consulenti PRIVACY srl

EVITA LE SANZIONI PRIVACY CON 5 SEMPLICI MOSSE! (PIÙ UNA)

A CURA DI:

Dott. Paolo Rosetti - CEO & DPO certificato
Massimiliano Sarto - DPO & Lead Auditor certificato

Avv. Fabio Pari - Avvocato del Foro di Rimini
Avv. Eugenia Canistro - Avvocato del Foro di Rimini
Avv. Filippo Capanni - Avvocato del Foro di Rimini

Rimini - Via Valentini 11
Milano - Piazza Città di Lombardia 1
Bologna - Via Vittorio Lugli 4/A-D
Ferrara - Viale Krasnodar 25

Vesione aggiornata al 15/09/2020

consulenti PRIVACY srl

LA TUA AZIENDA STA RISCHIANDO?

Dal 25 maggio 2018 è in vigore il Reg. UE n. 679/2016, conosciuto anche come GDPR. **La nuova normativa "responsabilizza" le aziende** che trattano dati personali, prescrivendo l'adozione di misure organizzative e tecniche adeguate per la tutela dei diritti e delle libertà delle persone fisiche.
In caso di controllo, **il Titolare del trattamento (che coincide con il titolare della attività) dovrà dimostrare di aver adottato politiche interne e misure adeguate al fine di evitare pesanti sanzioni amministrative** (che possono arrivare a sino a 20 milioni di euro per le violazioni più gravi o fino al 4% del fatturato annuo) ed eventuali responsabilità penali (ad esempio in caso di false comunicazioni al Garante).

Sappiamo già a cosa stai pensando: *"Non controlleranno mai le piccole-medie imprese!"* oppure *"Prima di fare controlli a noi partiranno da Google, da Facebook, dalle banche!"*.
Spesso, per queste false convinzioni, imprenditori e professionisti non si sono adeguati o hanno optato per adeguamenti low-budget puramente di facciata. In realtà tali credenze non hanno nessun riscontro nella realtà, tant'è che i**l Garante ha già sanzionato diverse imprese italiane** per il mancato rispetto della normativa e spesso lo ha fatto anche in presenza di documenti "formalmente ineccepibili" che, però, non avevano alcuna applicazione nella realtà aziendale.

Non ci credi? **Ecco alcuni esempi!**

LE SANZIONI

- Provvedimento n. 124/2020, **Supermercato**, illecito trattamento dei dati di un dipendente, sanzione **Euro 1.000,00**
- Provvedimento n. 115/2020, **Azienda di produzione di materiali chimici per l'edilizia**, illecito utilizzo/mancata disattivazione e-mail ex dipendente, sanzione **Euro 15.000**
- Provvedimento n. 17/2020, **Università**, data breach – misure di sicurezza insufficienti, sanzione **Euro 30.000**
- Provvedimento n. 118/2019, **Medico**, Misure di sicurezza insufficienti, sanzione **Euro 1.250**
- Provvedimento n. 120/2019, **Sito internet**, Diffusione di dati senza consenso, sanzione **Euro 10.000**
- Provvedimento n. 95/2019, **Telemarketing – social media**, Omissione informativa e mancata raccolta del consenso, sanzione **Euro 2.018**
- Provvedimento n. 91/2019, **Rivenditore telefonia**, Trattamento di dati all'insaputa degli interessati, sanzione **Euro 40.000**
- Provvedimento n. 102/2019, **Servizi alberghieri**, Errata acquisizione del consenso marketing modulo di prenotazione on-line, sanzione **Euro 4.000**
- Provvedimento n. 49/2019, **Medico**, Omissione informativa e utilizzo dei dati per finalità diverse da quelle di cura, sanzione **Euro 16.000**
- Provvedimento n. 39/2019, **Esercizio commerciale**, Conservazione immagini video-sorveglianza oltre il tempo massimo consentito, sanzione **Euro 11.940**
- Provvedimento n. 472/2018, **Concessionario di automobili**, Omissione informativa e omessa raccolta consenso, sanzione **Euro 18.400**
- Provvedimento n. 468/2018, **Agenzia immobiliare**, Comunicazione dei dati personali a soggetti terzi senza consenso dell'interessato, sanzione **Euro 4.000**

A queste sanzioni si aggiungono quelle comminate a ENI Gas&Luce e TIM per **pratiche marketing scorrette**, rispettivamente di 11 e 27 milioni di euro e quella ad UNICREDIT, per 600 mila euro, a causa di un **data breach,** oltre a quelle a WIND TRE e ILIAD, ciascuna di euro 16 milioni e 800 mila euro, per diverse **irregolarità nel trattamento dei dati degli utenti**.

