

Quattro domande a un fornitore di software di AI

Da inviare al fornitore prima di firmare, e da rifare a ogni rinnovo. Le FAQ dell'Agenzia per la cybersicurezza nazionale dicono che le clausole contrattuali da sole non bastano: per ogni domanda chiedete le evidenze, non la brochure.

01 Clausole

COSA CHIEDERE

- Quali clausole coprono sicurezza, subfornitura e cessazione del servizio.
- Entro quante ore viene notificato un incidente che tocca i nostri dati.
- Divieto di addestramento sui nostri dati, scritto nel contratto.
- Legge applicabile e foro competente.

EVIDENZE DA RICEVERE

- ☐ Contratto o allegato sicurezza con i tempi di notifica scritti
- ☐ Clausola di uscita con restituzione dei dati e formati
- ☐ Clausola di divieto di addestramento

Ricevuta il _____ • Valutazione: adeguata • da integrare • non adeguata

02 Evidenze

COSA CHIEDERE

- Quali prove dimostrano che le misure esistono, oltre alle clausole.
- Certificazioni (ISO 27001 o equivalente) e loro perimetro.
- Risultati dei test di sicurezza degli ultimi dodici mesi.
- Registro delle operazioni consultabile dal cliente.

EVIDENZE DA RICEVERE

- ☐ Certificato con perimetro ed ente
- ☐ Sintesi dei test con data ed esito
- ☐ Estratto di esempio del registro

Ricevuta il _____ • Valutazione: adeguata • da integrare • non adeguata

03 Dipendenze di secondo livello

COSA CHIEDERE

- Dove girano i modelli e chi fornisce l'infrastruttura.
- In quale paese stanno i dati a riposo e in transito.
- Chi altro può accedere: subfornitori, assistenza, sviluppo.
- Cosa succede se un subfornitore revoca il servizio.

EVIDENZE DA RICEVERE

- ☐ Elenco dei subfornitori con ruolo e paese
- ☐ Schema dei flussi di dati
- ☐ Contratti con i subfornitori sui punti 01 e 02

Ricevuta il _____ • Valutazione: adeguata • da integrare • non adeguata

04 Sostituibilità

COSA CHIEDERE

- Cosa resta all'azienda a fine contratto: dati, regole, configurazioni, sapere.
- In quali formati e in quanti giorni.
- Se il modello si può cambiare senza perdere il contesto.
- