
La prima guida in italiano sulla privacy per le
piccole imprese e le PMI

Il nuovo Regolamento Europeo sulla Privacy UE 2016/679



dott. Stefano Schmidt
Esperto Privacy per le PMI,
fondatore di Privacy Solver



Prima edizione
dicembre 2017
ed. a cura di Privacy Solver
marchio della società S.Schmidt Consulting srl
curata dal dott. Stefano Schmidt

Introduzione	5
Primo punto	7
Da maggio del 2018 scatteranno le nuove norme, più rigorose, in materia di protezione dati.....	7
Secondo punto	8
Cosa sono i dati personali?	8
Terzo punto	9
Perché cambiare le regole?	9
Quarto punto	10
Che cosa deve fare la tua azienda?	10
Quinto punto	11
Profilazione	11
Marketing	11
Sesto punto	12
Salvaguardia dei dati sensibili.....	12
Trasferimento dei dati al di fuori dell'UE.....	12
Settimo punto	13
Fai la protezione dei dati in base alla progettazione.....	13
Ottavo punto	14
Controlla se hai bisogno di un responsabile per la protezione dei dati.....	14
Nono punto	15
Tienine traccia	15
Decimo punto	16
Anticipare con valutazioni d'impatto.....	16
Ultimo punto	17
Il costo della non conformità.....	17
Dicono di Noi	19
Privacy Solver è la soluzione ai tuoi problemi privacy aziendali	23

Introduzione

Il 25 Maggio 2018 entra in vigore il nuovo regolamento Europeo sulla Protezione dei Dati Personali UE 2016/679.

Essendo un regolamento Europeo, NON ha bisogno di Decreti Attuativi, né di essere approvato dal Parlamento Italiano.

Quindi il 25 Maggio 2018 è la data ultima.

Detto questo, sappiamo benissimo che la privacy è percepita nelle aziende italiane solo come una scocciatura, una serie infinita di carte da far firmare ed un costo inutile.

E per questo si cercano sempre le strade più economiche per risolvere il problema.

Ma, come in quasi tutti i settori, anche in questo campo vale la regola che chi meno spende, più spenderà in futuro.

Sottovalutando la privacy, addirittura si può spendere di più per tre motivi:

1. Le sanzioni in cui si può incorrere per violazione della privacy.
2. I costi dovuti al non corretto utilizzo dei dati.

Mi spiego meglio.

Hai idea di che cosa sia il blocco dei dati?

No?

Te lo spiego in due parole...

Chiusura azienda.

Troppo catastrofico?

Purtroppo no.

Se tratti i dati dei tuoi clienti in modo non conforme alla normativa sulla privacy, puoi incorrere nel blocco dei dati.

Il Garante può vietarti di utilizzare tutti i dati dei tuoi clienti (non puoi utilizzarli più se non per questioni fiscali), quindi niente più nuove offerte, niente più pubblicità, niente più auguri di buon compleanno.

Dovranno essere loro a richiamarti.

Sempre se nel frattempo non saranno stati chiamati da un tuo concorrente che al contrario di te può farlo.

3. Il costo di un buon consulente dopo che hai fatto da solo o ne hai pagato poco uno scarso.

Questa breve guida vuole spiegare con parole semplici i cambiamenti che introduce il nuovo Regolamento Europeo in materia di Privacy.

Primo punto

Da maggio del 2018 scatteranno le nuove norme, più rigorose, in materia di protezione dati.

Ciò significa che i cittadini hanno un maggiore controllo sui loro dati e sui vantaggi, comportando un maggior impegno per le imprese.

Un insieme di regole per tutte le aziende che operano nell'UE, ovunque si trovino.

Quindi anche se operi da fuori della UE, come lo stato di San Marino, dalla Svizzera o dagli USA.

Scopri cosa significa per la tua PMI.



Secondo punto

Cosa sono i dati personali?

Per dati personali si intendono

- Nome e cognome
- Indirizzo
- Localizzazione
- Identificatore online
- Informazioni sulla salute
- Reddito
- Profilo culturale
- ... e molto altro ancora

Uso dei dati raccolti in negozio? Devi rispettare le regole.
Dati di processo per altre aziende? Questo vale anche per te.



