramente un ruolo centrare all'interno del GDPR, a sostegno di una materia, quella della privacy, finora sottovalutata sia a livello di importanza rispetto alla tutela della vita privata delle persone fisiche, sia per quanto concerne il livello di rischio nelle attività di gestione dei dati.

A livello amministrativo il Regolamento prevede:

Multe fino a 10 Milioni di Euro o, per le imprese, fino al 2% del fatturato annuo complessivo annuale (il più alto tra i due). →

Per (a titolo esemplificativo):

- Violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- Trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- Mancata o errata notificazione e/o comunicazione di un Data Breach all'Autorità nazionale competente;
- Violazione dell'obbligo di nomina del DPO;
- Mancata applicazione di misure di sicurezza.

Multe fino a 20 Milioni di Euro o, per le imprese, fino al 4% del fatturato annuo complessivo annuale (il più alto tra i due) →

Per (a titolo esemplificativo):

- Attestata violazione dei principi e delle norme del GDPR, con comprovato danno sugli interessati.
- Inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- Trasferimento illecito cross-border di dati personali ad un destinatario in un Paese terzo.

A livello penale invece il GDPR non prevede sanzioni specifiche, ma concede agli Stati membri UE di disporre diversamente riguardo alla fattispecie nel proprio ordinamento. A tal proposito, con l'entrata in vigore del D. Lgs. 101/2018 sono state predisposte sanzioni penali, ai sensi del riformato Codice Privacy, nei seguenti casi:

- Trattamento illecito dei dati;
- Comunicazione e diffusione illecita di dati personali, oggetto di trattamento su larga scala;
- Acquisizione fraudolenta di dati personali, oggetto di trattamento su larga scala;
- Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
- Inosservanza dei provvedimenti del Garante.

Il **Garante per la protezione dei dati personali** è l'organo competente ad infliggere le sanzioni elencate, ai sensi dell'articolo 15/3 del D. Lgs. 101/2018. Il suddetto organo collegiale deve valutare ogni caso di violazione, in modo tale da impartire sanzioni effettive, proporzionate e dissuasive (art. 83/1 GDPR), alla luce delle circostanze di cui all'art. 83/2 GDPR.

Gestire i dati: tipologia e rilevanza

Il Regolamento fa riferimento ad una serie di dati che devono essere rigidamente sottoposti a criteri di controllo, conservazione e tutela. Non esistendo però un confine netto tra categorie, vengono spesso a crearsi sovrapposizioni che possono causare incomprensione sui criteri effettivamente attuabili. Al fine di rendere più chiare le disposizioni a riguardo, di seguito forniamo un elenco meramente esplicativo.

Dati personali

Le informazioni che, prese singolarmente o combinate, identificano un individuo o lo rendono identificabile sono chiamate "dati personali". All'interno di questo gruppo troviamo:

- Nome e Cognome;
- Dati riportati sulla Carta di Identità;
- Indirizzo e-mail o cellulare;
- Nazionalità o genere;
- Coordinate bancarie;
- Indicazioni mediche generiche;
- Dati web di geolocalizzazione;
- Indirizzo IP o cookies;
- Informazioni sulla persona fisica in genere.

Dati particolari (ex sensibili)

Questa categoria di dati comprende informazioni mediche specifiche, indicazioni sull'etnia di una persona, sul suo orientamento sessuale o politico, sulla sua fede o credenza religiosa, sulla sua filosofia o sul suo stile di vita. Anche le impronte digitali e i dati biometrici in genere ricadono all'interno di questa tipologia.

Le Organizzazioni che elaborano dati personali sensibili sono chiamate ad adottare misure e tecniche di sicurezza più corpose.

Dati ad alto rischio (se dati personali e/o particolari cui può essere associata la definizione del rischio)

> *"**I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale**, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".*
>
> ***Considerando 75 GDPR***

In caso di utilizzo di nuove tecnologie e/o dati "ad alto rischio" per i diritti e le libertà delle persone è necessario il Formal Data Privacy Assestment (c.d. DPIA). Tale istituto mira a valutare il rischio che comporta l'attività sistematica ed estesa di elaborazione (anche su larga scala) di particolari tipologie di dati, nonché il monitoraggio sistematico di aree pubbliche (CCTV).