LE 5 MOSSE!

Cosa fare, allora, per evitare le sanzioni?
Prima di tutto **dovranno essere osservate le 5 "regole d'oro"(più una)** che spiegheremo brevemente in questa guida!

PRIMA MOSSA: FORMARE!

Il GDPR prevede espressamente l'obbligo di formare e responsabilizzare i propri collaboratori. Occorrerà quindi istruirli e incaricarli al trattamento dei dati che la vostra azienda tratta.

Questo adempimento è spesso sottovalutato e i dipendenti si trovano a non saper gestire i dati personali. **Il fattore di rischio più elevato per la sicurezza dei dati è infatti l'errore umano.** Noi pensiamo che **la formazione sia un'opportunità di crescita**: i regolamenti in generale suonano sempre come noiosi, ma il GDPR deve essere considerato da tutti come un'opportunità di crescita personale e non solo per l'azienda, in un mondo dove la condivisione delle informazioni è qualcosa che va oltre la propria attività lavorativa. Inoltre, acquisire *know-how* su privacy e sicurezza informatica fa prendere coscienza al personale dei rischi che si corrono trascurando o sottovalutando questi aspetti anche nella vita privata.

Durante le nostre attività di consulenza garantiamo la formazione del personale aziendale attraverso lezioni frontali tenute dai qualificati professionisti che compongono il nostro team.

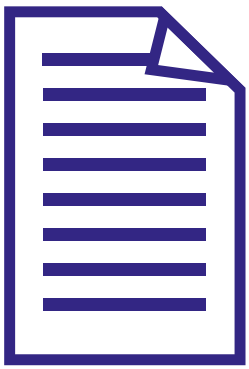
SECONDA MOSSA: INFORMARE!

Le **informative sono una parte importantissima** della documentazione necessaria per rispettare la normativa privacy. Dovrà essere redatta un'informativa per ogni categoria di destinatari, ad esempio clienti, fornitori e dipendenti.
Con questo documento l'azienda comunica ai terzi le regole ed i criteri utilizzati per il trattamento dei loro dati personali.
Non si tratta però solamente di un obbligo: diverse ricerche di mercato hanno dimostrato che i clienti preferiscono rivolgersi ad aziende e partner commerciali che, dando prova di essersi adeguate alla normativa, **trasmettono un'idea di serietà e trasparenza.**

Cosa deve contenere l'informativa?

L'informativa deve avere un contenuto "minimo", previsto dagli artt. 13 e 14 del GDPR. Ad esempio, le categorie di dati trattati, quali siano le finalità del trattamento, le basi giuridiche sulle quali effettuiamo quel determinato trattamento, i termini di conservazione, la richiesta di consenso per determinate tipologie di trattamento (ad es. il marketing).

Redigere l'informativa conformemente al GDPR è una tra le prime attività da svolgere per adeguarsi al Regolamento. Le tue informative sono a prova di GDPR? Raccogli correttamente il consenso quando serve?



TERZA MOSSA: DOCUMENTARE!

Il Registro dei trattamenti è il primo documento che viene richiesto in caso di ispezione e per quel momento dovrà essere pronto e aggiornato. Pronto significa: completo di tutti i flussi di dati che circolano all'interno dell'azienda, chiaro ed esaustivo. **L'importante è non dimenticarsi del proprio Registro:** rappresenta una fotografia della nostra azienda e come tale deve riprodurre la situazione attuale dell'organizzazione e deve essere sempre aggiornato.

Anche tu devi "avere" il Registro?

Le Linee Guida del Garante precisano che rientrano nell'obbligo di tenuta del registro:

- aziende, esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.;

- associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);

- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Per chiarire, la gestione delle buste paga non è un trattamento occasionale, come anche la gestione dei clienti e dei fornitori. Quindi qualsiasi azienda con almeno un dipendente è tenuta alla redazione del registro.

La nostra attività di consulenza prevede almeno un audit annuale presso l'azienda al fine di individuare tutti i trattamenti eseguiti e le modalità con cui i dati sono processati e conservati.

QUARTA MOSSA: NOMINARE!

Pensaci bene: **affidersti mai il tuo patrimonio ad istituti di credito non sicuri?** No, e così dovrebbe essere anche per i dati di cui sei Titolare.
Ogni consulente – commercialista, consulente del lavoro, webmaster, agenzie di marketing ecc. – **deve essere nominato Responsabile esterno del trattamento** dei dati personali che gli vengono affidati per lo svolgimento dei rispettivi compiti.