Terzo punto

Perché cambiare le regole?

Si tratta di una questione di fiducia...

Solo il 15% delle persone sentono di avere il controllo dei loro dati forniti online.

La mancanza di fiducia nelle vecchie norme di protezione dati frena l'economia digitale e, molto probabilmente, anche il tuo business.

... E di aiutare il boom commerciale.

Una serie di regole valide per tutte le aziende per trasferire dati nell'UE.

Diventa più facile ed equo fare affari.

Con il nuovo sistema si mantengono i costi più bassi e si aiuta a far crescere il business.

Le nuove regole dovrebbero aumentare la fiducia dei consumatori e, di conseguenza, aumentare il tuo business.

Quarto punto

Che cosa deve fare la tua azienda?

Tutelare i diritti delle persone che ti lasciano i propri dati.

Comunicazione

- Usa un linguaggio semplice.
- Di loro CHI SEI quando richiedi i dati.
- Di loro PERCHE' si elaborano i loro dati, QUANTO tempo di vuole perché vengano memorizzati, e CHI li riceverà.

Consenso

- Ottieni il loro esplicito consenso al trattamento dei dati.
- Raccolta dati dei bambini? Fai attenzione al limite di età, per ottenere il consenso dai genitori.

Accesso e portabilità

- Consenti alle persone ad avere accesso ai loro dati, e permetti che li diano ad altra azienda.

Avvertenze!

- Informa le persone della violazione dei loro dati, laddove c'è un grave rischio per loro.

Cancella i dati

- Dai alle persone il “diritto all'oblio”.
- Cancella i loro dati, se lo richiedono, se questo non compromette la libertà di espressione o la capacità di ricerca.

Quinto punto

Profilazione

Se la tua azienda utilizza la profilazione degli utenti per elaborare i trattamenti dei dati personali, crea accordi vincolanti per te che rispettino una corretta informazione per i tuoi clienti.

Assicurati di avere una persona, e non una macchina a controllo del processo, se il processo può finire con un rifiuto.

Dai sempre la possibilità al tuo cliente di contestare la decisione.

Marketing

Dai sempre alle persone la possibilità di cancellarsi dalle liste a cui si sono iscritte.



Sesto punto

Salvaguardia dei dati sensibili

Utilizza garanzie aggiuntive e maggiore sicurezza per le informazioni sulla salute, razza, orientamento sessuale, religione e credo politico.

Trasferimento dei dati al di fuori dell'UE

Adotta tutte le disposizioni legislative necessarie quando trasferisci i dati in paesi che non sono stati approvati dall'UE.



Settimo punto

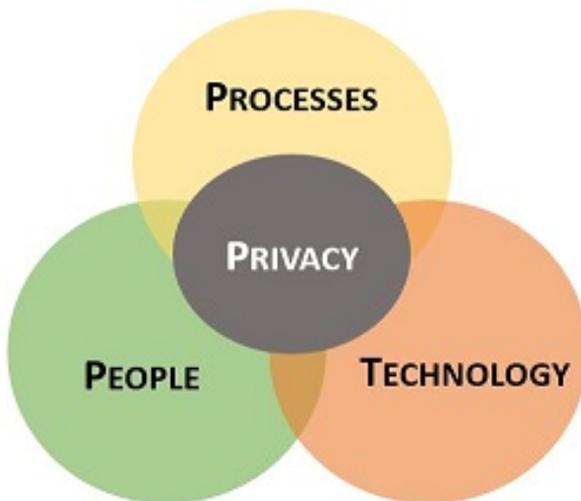
Fai la protezione dei dati in base alla progettazione

Costruisci le garanzie di protezione dei dati personali nei tuoi prodotti e servizi fin dalle prime fasi di sviluppo.

Attenzione!

Elabori i dati per un'altra azienda?

Assicurati di avere un contratto a tenuta stagna che elenca le responsabilità di ciascuna delle parti.



Ottavo punto

Controlla se hai bisogno di un responsabile per la protezione dei dati



Questo non sempre è obbligatorio.

Dipende dal tipo e dalla quantità di dati raccolti, se l'elaborazione è il tuo business principale, e se si fa su larga scala.

