

Gruppo di lavoro Area legale

PRIVACY 2018

GDPR: General Data Protection Regulation

Linee Guida

Il presente documento è stato realizzato dal Gruppo di lavoro Area Legale con il contributo di:

Guido Calderaro (EXCISE & CUSTOMS CONSULTING SRL), **Michela Catenaccio** e **Niccolò Agliati** (UCIMU), **Silvia Corvino** (ZF Group), **Silvia Gasca** (SKF INDUSTRIE SPA), **Emanuela Pregnotato** (ANFIA), **Alessandra Romersi** (MAGNETI MARELLI SPA), **Luca Saglione** (PwC).

Documento chiuso con informazioni disponibili al 31 Luglio 2018.

Gruppo di lavoro Area legale

INDICE

1. PREMESSE.....	pag.4
2. PRIVACY: DALLA DIRETTIVA AL REGOLAMENTO. STORIA E RAGIONI DEL CAMBIAMENTO.....	pag.5
3. DEFINIZIONI.....	pag.9
4. NUOVO REGOLAMENTO GDPR.....	pag.13
a. Ambito di applicazione.....	pag.13
b. Soggetti.....	pag.13
c. Accountability : principio di autoresponsabilizzazione dell'azienda nella gestione del dato.....	pag.18
d. Registro delle attività di trattamento.....	pag.20
e. Protezione dei dati fin dalla progettazione (<i>Privacy by design</i>) e protezione per impostazione predefinita (<i>Privacy by default</i>).....	pag.22
f. Diritto alla portabilità dei dati : Data portability	pag.23
g. Diritto alla cancellazione (o diritto all'oblio).....	pag.24
h. Informativa.....	pag.26
i. Documento di valutazione d'impatto nel trattamento dei dati (Privacy impact assessment o DPIA).....	pag.29
j. Data breach notification.....	pag.31
k. Sanzioni.....	pag.33
5. TRATTAMENTO DEI DATI EXTRA UE E INTEGRAZIONE GDPR	pag.34
6. PROPOSTA DI APPROCCIO METODOLOGICO PER LA COMPLIANCE AL GDPR....	pag.38
7.FAQ	pag.48
8.LINK UTILI.....	pag.57
9.ALLEGATI.....	pag.58

Gruppo di lavoro Area legale

1. PREMESSE

Il nuovo Regolamento UE 2016/679, comunemente identificato come GDPR - dall'acronimo inglese *General Data Protection Regulation* - è entrato in vigore in tutti gli Stati Membri dell'Unione Europea il 24 Maggio 2016 ed è **applicabile a partire dal 25 Maggio 2018**. Alla data di chiusura del presente documento non sono state ancora approvate le disposizioni per l'adeguamento della normativa nazionale a quella del GDPR¹.

Il Regolamento, che offre una maggiore tutela alle persone fisiche e rende le aziende più responsabili nell'uso dei dati personali, rappresenta un significativo passo in avanti nella **legislazione relativa alla protezione dei dati** che assume una posizione di prima linea tra i processi aziendali, con un impatto significativo sulla gestione delle informazioni personali relative sia a clienti che a dipendenti. **Si propone inoltre di rafforzare il livello di tutela dei dati per tutte le persone fisiche all'interno dell'UE, indipendentemente da dove sono custoditi i dati.**

Il GDPR cambia altresì la filosofia del trattamento dei dati sostituendo il precedente approccio di natura prevalentemente formale, con un approccio basato **sull'analisi del rischio e sull'adeguamento continuo** alle innovazioni tecnologiche e dei processi interni.

Le presenti Linee Guida hanno l'intento di fornire una sintesi dei **passaggi chiave** della nuova normativa e le **prime indicazioni operative** in materia, suggerendo un esempio di **approccio metodologico** per il primo setup di un sistema di compliance conforme ai requisiti del GDPR. E' stato inoltre inserito un capitolo dedicato alle **FAQ** sulla base delle prime richieste pervenute dalle aziende associate.

Nei prossimi mesi è in programma la pubblicazione di una nuova versione della presente guida che tenga conto degli interventi normativi di adeguamento nazionale e di una casista più ampia di situazioni applicative.

¹ Lo schema di decreto legislativo è stato trasmesso per l'esame alla Presidenza della Camera dei Deputati il 10 maggio 2018.