La necessità dello svolgimento del DPIA resta una valutazione in capo al titolare e/o al responsabile del trattamento dei dati, in virtù del principio di accountability precedentemente citato. Il WP-29, oggi European Data Protection Board [2], incoraggia la sua esecuzione anche in caso di mancata esigenza, in quanto strumento utile, per i titolari del trattamento, al rispetto della legge sulla protezione dei dati, mentre l'articolo 35/3 del GDPR espone le **casistiche generiche** che richiedono il suo svolgimento:

a) Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) Il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il regolamento non specifica cosa rappresenti un trattamento "su larga scala". Il Gruppo di lavoro WP-29 ha tuttavia inserito delle raccomandazioni all'interno del documento: "Linee guida sui responsabili della protezione dei dati" invitando in particolar modo a tenere conto, dei fattori qui elencati al fine di stabilire se un trattamento sia effettivamente effettuato **su larga scala**:

- Il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- Il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- La durata, ovvero la persistenza, dell'attività di trattamento;
- La portata geografica dell'attività di trattamento.

Relativamente al richiamo del Considerando 75 in merito ai "diritti e libertà delle persone fisiche", va precisato inoltre che tale espressione si riferisce nello specifico alla protezione dei dati e alla vita privata, ma includendo anche gli altri diritti fondamentali dell'uomo (libertà di parola, libertà di pensiero, libertà di circolazione, divieto di discriminazione, diritto alla libertà di coscienza e di religione).

[2] L'European Data Protection Board, o Comitato europeo per la protezione dei dati è l'organismo che ha sostituito il Gruppo di lavoro articolo 29 (Working Party article 29 o WP29, […]. Il suo compito principale è garantire il principio di congruità e coerenza, cioè assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia. […].
Fonte: https://protezionedatipersonali.it/gruppo-di-lavoro-art-29.

I protagonisti del GDPR

Molte imprese gestiscono di routine la raccolta, l'elaborazione e lo scambio di dati personali. Definire le figure interessate dal trattamento dei dati e quelle previste dal GDPR, puntando inoltre ad una piena comprensione del livello di responsabilità, è strettamente necessario, al fine di condurre le normali attività aziendali nel pieno rispetto della normativa in materia. Queste figure sono:

- **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (GDPR art. 4 p.7).

- **Contitolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, unitamente agli altri titolari del trattamento, "determina congiuntamente le finalità e i mezzi del trattamento […]" (GDPR art. 26 p.1).

- **Responsabile del trattamento dei dati:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 p.8, art. 28).

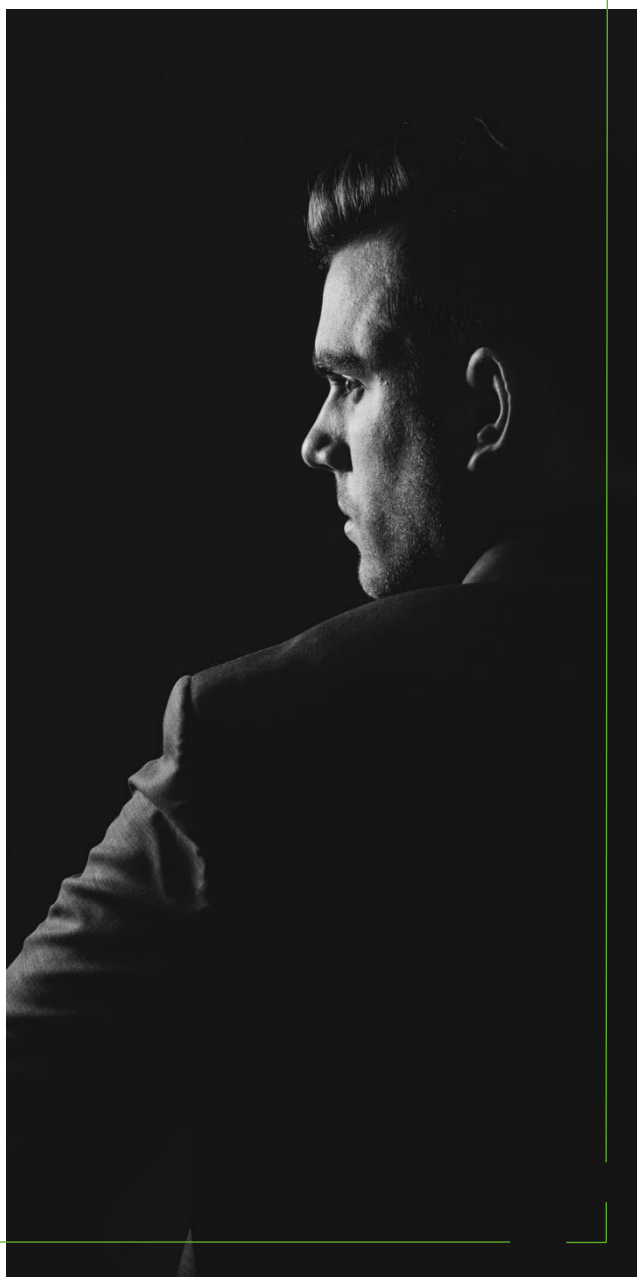
- **Sub-responsabile:** nominato dal responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e il primo responsabile (art. 28 p. 4).