SI. Se si elaborano dati personali per indirizzare la pubblicità attraverso motori di ricerca basati sul comportamento delle persone in linea.

NO. Se invii ai tuoi clienti un annuncio una volta all'anno per la promozione della tua attività locale. Ma attenzione, una sola volta all'anno!

SI. Se elabori dati personali su genetica e sanitaria per un ospedale.

NO. Se sei un medico di famiglia e raccogli i dati sulla salute dei tuoi pazienti.

Nono punto

Tienine traccia

Le PMI devono tenere un registro che comprovi:

- Se il trattamento dei dati è regolare
- Se i dati trattati sono una minaccia verso i diritti delle persone e delle loro libertà
- Se trattano dati sensibili o precedenti penali

La documentazione del registro deve contenere:

- Nome e contatti del commercio
- Motivi per l'elaborazione dei dati
- Descrizione delle categorie di persone interessate e dei dati personali
- Le categorie di organizzazioni che ricevono i dati e il trasferimento dei dati stessi in un altro paese o organizzazione
- Termine per la rimozione dei dati, se possibile
- Descrizione delle misure di sicurezza utilizzate durante l'elaborazione



Decimo punto

Anticipare con valutazioni d'impatto

Le valutazioni d'impatto possono essere richieste per le elaborazioni ad ALTO RISCHIO,

come in caso di:

- Nuove tecnologie.
- Automazione, elaborazione sistematica e valutazione dei dati personali.
- Monitoraggio su larga scala di una zona accessibile al pubblico (esempio, telecamere a circuito chiuso).
- Trattamento dei dati sensibili su larga scala, come la biometria.



Ultimo punto

Il costo della non conformità

Il tuo Garante per la Protezione dei Dati locale controlla la conformità. Il suo lavoro è controllato a livello UE.
Il costo per la violazione delle regole può essere alto.

Si può incorrere in una:

- Sospensione dell'elaborazione dei dati
- Sanzione fino a € 20 milioni
e/o
- 4% del fatturato annuo globale della tua azienda.

Se hai aziende estere o hai aziende con cui sei un gruppo aziendale come previsto dal codice civile, si calcola il fatturato di tutto il gruppo.



Vuoi approfondire l'argomento del Nuovo Regolamento Europeo sulla Privacy con video e report dedicati?

Vai alla pagina
bit.ly/BONUSGUIDA

ed accedi ai contenuti bonus dedicati a te.

Dicono di Noi

“Il dott. Stefano Schmidt, unitamente al suo Team, hanno collaborato per oltre 10 anni con la nostra società per garantirci l’assoluto rispetto della normativa in tema di privacy.

Il suo intervento ha riguardato sia la sede centrale che i vari punti vendita in una attività che è stata portata avanti in più steps:

La prima fase ha riguardato l’analisi dello status quo e la identificazione dei gaps rispetto ai requisiti richiesti dalla legge.

La seconda fase ha riguardato la messa a punto di procedure ad hoc volte a garantire la compliance alla legge sia per i punti vendita che per la sede.

La terza fase ha riguardato l’implementazione delle stesse procedure.

Poi si è passati alla fase di mantenimento che consisteva sia nella visita periodica presso le varie sedi operative al fine di controllare il continuo rispetto delle procedure, sia nella gestione dei casi più complessi in cui era necessario anche rispondere alle richieste dei vari clienti sia quando era necessario interloquire con l’Authority preposta, attività quest’ultima, in cui il dott. Schmidt ha sempre dimostrato di sapersi muovere agevolmente grazie a contatti diretti e di continuo e proattivo interscambio informativo con l’Autorità.”

Andrea Scozzoli
Amministratore Delegato
Managing Director
Unieuro S.p.A.

“Ho conosciuto Stefano al mio ingresso in azienda e mi è stato subito di aiuto nell’inquadrare le tematiche fondamentali su cui focalizzare la nostra azione.

Disponibile e competente ha sempre presidiato l’ambito normativo in modo puntuale, aiutandoci a calare nel nostro contesto gli adempimenti per essere conformi alle norme di legge. Nel settore dell’ICT, tale conformità si è spesso tradotta nella capacità di far fronte alle esigenze dei clienti di cui spesso abbiamo in custodia i dati personali. Insomma una collaborazione vincente!”

