L'APPROFONDIMENTO

# I costi del GDPR, per le imprese ma soprattutto per le autorità nazionali: i possibili impatti





Il GDPR ha segnato una svolta di settore epocale garantendo un maggior controllo sui propri dati personali, ma non è privo di costi per le imprese e soprattutto per le autorità nazionali di protezione dei dati sia dal punto di vista economico sia da quello delle risorse disponibili per svolgere i loro compiti

31 Mag 2021

J **Roberto A. Jacchia**
Avvocato, senior partner, Studio De Berti Jacchia

S **Marco Stillo**
Associate, Studio De Berti Jacchia

Da quando è diventato applicabile il 25 maggio 2018, il **Regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR)** ha segnato una svolta di settore epocale, non solo creando **parità di condizioni per tutte le imprese che operano sul mercato europeo** indipendentemente dal luogo in cui sono stabilite, bensì garantendo anche che tutti coloro che trattano dati personali nell'ambito della sua applicazione siano maggiormente responsabilizzati e responsabili.

Nonostante rappresenti uno strumento essenziale per garantire che le persone dispongano di un **maggiore controllo sui loro dati personali** e che gli stessi siano trattati per una finalità legittima, in maniera lecita, corretta e trasparente, tuttavia, il GDPR non è stato privo di **costi**.

A pagare questi ultimi sono state, in primo luogo, le **imprese**.

Adeguarsi alle norme del GDPR, infatti, comporta costi non solo tecnologici, ma anche organizzativi. Oltre che per le imprese, tuttavia, il GDPR ha comportato diversi costi anche per le **autorità nazionali di protezione dei dati** dal punto di vista economico e soprattutto da quello delle **risorse disponibili per svolgere i loro compiti**.

## Indice degli argomenti



## L'impatto del GDPR sulle autorità nazionali

Le **autorità nazionali di protezione dei dati** svolgono un ruolo essenziale nel garantire che il GDPR sia applicato correttamente. Di conseguenza, l'incremento delle loro responsabilità ha comportato la necessità di **maggiori risorse rispetto al passato**.

E-mail aziendale

Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

ISCRIVITI SUBITO

Secondo quanto stabilito dall'**articolo 52 del GDPR**, ogni Stato membro deve provvedere affinché le rispettive autorità di controllo siano dotate delle **risorse umane, tecniche e finanziarie nonché delle infrastrutture necessari per l'effettivo adempimento dei propri compiti** e l'esercizio dei propri poteri, un obbligo che la Commissione ha più volte ribadito nel corso degli anni (da ultimo nella sua comunicazione del 24 giugno 2020).

Benché dal **2016 al 2019** la maggior parte delle autorità di controllo abbia effettivamente beneficiato di un **aumento del personale e del bilancio**, con picchi soprattutto per le autorità irlandesi e lussemburghesi in quanto le grandi multinazionali tecnologiche più importanti sono ivi stabilite, la **situazione** è tuttavia ancora **estremamente disomogenea** tra gli Stati membri.

Più particolarmente, **dal 2019 il personale e il budget a disposizione delle autorità di controllo è aumentato solamente in misura marginale**, non risultando sufficiente a consentire loro di svolgere i numerosi compiti che sono chiamate ad assolvere ai sensi del GDPR.

Ciò, a sua volta, le costringe ad affidarsi a consulenti e legali esterni per far fronte alla mole di lavoro, con un conseguente ulteriore

aggravio del budget.

## Le conseguenze a livello sanzionatorio

La mancanza di risorse sufficienti non ha comunque impedito alle autorità nazionali di **intervenire nei confronti delle imprese** sanzionandole per il mancato rispetto delle norme sulla privacy, ivi comprese quelle del GDPR, con ammende particolarmente consistenti.

In particolare, nel gennaio 2019 la **Commissione nazionale francese per la protezione dei dati (***Commission nationale de l'informatique et des libertés***, CNIL)** aveva inflitto a **Google** una multa pari a circa 50 milioni di euro per aver violato il GDPR:

1. non avendo fornito agli utenti un avviso in una forma facilmente accessibile e con un linguaggio chiaro e semplice della necessità di configurare i propri dispositivi mobili secondo la piattaforma Android;
2. non avendo ottenuto il consenso degli utenti al trattamento dei loro dati personali per scopi di personalizzazione degli annunci.

Nel gennaio 2020, inoltre, il **Garante per la *privacy* italiano** aveva irrogato a TIM una sanzione pari a circa 27 milioni di euro per numerosi trattamenti illeciti di dati legati all'attività di marketing, consistenti in chiamate promozionali indesiderate effettuate senza consenso o nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni, oppure ancora, malgrado il fatto che le persone contattate avessero espresso la volontà di non

ricevere telefonate promozionali.