- **Interessato:** è la persona fisica a cui si riferiscono i dati personali (art. 4 p.1), a cui la normativa attribuisce specifici diritti.

- **Incaricato (o autorizzato):** è il soggetto, persona fisica, che effettua materialmente le operazioni di trattamento sui dati personali. Il GDPR non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 GDPR).

Data Protection Officer: la nuova figura di supporto al trattamento dei dati

A partire dalla fase di acquisizione, la protezione delle informazioni deve essere tutelata attraverso adeguati servizi. A tal proposito è stata introdotta una nuova figura: il Data Protection Officer, incaricato di affiancare il titolare ed il responsabile del trattamento dei dati.



In particolare **il DPO**:

- Vigila sull'osservanza del Regolamento e, più in generale, della normativa vigente in materia di privacy;
- Informa e affianca il Titolare del trattamento nella gestione degli obblighi impartiti dal Regolamento e dalla normativa privacy;
- Svolge una funzione di supporto al Titolare in ogni azione che coinvolga il trattamento di dati personali (compresa la stesura del Registro dei dati del trattamento);
- Collabora con il Titolare e/o con il Responsabile del trattamento nella valutazione dei DPIA;
- Collabora con il Titolare e/o con il Responsabile del trattamento nel promuovere la cultura della protezione dei dati all'interno dell'azienda, formazione e sensibilizzazione;
- Si costituisce elemento di contatto tra l'Autorità Garante ed il Titolare del trattamento, in materia di protezione dei dati personali.

Tre sono i casi specifici in cui è necessaria l'introduzione del DPO:

1. Quando ad effettuare il trattamento è un'autorità o organismo pubblico, fatta eccezione per le autorità giurisprudenziali nell'esercizio delle loro funzioni giurisprudenziali (art. 37 p. 1, a);
2. In presenza di trattamenti che per loro natura, ambito di applicazione e finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala (art. 37 p. 1, b);
3. Trattamenti su larga scala di categorie particolari di dati personali e dati relativi a condanne penali e a reati (art. 37 p. 1, c).

Applicare il GDPR

Grazie al principio dell'accountability, titolari e responsabili del trattamento, prendono coscienza circa l'importanza delle proprie azioni a tutela dei dati personali delle persone fisiche, contemplando inoltre la possibilità di doverne rendere conto a terzi che ne fanno richiesta. Naturale conseguenza di ciò, è l'adozione di politiche e misure adeguate a dimostrare il massimo impegno nel rendere il trattamento dei dati conforme al GDPR. Cosa può fare un'organizzazione per adeguarsi fin dal subito al Regolamento e alla normativa sulla privacy?

