

PRATICAN. _____

AFFIDAMENTO D'INCARICO DI PREANALISI GRATUITA
VALUTAZIONE DEL RISCHIO IN MATERIA DI PRIVACY

SEGNALATORE: _____ COD: _____

COLLABORATORE: _____ COD: _____

AZIENDA: _____

SETTORE: _____

SEDE: _____

P.IVA: _____ C.F.: _____

TITOLARE / RAPP. LEGALE P.T.: _____

E-MAIL AZIENDALE: _____

PEC: _____

REFERENTE AZIENDALE: _____

NUMERO TEL. REF. : _____

FINALITA'

Il seguente questionario viene compilato al fine di effettuare un' analisi gratuita in riferimento alla gestione del trattamento dei dati personali e al grado di adeguatezza dello stesso, alla luce del nuovo Regolamento Europeo n. 679/2016 (GDPR).

Teca S.r.l. si propone, recepite le informazioni rese con il presente questionario, di eseguire una valutazione di impatto per l'individuazione e la gestione del rischio, definendo gli adempimenti pratici necessari al fine di evitare l'incombere di sanzioni.

Teca, inoltre, intende offrire assistenza alle aziende, per l'adozione di idonee misure tecniche e procedure organizzative, utili ad osservare gli obblighi prescritti dal GDPR.

1) Qual è il numero dei dipendenti ad oggi?

2) Qual è il volume d'affari relativo all' ultimo esercizio aziendale?

3) La Vostra organizzazione aziendale tratta categorie particolari di dati personali? (Es. informazioni di salute, ecc..).

4) Nel momento in cui vengono trattati dati personali, viene richiesto il consenso sottoscritto ai soggetti interessati? Se sì, richiedere copia.

5) La Vostra organizzazione aziendale effettua attività di marketing e/o comunicazioni? Se sì, acquisisce il consenso dei soggetti interessati? Chiedere copia.

6) I dati in Vostro possesso vengono aggiornati e/o cancellati con una determinata frequenza? Se sì, ogni quanto tempo?

7) La Vostra organizzazione aziendale fornisce dati a terzi? Se sì chi sono? Sono state fornite le informative agli interessati e predisposte le rispettive nomine?

8) I dati in Vostro possesso si trovano solo su materiale cartaceo (es. documenti) o anche su piattaforma informatica (es. software, in rete, etc.)?

9) Chi può accedere ai dati personali in Vostro possesso?

10) La Vostra organizzazione aziendale è stata sottoposta ad un processo di analisi di trattamento dei dati personali? Se sì:

10 a) È mai stata sottoposta ad un processo di valutazione del rischio per la sicurezza dei dati trattati?

10 b) Il personale impiegato in azienda è stato informato sulle modalità di trattamento dei dati personali?

10 c) Sono state aggiornate le informative e le varie nomine in materia di privacy?

10 d) La Vostra organizzazione aziendale ha provveduto alla nomina di un Responsabile per il trattamento dei dati personali?

10 e) Il Responsabile per il trattamento dei dati personali e il soggetto Incaricato alla loro “custodia” sono stati nominati con un atto scritto?

10 f) L'azienda prevede attività di formazione e/o aggiornamento periodico in materia di sicurezza dei dati trattati?

10 g) Alle figure incaricate al trattamento dei dati personali, sono state impartite le istruzioni finalizzate al controllo e/o alla custodia -per la durata dell'intero ciclo di trattamento- degli atti e dei documenti contenenti dati personali?

11) È stata effettuata un'analisi dei rischi per i dati trattati (es. furti, incendi, guasti, comportamenti fraudolenti, errori degli operatori, intrusioni interne e/o esterne ...), con l'elenco delle misure relative da adottare?

12) Esiste una descrizione dettagliata delle apparecchiature costituenti il sistema informatico aziendale? (server, PC, notebook, tablet, smartphone, sistemi operativi, applicativi utilizzati, dispositivi di copia dei dati, dispositivi di connessione interna ed esterna)? Se sì, chiedere copia. Se no predisporne una.

13) Di quanti devices (dispositivi a postazione fissa e/o mobili), è dotata l'azienda? Che sistema operativo è installato su ogni devices? Sono dotati di anti virus e anti malware?

14) È previsto un contratto di manutenzione con un sistemista informatico? Se sì, cosa prevede?

15) L'accesso al sistema da parte degli incaricati viene effettuato tramite password?

16) La password rispetta le regole di lunghezza (minimo 8 caratteri) e di complessità?

17) La password viene modificata ogni 6 mesi (3 mesi in caso di dati particolari)?

18) Ci sono dispositivi portatili assegnati al personale operante all'esterno (notebook, tablet, smartphone)? Se sì, sono protetti da password?

19) Vi sono collaboratori che lavorano da remoto? (telelavoro, trasferte...)

20) Viene effettuata una copia dei dati trattati? Se sì, su che supporto e dove vengono conservati. Esiste una procedura - documentata- di copia dei dati trattati?

21) Vengono effettuate copie dei dati anche in Cloud? (backup su server remoto). Se sì, questi ultimi sono certificati?

22) Eventuali servizi forniti in Cloud prevedono un contratto di servizio?

23) È stato installato un firewall? Esiste una copia delle prescrizioni contenuti nel firewall?

24) La struttura aziendale è dotata di sistemi di videosorveglianza? Se sì, di che tipo (interni e/o esterni)?

25) Esiste una mappa della rete LAN? Se sì, la stessa è certificata?

26) Esiste una o più reti WIFI? Chi può accedervi, a quali dati è consentito l'accesso e con quali regole di sicurezza?

27) In caso di furto dei dati trattati, attraverso quali modalità vengono avvisati i clienti e le autorità competenti?

28) Esiste una crittografia dei dati presenti su eventuale DBMS?

29) E' previsto un sito aziendale? Se sì, qual è il suo dominio? L'eventuale sito istallato è munito di certificazione SSL?

30) Per comunicare con i Vostri clienti/fornitori, utilizzate la mail aziendale ad es.:@dominio.it/.com/.net ecc.. o email di provider internazionali ad es.@gmail.com?

31) Nel caso in cui un cliente voglia esercitare il diritto di recesso o oblio dei dati personali, è descritta la procedura da seguire per farvi fronte, in forma rapida e intuitiva?

NOTE: _____

IL CLIENTE

_____, li ____ / ____ / ____