Ma chi è il Responsabile esterno?

Il responsabile esterno del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Si tratta di 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.

Il Titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento, e che le sue decisioni siano conformi alle leggi. Compito specifico del Titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili.

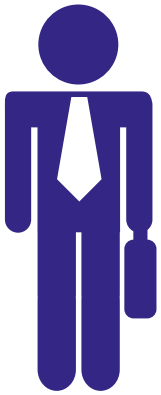
Il titolare deve sempre poter sindacare le decisioni dei responsabili ed i trattamenti affidati devono essere disciplinati da un contratto o altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati.

Ti chiederai: quindi? cosa devo fare?
Ai sensi dell'art. 28 GDPR, dovrai:

- **Nominare** formalmente i soggetti individuati come Responsabili esterni del trattamento

- Effettuare una ***due diligence*** sulle garanzie prestate dai designandi Responsabili in ordine al rispetto della normativa privacy vigente

Nel corso dell'adeguamento il nostro team individuerà i soggetti a cui "affidi" i dati dei tuoi clienti e dei tuoi dipendenti, procedendo alla redazione delle nomine richieste e supportandoti nelle attività di due diligence



QUINTA MOSSA: PREVENIRE!

Lo sappiamo tutti: **il dato è sempre più digitale!** È quindi fondamentale **curare la sicurezza del tuo sistema IT**: aggiornare i sistemi operativi, dotarti di antivirus professionali, verificare la vulnerabilità degli stessi ad intrusioni non autorizzate.

Cosa succede se subisco un attacco?

Le conseguenze di un attacco informatico sono molteplici (e nessuna di queste è piacevole!):

- **comunicazione al Garante entro 72 ore** dalla scoperta dell'accaduto qualora vengano compromessi o trafugati dati personali (es. dei tuoi clienti)
- **perdita di credibilità commerciale** nei confronti di clienti e fornitori non va sottovalutata, i quali avranno la percezione di aver affidato i propri dati personali ad una impresa non sicura (solo sulla privacy?)
- **attività paralizzata** e richiesta di riscatto per avere accesso ai propri dati (capita spesso infatti che professionisti del crimine informatico riescano a "sequestrare" tutti i dati presenti nel sistema informatico aziendale, chiedendo ingenti riscatti in BITCOIN)

Prevenire è meglio che curare!

Il primo passo è quello di affidare a professionisti del settore l'analisi del livello di sicurezza informatica dell'azienda, in modo da individuarne i gap e procedere con un piano efficace di remediation.

Nella nostra attività di consulenza prestiamo particolare attenzione al tema della cyber security, ritenendo che i seguenti interventi siano di fondamentale importanza per un completo adeguamento dell'azienda alla normativa privacy:

- **people security**, con soluzioni che vanno dall'identity and access management al self-service single sign-on, passando per sistemi di governance and compliance e authentication and authorization;

- **software security,** per la messa in sicurezza delle applicazioni e degli ambienti It attraverso tecnologie di API management, audit, patching e configuration, application performance, ecc.;

- **data security**, analisi delle minacce informatiche incombenti sul perimetro aziendale, crittografia e soluzioni di mascheramento dei dati, soluzioni per il controllo dei privilegi degli utenti.

Richiedi la consulenza di un nostro esperto informatico per eseguire un check della tua struttura informatica e implementare le misure di sicurezza necessarie per la protezione dei tuoi dati e di quelli dei tuoi clienti

MOSSA BONUS: AFFIDARSI A DEI PROFESSIONISTI!

Per noi la privacy non è solo un obbligo, ma rappresenta un'opportunità che l'azienda può sfruttare per porre rimedio ad altre criticità, mantenendo alto il livello di competitività sul mercato.
La nostra attività di adeguamento si distingue per il costante affiancamento del cliente, che non viene mai lasciato solo nella gestione di tutti gli adempimenti iniziali e nel processo di mantenimento della conformità nel corso del tempo

SCOPRI DI PIÙ E VIENI A CONOSCERE IL NOSTRO TEAM SU:

WWW.ICONSULENTIPRIVACY.IT

CONTATTI:

info@iconsulentiprivacy.it
0541 1798723

Rimini - Via Valentini 11
Milano - Piazza Città di Lombardia 1
Bologna - Via Vittorio Lugli 4/A-D
Ferrara - Viale Krasnodar 25