1. FORMAZIONE

Un primo passo riguarda la formazione e la sensibilizzazione alla tematica. Tutti i dipendenti, i colleghi, i collaboratori ed i partner devono essere consapevoli dell'importanza del Regolamento ed essere adeguatamente istruiti ad agire nel rispetto dalla privacy.

Attività riguardanti la formazione e la conoscenza della materia possono essere:

- Corsi di formazione con approfondimento a vari livelli;
- Conferenze con esperti del settore e figure specifiche coinvolte;
- Studio di case history con relativi dibattiti.

2. GESTIONE

Un secondo step mira ad una corretta gestione dei processi di trattamento (acquisizione, elaborazione e trasferimento). Qualunque tipologia di attività che possa, direttamente o indirettamente, coinvolgere informazioni personali o particolari (specialmente se rientranti nelle casistiche di alto rischio), deve essere trattata conformemente al GDPR, predisponendo inoltre la relativa e aggiornata documentazione.

Nello specifico tra le attività suggerite rientrano:

- Audit relativi alla mappatura dei dati e dei processi di gestione delle informazioni;
- Predisposizione dei documenti aggiuntivi introdotti dal Regolamento[3];
- Adesione a codici di condotta specifici (es. riguardo l'uso di smartphone o altri strumenti);
- Adeguamento dei documenti legali interni;
- Aggiornamento dei contratti stipulati;
- Accertamento dell'effettivo ottenimento dell'autorizzazione al trattamento.

3. MONITORAGGIO

Terzo passaggio riguarda la valutazione d'impatto sulla privacy. In presenza di modifiche alle politiche e configurazioni interne aziendali, è bene monitorare gli sviluppi interni in relazione alla normativa, al fine di accertare la corrispondenza delle procedure adottate per la tutela dei trattamenti con quelle suggerite dal GDPR.

In questo caso attività che possono essere svolte sono:

- Valutazione preventiva della rilevanza dei dati;
- Accertamento sul livello di sicurezza della strumentazione utilizzata;
- Descrizione sistematica dei trattamenti previsti;
- Valutazione dei rischi per i diritti e le libertà.
- Previsione di misure per affrontare i rischi.

[3] Vedi il Registro dei Trattamenti pag. 10

Lasciare una traccia: il registro dei trattamenti

Il GDPR prevede che tutti i trattamenti e le relative operazioni debbano essere sistematicamente tracciate. Per lo svolgimento di questa operazione si ricorre al "registro dei trattamenti", utilissimo strumento introdotto dall'articolo 30 del Regolamento. Esso intende rappresentare un valore aggiunto non solo per quelle realtà che, per legge, hanno l'obbligo di registro delle attività privacy, ma più in generale, per tutte quelle organizzazioni che intendono dimostrare un allineamento ed un impegno concreto nel rispetto della normativa.

Gli elementi del registro sono:

- Finalità del trattamento (le motivazioni per cui è richiesto);
- I termini inerenti la cancellazione delle varie tipologie di dati;
- Descrizione relativa alle categorie di interessati;
- Informazioni di contatto relative a Titolare (ed eventuali Contitolari), Responsabile, e Responsabile della protezione dei dati (DPO);
- Una spiegazione generica riguardante le misure di sicurezza organizzative e tecniche di cui all'articolo 32, p. 1;
- Traccia e descrizione relativa al trasferimento del dato e la documentazione, contenente le garanzie adeguate, relativa ai trasferimenti di cui al secondo comma dell'articolo 49;
- Specifica sui destinatari a cui sono stati o verranno comunicati i dati, compresi i destinatari di paesi terzi UE ed eventuali organizzazioni internazionali.

L'obbligo di tenuta del registro dei trattamenti compete alle organizzazioni che:

- Trattano informazioni potenzialmente rischiose per i diritti e le libertà dell'interessato;
- Sono composte da almeno 250 dipendenti.

L'elenco di controllo

Un ultimo valido strumento per allineare le organizzazioni alle regole del GDPR è la Check List di controllo, un vero e proprio elenco di domande su cui riflettere e mettere chiarezza al fine di ottenere un quadro quanto più esaustivo possibile sulla gestione interna del trattamento dei dati.

Dati Personali raccolti da cittadini UE

1. Quali sono i dati personali raccolti?
2. I dati personali vengono trasmessi? come?
3. Restano all'interno dell'UE?
4. Dove vengono memorizzati i dati personali?
5. Quali sono le procedure di conservazione dei dati personali?
6. Chi si occupa della custodia dei dati personali?

Procedure per il Consenso alla raccolta Dati Personali

1. Viene evidenziato chiaramente il responsabile del trattamento e il responsabile della protezione?
2. Il consenso viene richiesto esplicitamente e con termini inequivocabili?
3. Come possono gli interessati accedere ai propri dati personali?
4. Sono esplicati I tempi di memorizzazione del dato?
5. Gli interessati hanno diritto ad accedere ai loro dati personali, correggerli, richiederne l'eliminazione?
6. Il ritiro del consenso è facile da effettuare?
7. Vengono evidenziate le conseguenze in caso si decidesse di non fornire dati personali?
8. Il trasferimento eventuale dei dati extra UE è comunicato in modo chiaro?
9. L'invio dell'informazione in caso di violazione dei dati personali è a norma di legge?

Procedute per la manutenzione dei registri dei dati e le policy per l'elaborazione dei dati

1. Viene tenuta una registrazione del trattamento dei dati personali?
2. Qual è il livello di sicurezza relativo alle registrazioni dei dati personali?
3. I consensi vengono registrati?
4. Sono previste azioni contro vulnerabilità incidenti che possono mettere a rischio i dati?
5. Vengono aggiornate le specifiche sulle procedure per l'elaborazione dei dati personali?
6. Esiste una procedura per inviare, entro 72 ore, le notifiche di Data Breach?
7. C'è una procedura per valutare la possibilità di operazioni a rischio?
8. Viene compilato un registro delle modificazioni delle procedure?
9. Il contratto è conforme al GDPR nei casi di elaborazioni dei dati esternalizzate?
10. Vi è un responsabile della protezione dei dati personali?
11. Che controllo viene effettuato per l'accesso a server o edifici ove sono contenuti i dati?
12. C'è un rappresentante nella UE per eventuali titolari non UE

Comportamento degli operatori

1. Sono presenti ed aggiornati adeguati strumenti antivirus e/o anti-malware?
2. Viene svolta una adeguata formazione del personale?
3. Esistono documenti interni riguardanti il trattamento dei dati?
4. Chi è responsabile per le credenziali di accesso ai sistemi?
5. Vengono eseguiti backup dei dati? Esiste un responsabile?
6. Vengono disattivati profili relativi a rapporti di lavoro cessati?
7. Vengono individuati ed arginati gli accessi sospetti ai sistemi?
8. Viene garantita la Business Continuity?

Questi sono solo alcuni e più immediati suggerimenti che possono essere attuati, ma le possibilità per aumentare il livello di sicurezza e di tutela dei dati trattati sono davvero numerose e spesso richiedono una conoscenza davvero approfondita della materia.

Il ricorso a servizi di affiancamento e/o l'inserimento di figure ufficiali, altamente specializzate all'interno della propria organizzazione, è il metodo migliore, più veloce e soprattutto sicuro per tutelare sé stessi e l'effettivo interessato del trattamento.

Kibs Studio, a fronte di ciò, mette a disposizione servizi operativi (privacy manager) o di affiancamento alla direzione (privacy manager), a chiunque abbia la necessità di valutare e o trattare dati personali e particolari.

Kibsstudio.com

*** KIBS Studio è un marchio ONE OFF Services scpa

SEDE LEGALE
One Off Services S.C.P.A
Viale XXIV Maggio, N°5
34170 - Gorizia (GO)

SEDE OPERATIVA VENETO
Via XIII Martiri, N°88
Tel./Fax. +39 0421 - 223661
30027 - San Doná Di Piave (VE)
kibsstudio@kibsstudio.com

SEDE OPERATIVA EMILIA - ROMAGNA
Via Armando Gnani, N°54
Tel. +39 0544 - 502170
48124 - Ravenna (RA)