

Data Protection Officer (artt. 37-39 GDPR 2016/679)

1. Obbligatorio per aziende operanti nei segg. settori:
 - a. strutture pubbliche
 - b. trasporti
 - c. utilities
 - d. elaborazione dati di geolocalizzazione
 - e. ospedali e assimilati
 - f. gestione reti stradali
 - g. assicurazioni
 - h. banche
 - i. web o tel. mktg
 - j. servizi di broadcasting
 - k. gestione dati giudiziari
 - l. ecc.

e in genere anche quando si trattano grandi quantità di dati.

2. Il DPO è l'intermediario ufficiale con Autorità Nazionale di controllo (Garante e GGFF Unità speciale privacy)
3. Non è responsabile per osservanza del Regolamento (la responsabilità resta al controller o titolare del trattamento)
4. Il controller documenta per iscritto perché nomina il DPO
5. Nomina (di interno o esterno) con compiti e autonomia (art.37) e con le capacità ex art. 39 (soprattutto conoscenza approfondita del Reg. Europeo, comprensione dei processi aziendali, comprensione delle necessità sicurezza della struttura)
6. Pubblicazione del contratto del DPO: interna e ad Autorità di controllo
7. Coinvolgimento del DPO (art. 38) in tutte le azioni che comportano la gestione della sicurezza dei dati
8. In caso di parere negativo del DPO (in tema di attività per la protezione dei dati) occorre documentare la sua posizione
9. DPO deve avere:
 - a. supporti logistici
 - b. supporti economici
 - c. accesso alle diverse funzioni aziendali
 - d. training continuo

10. Compiti:

- a. partecipa al Data Protection Impact Assessment (steso dal controller)
- b. quelli dettagliati dall' art. 39 con particolare attenzione al coordinamento di un controllo periodico su tutte le misure di sicurezza di tipo tecnico e organizzativo messe in atto

11. Deve essere data comunicazione agli interessati al momento della raccolta dei loro dati personali