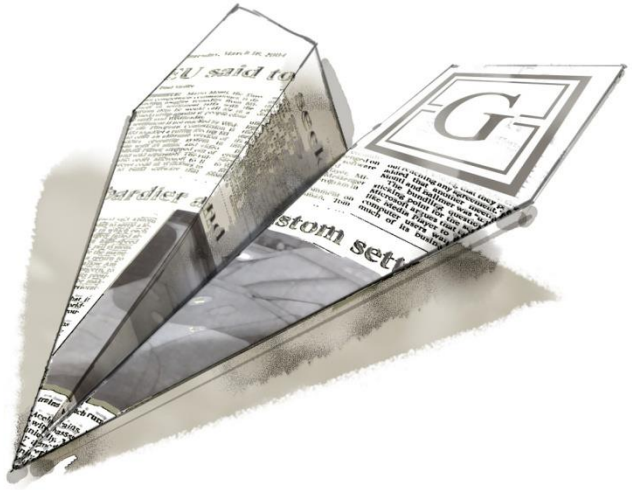
STUDIO LEGALE
GIACOPUZZI
DIRITTO D'IMPRESA



GDPR: stato dell'arte e criticità della prima applicazione

Avv. Luca Giacopuzzi – Avv. Francesca R. Pagliaro

CONFINDUSTRIA
Verona

GDPR: NOZIONI INTRODUTTIVE

- ✓ L'art. 4 GDPR, il «vocabolario della privacy»
- ✓ Ogni trattamento deve trovare fondamento in un'idonea base giuridica: il consenso, ma non solo!
- ✓ I principi applicabili al trattamento di dati personali: tra essi, l'accountability

Sostanza e non (solo) forma.

IL TITOLARE DEL TRATTAMENTO

- ✓ La persona che determina le **finalità** e i **mezzi** del trattamento
- ✓ Deve mettere in atto **misure tecniche e organizzative** adeguate ed efficaci per garantire e dimostrare che il trattamento è effettuato conformemente al regolamento

C’è da fare, ma, anche e soprattutto,
c’è da dimostrare di aver fatto
(«accountability»)

I CONTITOLARI DEL TRATTAMENTO

- ✓ Due o più titolari che determinano **congiuntamente** le finalità e i mezzi del trattamento
- ✓ Un obbligo: **l'accordo interno**, che rifletta i rispettivi ruoli e i rapporti con gli interessati

Gli interessati possono agire nei confronti di chiunque

IL RESPONSABILE DEL TRATTAMENTO

- ✓ Il trattamento è **effettuato per conto** del titolare
- ✓ Il titolare documenta la nomina con un **contratto**, a contenuto obbligato
- ✓ Il responsabile ha **obblighi propri**
- ✓ Il responsabile del trattamento non è il responsabile della protezione dei dati
- ✓ Il sub-responsabile: serve l'autorizzazione del titolare e…tanta attenzione!

E' l'outsourcer.
Ma preserviamo gli effetti della figura del responsabile interno

L’INCARICATO DEL TRATTAMENTO

- ✓ Dov’è scomparso? Nel regolamento non vi è traccia del termine «incaricato»
- ✓ La «persona autorizzata al trattamento» chi è?

Le modalità di designazione già note sono compatibili con la filosofia del regolamento

L'INFORMATIVA

- ✓ E' dovuta per qualunque trattamento
- ✓ E'strumento di trasparenza: fornisce agli interessati informazioni chiare e complete
- ✓ **Modalità**: è concisa, trasparente, intellegibile e facilmente accessibile
- ✓ **Contenuti**: con alcuni abbiamo già familiarizzato; altri sono elementi di novità
- ✓ **Tempi**: quando la si deve fornire?

Rimane uguale solo
il numero dell'articolo

IL CONSENSO

- ✓ Tale è qualsiasi manifestazione di volontà (dell'interessato) libera, specifica, informata e inequivocabile
- ✓ Consenso tacito o presunto? No, grazie
- ✓ Più finalità? Più consensi
- ✓ Si alza l'asticella: il consenso cd. «esplicito» (ex-sensibili, profilazione, extra UE)

Non deve (più) essere necessariamente documentato per iscritto.
Ma l'onere della prova è immutato

GDPR E D. LGS. 196/03 NOVELLATO

- ✓ Uno sguardo d'insieme
- ✓ Focus sul D. Lgs. 101/18
- ✓ E ora, **che succede**?
- ✓ Una **lettura combinata** ben fatta: come procedere

Una compliance «sofisticata»,
perchè articolato
è lo scenario normativo

IL RISARCIMENTO DEI DANNI

- ✓ Il danno cd. «da trattamento»: materiale e immateriale
- ✓ Le altre regole del gioco: dalla **solidarietà passiva** all'azione di **regresso**

L'onere della prova:
a ognuno il suo!

