Questionario di valutazione della conformità al Regolamento Europeo sulla Protezione dei Dati (GDPR)

Data

Titolare del trattamento

cliccare sulla casella scelta

01	La Vostra organizzazione ha un numero di dipendenti pari o superiore a 250?	SI ☐ NO ☐
02	Il Titolare del trattamento ha definito la politica di gestione sulla protezione dei dati ?	SI ☐ NO ☐
03	Il Titolare del trattamento ha nominato il Responsabile del trattamento ?	SI ☐ NO ☐
04	Esistono contitolari del trattamento ?	SI ☐ NO ☐

Commenti

TIPOLOGIA DEI DATI TRATTATI		
05	Per ciascun trattamento sono individuate le categorie di interessati (ad es., clienti, fornitori, dipendenti, agenti, consulenti e candidati, ecc.)?	SI ☐ NO ☐
06	Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?	SI ☐ NO ☐
07	Oltre ai dati comuni il trattamento include dati sensibili (origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone) ?	SI ☐ NO ☐
08	Oltre ai dati comuni il trattamento include dati biometrici ?	SI ☐ NO ☐
09	Oltre ai dati comuni il trattamento include dati giudiziari ?	SI ☐ NO ☐
11	Sono esplicitate le finalità dei trattamenti effettuati e la relativa base giuridica?	SI ☐ NO ☐
12	Viene definito il termine di conservazione dei dati ?	SI ☐ NO ☐
13	Viene condotta attività di profilazione (qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica)?	SI ☐ NO ☐
14	Esiste un elenco degli archivi che contengono i dati e la loro dislocazione ? (Server , Personal computer, Sito Web)	SI ☐ NO ☐
16	L'accesso ai dati da parte degli incaricati è regolato da una procedure di autenticazione e autorizzazione ?	SI ☐ NO ☐
17	I dati cartacei di tipo riservato o sensibili sono conservati in armadi con serratura ?	SI ☐ NO ☐

Commenti

INFORMATIVA E CONSENSO

18	E' stata predisposta un'adeguata informativa per i clienti, fornitori, dipendenti, agenti, consulenti e candidati, con evidenza della base giuridica del trattamento ?	SI ☐ NO ☐
19	Nella Informativa è indicato il periodo di conservazione dei dati ?	SI ☐ NO ☐
20	Viene fatto firmare il consenso per il trattamento di eventuali dati sensibili ?	SI ☐ NO ☐
21	Vengono gestiti dati relativi ai minori?	SI ☐ NO ☐
22	Esiste una procedura per gestire le richieste dell'interessato?	SI ☐ NO ☐

Commenti

INCARICATI DEL TRATTAMENTO

23	E' stata redatta una lista degli incaricati che interagiscono con i dati personali?	SI ☐ NO ☐
24	I componenti della lista sono stati formalmente nominati ? (lettera di incarico)	SI ☐ NO ☐
25	E' stata prevista o effettuata la formazione degli incaricati ? (mansionario)	SI ☐ NO ☐
26	Esiste un elenco che indica per ciascun incaricato gli archivi dati gestiti ?	SI ☐ NO ☐

27	E' stato fatto l'elenco degli amministratori di sistema ? (tecnici interni o esterni che possono accedere ai dati al di fuori delle normali procedure)	SI ☐ NO ☐

28	Gli amministratori di sistema sono stati designati con lettera di incarico ?	SI ☐ NO ☐

29	E' stato implementato un sistema di registrazione degli accessi da parte degli amministratori di sistema ? (log degli amministratori di sistema)	SI ☐ NO ☐

Commenti

ELENCO DELLE APPARECCHIATURE

30	Esiste la descrizione dettagliata delle apparecchiature che costituiscono il sistema informatico ? (server, PC, notebook, tablet, smartphone, sistemi operativi, applicativi utilizzati, dispositivi di copia dei dati, dispositivi di connessione interna e con l'esterno) ?	SI ☐ NO ☐

ADEGUATE MISURE DI SICUREZZA		
31	L'accesso al sistema da parte degli incaricati viene effettuato tramite password ?	SI ☐ NO ☐
32	La password rispetta le regole di lunghezza (minimo 8 caratteri) e di complessità?	SI ☐ NO ☐
33	La password viene modificata ogni 6 mesi (3 mesi in caso di dati sensibili) ?	SI ☐ NO ☐
34	I dispositivi portatili assegnati al personale che opera all'esterno (notebook, tablet, smartphone) sono protetti da password?	SI ☐ NO ☐
35	Esiste una procedura di copia dei dati documentata ?	SI ☐ NO ☐
36	I supporti di copia sono conservati nello stesso locale dove si trova il server e i PC?	SI ☐ NO ☐
37	Esistono supporti di copia rimovibili ?	SI ☐ NO ☐
38	I supporti di copia dismessi vengono distrutti con procedura documentata?	SI ☐ NO ☐
39	Vengono effettuate copie dei dati anche in Cloud? (backup su server remoto)	SI ☐ NO ☐
40	Eventuali servizi forniti in cloud hanno un contratto di servizio ?	SI ☐ NO ☐
41	I sistemi sono protetti con software antivirus ?	SI ☐ NO ☐
42	I sistemi sono protetti con software antimalware ?	SI ☐ NO ☐
43	E' stato installato un firewall ?	SI ☐ NO ☐

44	Sono presenti sistemi operativi non più aggiornabili (Windows Server 2003, Windows XP, Office 2007) ecc.	SI ☐ NO ☐

45	E' stata fatta un'analisi dei rischi (furto, incendio, guasti, comportamenti fraudolenti, errori degli operatori, intrusioni interne e esterne , ….) con l'elenco delle misure da adottare ?	SI ☐ NO ☐

Commenti

VIDEOSORVEGLIANZA		
46	Esiste un impianto di videosorveglianza ?	SI ☐ NO ☐
47	E' stata predisposta un'adeguata informativa?	SI ☐ NO ☐
48	Se viene ripreso il personale esiste l'accordo sindacale e/o l'accordo con i lavoratori ?	SI ☐ NO ☐
49	Eventuali registrazioni vengono cancellate nei termini previsti ?	SI ☐ NO ☐

Commenti

DATA BREACH **(distruzione o perdita di dati personali)**		
50	Esistono procedure di crittografia dei dati?	SI ☐ NO ☐
51	In caso di incidente che coinvolgesse i dati personali, avete creato un processo di raccolta informazioni e gestione dell'incidente?	SI ☐ NO ☐