AVVOCATI E INFORMATICA
TRATTAMENTO DEI DATI PERSONALI E GESTIONE DEI DOCUMENTI INFORMATICI: PROFILI DEONTOLOGICI

L’avvocato e i SaaS

Torino, 5 Ottobre 2022

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Di cosa parliamo

- Cosa sono i SaaS
- Gli obblighi
- Sentenze Schrems

Avv. Marco Ciurcina
ciurcina@studiolegale.it

I SaaS

- Gsuite,
- Office365,
- Dropbox,
- Posta elettronica,
- WhatsApp,
- Google Analytics,
- Ecc.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

per dati dei clienti

- Segretezza (art. 13 Codice Deontologico)
- Tutela dei dati personali (GDPR)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 13 Codice Deontologico

Dovere di segretezza e riservatezza

L’avvocato è tenuto, nell’interesse del cliente e della parte assistita, alla rigorosa osservanza del ***segreto professionale*** *e al* ***massimo riserbo*** *su fatti e circostanze in qualsiasi modo apprese nell’attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell’attività di consulenza legale e di assistenza stragiudiziale e comunque per ragioni professionali.*

Gli obblighi

GDPR

A) Da fare:

- attuare in modo efficace i principi ex art. 5.1 GDPR
- soddisfare le condizioni di liceità ex art. 6.1 GDPR
- rispettare i vincoli ex artt. 9 e 10 GDPR
- fornire l'informativa agli interessati (artt. 13 e 14 GDPR)
- attuare i principi di privacy by design e by default (art. 25 GDPR)
- redigere accordi con i contitolari del trattamento e/o **contratti** o altri atti giuridici **con i responsabili del trattamento** (artt. 26 e **28 GDPR**)
- redigere le istruzioni agli incaricati del trattamento (art. 29 GDPR)
- tenere il registro delle attività di trattamento (art. 30 GDPR)
- garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR)

Gli obblighi

GDPR

B) Da valutare (e fare se necessario):

- eseguire la valutazione d’impatto sulla protezione dei dati (art. 35 GDPR)
- designare il responsabile della protezione dei dati personali (art. 37 GDPR)
- rispettare le condizioni di liceità del **trasferimento dei dati all’estero** (**artt. 44-50 GDPR**)
- redigere l’informativa e/o il banner cookie (art. 122 Codice Privacy)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

GDPR

C) Da monitorare nel tempo (e fare quando necessario):

- replicare alle richieste degli interessati ed inviare le notifiche (artt. 15-22 GDPR)
- eseguire la notifica al Garante della Privacy e la comunicazione all'interessato (artt. 33 e 34 GDPR)
- eseguire la consultazione preventiva ex art. 36 GDPR)
- aderire a codici di condotta e/o adottare certificazioni (artt. 40-43 GDPR)
- aggiornare le misure di cui ai punti A e B.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 28 GDPR e SaaS

Tra gli obblighi, contrattualizzare responsabili del trattamento (inclusi i fornitori di SaaS che implicano il trattamento) ai sensi dell’art. 28 GDPR

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 28 GDPR e SaaS

Decisione di Esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle **clausole contrattuali tipo** tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021D0915&from=EN

Gli obblighi

Art. 28 GDPR e SaaS

I fornitori di SaaS

- Incluso nel contratto
- Addendum contrattuale (DPA) previsto by default
- Addendum contrattuale da richiedere

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 44-50 GDPR e SaaS

Condizioni di liceità del trasferimento extra UE

- Decisione di adeguatezza (art. 45 GDPR)
- Clausole contrattuali tipo (art. 46.2.c GDPR)
- Ecc.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 45 GDPR e SaaS

2013: rivelazioni di Snowden, Risoluzione del Parlamento UE, Comunicazione della Commissione UE

2015: sentenza CGUE cd. Schrems I

2016: Privacy Shield

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 45 GDPR e SaaS

Schrems II

Il Privacy Shield è nullo

l diritto USA non offre adeguate garanzie di tutela dei diritti degli interessati: il fornitore statunitense è soggetto a norme (FISA 702 e E.O. 12333, in combinato disposto con PPD-28) che permettono attività di sorveglianza di massa in modo non rispettoso dei diritti fondamentali riconosciuti nell'UE

Gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE del 10 novembre 2020 (versione 2.0 del 18 giugno 2021)

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 1/2020 EDPB

Clausole Contrattuali Tipo, ma:

- eseguire la valutazione del diritto del paese nel quale si esegue il trasferimento;
- prevedere idonee misure supplementari (come per esempio la criptazione dei dati personali) di modo che non sia possibile utilizzare i dati personali in violazione dei diritti degli utenti al di fuori dell'UE.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 1/2020 EDPB

“Si osservi che anche l’accesso remoto da parte di un’entità di un paese terzo a dati situati nel SEE è considerato un trasferimento” (nota 22).

N.B.: il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"): consente alle autorità statunitensi di accedere ai dati contenuti nei server delle società statunitensi, anche se gestiti al di fuori degli Stati Uniti

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Gli obblighi

Art. 46.2.c GDPR e SaaS

ma

“Il Tribunale regionale superiore di Karlsruhe chiarisce che l'utilizzo di un server europeo e di un fornitore di servizi di hosting con una società madre statunitense non è di per sé illegale ai sensi della legge sulla protezione dei dati”

https://www.heuking.de/en/news-events/newsletter-articles/detail/olg-karlsruhe-stellt-klar-einsatz-eines-europaeischen-server-und-hosting-dienstleisters-mit-us-amerikanischer-konzernmutter-nicht-per-se-datenschutzrechtlich-unzulaessig.html

Grazie

ciurcina@studiolegale.it