Più recentemente, e per motivi analoghi, **Fastweb** è stata sanzionata per un importo di circa 4,5 milioni. Infine, nell'ottobre 2020 l'**Ufficio del Commissario britannico per l'Informazione** (***Information Commissioner's Office***, **ICO**) aveva sanzionato, da un lato, la **British Airways** per circa 20 milioni di sterline, per alcune lacune di sicurezza nel trattamento dei dati che avevano consentito a terzi di ottenere l'accesso non autorizzato alle informazioni personali e alle carte di credito di oltre 400.000 clienti e, dall'altro lato, la **Marriott,** per circa 18,4 milioni di sterline, relativamente ad un data breach che nel 2014 aveva causato la violazione dei dati di oltre 339 milioni di clienti in tutto il mondo.

## Il nuovo approccio dei Tribunali nazionali

Negli ultimi tempi, tuttavia, diversi **Tribunali nazionali** hanno iniziato a **riformare le decisioni dei regolatori o ridurre l'importo delle sanzioni**, sollevando dubbi sulla disomogeneità di vedute tra autorità giudiziarie e di protezione dei dati in merito all'applicazione del GDPR.

Più particolarmente, in data 2 dicembre 2020 il **Tribunale amministrativo federale austriaco** ha annullato la sanzione pari a circa 18 milioni di euro inflitta alla *Österreichische Post* da parte dell'autorità per la protezione dei dati, per aver violato il GDPR elaborando i dati dei suoi clienti al fine di determinarne la loro presunta affinità politica.

Secondo il Tribunale, tuttavia, l'autorità non era riuscita a fornire,

come richiesto da una recente legge nazionale austriaca, il nominativo della persona fisica a cui imputare la violazione del GDPR, non risultando pertanto in grado di identificare il soggetto che aveva deciso di svolgere le attività di trattamento non consentite.

In novembre 2020, il **Tribunale amministrativo di Stoccolma** ha ridotto da circa 7,3 milioni di euro a 5 milioni una sanzione inflitta da parte dell'autorità garante svedese contro Google per aver violato il diritto di oblio di un utente.

Nel febbraio 2021, il **Tribunale regionale di Berlino** aveva invalidato la multa pari a circa 14,5 milioni di euro inflitta dal Commissario per la protezione dei dati e della libertà di informazione contro la *Deutsche Wohnen SE,* per non aver predisposto misure volte a consentire la regolare cancellazione dei dati dei locatari che non erano più necessari.

Secondo il Tribunale, infatti, il Commissario non aveva sufficientemente specificato gli atti della società che avevano comportato la violazione del GDPR. Già nel novembre del 2020, il **Tribunale Regionale di Bonn** aveva ridotto del 90% una pena pecunaria imposta a 1&1 in ragione di errori della valutazione della situazione nella determinazione dell'ammontare della sanzione.

## Considerazioni conclusive

Peraltro, questa nuova tendenza nel senso dell'annullamento o della riduzione delle sanzioni comminate alle imprese per le violazioni del GDPR crea grande incertezza giuridica e rischia di

aggravare ulteriormente il problema della mancanza di risorse delle autorità nazionali di protezione dei dati per adempiere ai propri compiti.

Da un lato, al fine di garantire il pieno rispetto del GDPR, infatti, queste ultime potrebbero essere costrette ad impugnare le decisioni di primo grado, e, dall'altro, le imprese sono incoraggiate a fare ricorso più spesso contro i provvedimenti sanzionatori delle autorità, il tutto con ulteriori costi, tanto finanziari quanto di personale, così alimentando un circolo vizioso.

Un intervento dei Governi nazionali sarebbe pertanto auspicabile al fine di evitare che il GDPR perda di credibilità: infatti, se le autorità deputate a garantirne il rispetto non dispongono delle risorse necessarie, difficilmente i cittadini possano riporre in loro fiducia per una tutela efficace dei loro dati personali.

Non ultimo, un dispiegamento maggiore di risorse potrebbe scongiurare l'avvio di procedure di infrazione da parte della Commissione nei confronti degli Stati membri per la violazione degli obblighi derivanti dall'articolo 52 del GDPR ed in particolare il comma 4: "*Ogni Stato membro provvede affinché ogni autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato*".

DIGITAL EVENT, 15 LUGLIO

## Device management per un lavoro ibrido semplice e sicuro

# Mobility

# Risorse Umane/Organizzazione

Leggi l'informativa sulla privacy

E-mail

E-mail aziendale

Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

ISCRIVITI SUBITO



## Personaggi

M Marco Stillo

R Roberto A. Jacchia

## Argomenti

D Data Protection

D dati personali

G Gdpr

I infrastrutture

P Privacy

## Canali