Ing. Paolo Levizzani
Quality Manager
Acantho SpA

“Il dr. Stefano Schmidt è stato consulente della società Hera Ferrara s.r.l. con l’incarico di assistere la società negli adempimenti connessi alla normativa sulla privacy.

Ha svolto il suo incarico negli anni 2006-2009, all’indomani dell’incorporazione della società multi utility AGEA S.p.A. in Hera S.p.A.

L’incarico svolto dal professionista era in particolare rivolto ad introdurre all’interno della società un sistema di gestione della privacy che prevedeva l’analisi dei rischi connessi al trattamento dati, la gestione delle nomine dei responsabili e degli incaricati al trattamento, l’introduzione di misure di sicurezza, audit interni, informative ai clienti, notifiche al garante e altro ancora.

Nel periodo suddetto il dr. Stefano Schmidt svolgeva le attività professionali in diverse società operative del Gruppo Hera cercando di uniformarne gli adempimenti all’interno del Gruppo stesso in una fase di sviluppo societario in cui non era stata costituita una unità centralizzata adeguatamente strutturata e competente in materia di Privacy.

L’attività del dr. Schmidt è stata quindi importante per accompagnare il Gruppo Hera nella sua prima fase di sviluppo fino a quando a livello organizzativo HERA S.p.A. si è dotata di una propria struttura interna di coordinamento centralizzato degli adempimenti privacy adeguato alla complessità delle proprie attività.

Enrico Bordigoni
Area Manager Ferrara
Direzione centrale rapporti enti locali
HERA S.p.A. Via C.Diana 40 44124 Cassana FE
www.gruppohera.it

Stefano Schmidt

Mi sono laureato all'Università di Bologna alla facoltà di Economia e Commercio.

Mi occupo di privacy dal 2004 anno dell'entrata in vigore dell'attuale testo unico D.Lgs. 196/03.

Ho iniziato a lavorare con clienti di primaria importanza come il Gruppo Hera, Marcopolo Expert, oggi Unieuro; nel campo delle telecomunicazioni con Acantho; ho tenuto innumerevoli corsi di formazione, tra cui anche per il personale dei comuni dell'Alto Reno (Porretta Terme, Gaggio Montano ecc); interagito con Telecom e Vodafone, maturando in questi anni una elevata esperienza nel campo della privacy.

Interagisco costantemente con l'Autorità Garante per la protezione dei dati personali, sia partecipando a corsi di aggiornamento, sia in prima persona come consulente di parte.

La domanda sovente che mi viene fatta è come mai mi chiamo Schmidt; mi piace raccontare la storia della mia famiglia partendo con un incipit che lascia le persone smarrite, "la mia famiglia viene da Monaco di Baviera – Austria".

La reazione più frequente è questa: due occhi sgranati tra l'incredulo ed il perplesso. Poi con calma, dopo essermi goduto il momento, gli spiego che nella prima metà del 1700 la città di Monaco di Baviera era sotto l'impero degli Asburgo, e che da lì partirono i miei avi per andare a vivere nel Regno delle due Sicilie. Da lì è stato un attimo nascere a Bologna e studiare nell'Ateneo più antico del mondo!

Privacy Solver è la soluzione ai tuoi problemi privacy aziendali

Privacy Solver, il Risolutore Privacy! Il sistema di gestione della privacy dedicato a chi preferisce lavorare e lasciare la noiosa gestione privacy ad un esperto che la gestisca per lui.

Vuoi approfondire l'argomento del Nuovo Regolamento Europeo sulla Privacy con video e report dedicati?

Vai alla pagina
bit.ly/BONUSGUIDA

ed accedi ai contenuti bonus dedicati a te.



Adeguiamo la tua azienda alla nuovo Regolamento Europeo Privacy UE 2016/679, senza rischi e togliendoti ogni fastidio.

- No a soluzioni standardizzate e preconfezionate
- No a mancanza di informazioni immediate e rischi inutili di sanzioni
- No a specialisti improvvisati o generalisti che oltre alla privacy fanno mille altri servizi

Non affidare la tua azienda a nessun consulente prima di aver contattato

noi allo 051 0827333

mail@privacysolver.it

www.privacysolver.it