LE SANZIONI AMMINISTRATIVE E PENALI

- ✓ Fino a € 10 milioni o fino al 2% del fatturato mondiale totale annuo
- ✓ Fino a € 20 milioni o fino al 4% del fatturato mondiale totale annuo
- ✓ Effettive, proporzionate e dissuasive. Così è (se vi pare)
- ✓ I **criteri di valutazione** di cui all'art. 83, paragrafo 2 reg.
- ✓ Le linee guida del Gruppo di lavoro articolo 29

Sanzioni
ad ampio spettro:
anche penali!

IL RAPPORTO DI LAVORO

- ✓ La compliance: dall'**assunzione** alla **cessazione** del rapporto (v. Newsletter 439/18)
- ✓ Servono misure appropriate: sempre. Per un trattamento «trasparente» e condotto nel rispetto della normativa, anche giuslavoristica
- ✓ L'**informativa**: chiara e completa. E **consenso**. Senza dimenticare le **policy** aziendali
- ✓ Attenzione ai trattamenti «sui generis»: dal telelavoro allo smart working
- ✓ Dipendenti, ma non solo: agenti, stagisti, collaboratori…

Le «dritte»?
Nei provvedimenti (WP 29
e Autorità di controllo)

LA DISCIPLINA DELLA POSTA ELETTRONICA

- ✓ **No** al controllo massivo delle email
- ✓ **No** alla conservazione senza limite delle email
- ✓ **Che fare in costanza di rapporto**? Salvo situazioni precontenziose o contenziosi in atto, si ricorra a sistemi di gestione documentale con cui archiviare via via i documenti pertinenti
- ✓ **Che fare dopo** la cessazione del rapporto? Autorespondent e successiva disattivazione della casella di posta, con eliminazione dal server dei messaggi ivi presenti

No a controllo massivo
e a conservazione *sine die*

L'OPINION 2/2017 DEL WP 29

- ✓ Un **nuovo parere per nuovi rischi** da fronteggiare: i 9 scenari.
- ✓ Il **consenso** spesso non basta. E il **legittimo interesse**?
- ✓ Recruitment; in-employment screening; controllo IT sul luogo di lavoro e fuori sede
- ✓ Verifica delle presenze e del rispetto dell'orario di lavoro; videosorveglianzaù
- ✓ Geolocalizzazione dei veicoli; comunicazione dati a terzi e trasferimento extra-UE

Analisi e misure (ove necessario, anche la DPIA!) a monte e non a valle

IL MARKETING

- ✓ **Soluzioni differenti** per scenari diversi: si considerino target e mezzi
- ✓ Consenso e legittimo interesse: chi «vince»?
- ✓ GDPR e D. Lgs. 196/03 (art. 130): **tiriamo le somme!**
- ✓ Spam, le linee-guida del Garante
- ✓ Le novità in tema di **telemarketing**: i prefissi sentinella, e non solo

Consulenza puntuale,
caso per caso

IL DATA PROTECTION OFFICER

- ✓ E’ figura **apicale**: con i vertici aziendali il rapporto è continuo e diretto
- ✓ E’ figura **diversa**, per ruolo e funzioni, rispetto al responsabile del trattamento
- ✓ Quando è richiesta la **nomina**
- ✓ Quali **requisiti** deve avere. T.A.R. Friuli Venezia Giulia: sent. 287/2018
- ✓ Quali **compiti** deve assolvere

DPO
NON
RDT

LA VALUTAZIONE D'IMPATTO (DPIA)

- ✓ **Cosa è** (un processo continuativo e scalabile) e **cosa riguarda** (un trattamento)
- ✓ Quando è **obbligatoria** (i 9 critieri WP 29: almeno 2/9). Ma vince l'accountability…
- ✓ Aiuta non soltanto a rispettare le prescrizioni del regolamento, ma anche ad attestare di aver adottato misure idonee a neutralizzare o minimizzare i rischi
- ✓ Quando va effettuata e da chi; il ruolo del DPO
- ✓ Come gestire la cd. consultazione preventiva

Prezioso strumento di accountability

LA DURATA DEL TRATTAMENTO

- ✓ Il principio di **limitazione della conservazione** (art. 5.1.e GDPR)
- ✓ Il considerando 39 e il richiamo al «minimo necessario». E al termine di cancellazione
- ✓ La casistica principale: CV (ricevuto spontaneamente o sollecitato), dipendenti, fornitori, clienti, marketing (soft spam o clienti potenziali), registro visitatori, email aziendale, videosorveglianza, biometria

Presupposti rigidi e
analisi condotta con rigore

STUDIO LEGALE
GIACOPUZZI

DIRITTO D'IMPRESA

37121 Verona,
Stradone San Fermo n.21
Tel.: 045.8011287

www.studiogiacopuzzi.it
posta@studiogiacopuzzi.it

GRAZIE PER L'ATTENZIONE