Checklist sul GDPR

(sviluppata a partire da quella dell'autorità di controllo del Regno Unito – ICO, maggio 2018)

Il Soggetto giuridico (società, associazione, organizzazione, ente, ecc.) in questione:

ADEMPIMENTO	SITUAZIONE (Sì/No/N.A.)	RIFERIMENTI NORMATIVI (artt. GDPR)	CATEGORIA
1. ha identificato se deve o meno nominare un Responsabile Della Protezione Dei Dati o Data Protection Officer (DPO) ovvero se è opportuno nominarlo anche in assenza di obbligo legale		37	DPO
2. ha nominato un Responsabile Della Protezione Dei Dati o Data Protection Officer (DPO)		37-39	DPO
3. ha condotto un controllo delle informazioni per mappare i flussi di dati (data flows).		24	TRATTAMENTI
4. ha documentato quali dati personali detiene, da dove provengono, con chi li condivide, cosa fa con essi e per quale finalità (censimento dei vari trattamenti di dati personali), predisponendo ove necessario, i registri delle attività di trattamento		30	TRATTAMENTI
5. ha identificato le basi legali per l'elaborazione (presupposti di legittimità) e le ha documentate.		6-10	TRATTAMENTI
6. ha identificato il periodo di conservazione dei dati personali o comunque la logica per definire la durata della conservazione dei dati personali o quando devono essere eliminati		5	TRATTAMENTI
7. ha definito i compiti e l'ambito del trattamento consentito		26-29	TRATTAMENTI
8. ha identificato se una delle operazioni di trattamento costituisce un processo decisionale automatizzato e, in tal caso, ha adottato procedure per far fronte ai requisiti.		13,14,15,22	TRATTAMENTI
9. ha adottato una politica di protezione dei dati personali appropriata.		24	TRATTAMENTI
10. ha una politica di sicurezza delle informazioni supportata da appropriate misure di sicurezza.		24,25,32	TRATTAMENTI
11. ha effettuato l'analisi dei rischi per i diritti e le libertà fondamentali delle persone fisiche di cui tratta i dati personali, nonché l'analisi dei rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta		32	TRATTAMENTI
12. gestisce i rischi delle informazioni in modo strutturato in modo che la direzione comprenda l'impatto sul business dei rischi relativi ai dati personali e questi siano affrontati in modo efficace.		24,32	TRATTAMENTI

ADEMPIMENTO	SITUAZIONE (Sì/No/N.A.)	RIFERIMENTI NORMATIVI (artt. GDPR)	CATEGORIA
13. ha implementato misure tecniche e organizzative adeguate per integrare la protezione dei dati nelle attività di elaborazione sin dalla progettazione (by design) e per impostazione predefinita (by default)		25	TRATTAMENTI
14. ha identificato se deve o meno condurre una valutazione di impatto per la protezione dei dati (DPIA) ha in atto processi per agire in tal senso.		35	TRATTAMENTI
15. ha designato tutte le persone autorizzate al trattamento		29	PERSONALE E ACCORDI
16. ha svolto e offre la formazione sulla sensibilizzazione alla protezione dei dati per tutto il personale.		29	PERSONALE E ACCORDI
17. ha un accordo con ogni contitolare dei trattamenti di dati personali svolti in contitolarità		26	PERSONALE E ACCORDI
18. ha un contratto con qualsiasi responsabile del trattamento a cui si affidi		28	PERSONALE E ACCORDI
19. se trasferisce dati personali al di fuori dello Spazio economico europeo, ha identificato i paesi e le organizzazioni internazionali verso cui sono trasmessi tali dati personali		44	ESTERO
20. ha identificato le basi legali per il trasferimento di dati personali al di fuori dello Spazio economico europeo		44-49	ESTERO
21. garantisce un livello adeguato di protezione per i dati personali trasferiti al di fuori dello Spazio economico europeo		46-47	ESTERO
22. ha predisposto idonee informative per gli interessati sia nel caso di raccolta dei dati personali direttamente presso l'interessato, sia nel caso di raccolta indiretta dei dati presso terzi		13-14	INFORMATIVE E CONSENSI
23. comunica quanto previsto nelle informative ad ogni interessato secondo i tempi e le modalità previste		12	INFORMATIVE E CONSENSI
24. ha esaminato il modo in cui chiede e registra il consenso		7-8	INFORMATIVE E CONSENSI
25. ha sistemi per registrare e gestire il consenso in corso		7-8	REGISTRI E CONTROLLI
26. ha processi efficaci per identificare, segnalare, gestire e risolvere le eventuali richieste degli interessati		12,15-22	REGISTRI E CONTROLLI
27. ha processi per identificare, segnalare, gestire e risolvere eventuali violazioni dei dati personali.		33-34	REGISTRI E CONTROLLI
28. ha processi per gestire la cooperazione con l'Autorità di controllo (Garante)		31	REGISTRI E CONTROLLI
29. ha processi per garantire che i dati personali rimangano precisi e aggiornati.		5	REGISTRI E CONTROLLI
30. controlla periodicamente la conformità alla propria politica di protezione dei dati personali e riesamina regolarmente l'efficacia della gestione dei dati e dei controlli di sicurezza.		24	REGISTRI E CONTROLLI

Numero di “Sì”: Numero di “No”: Numero di “N.A.”: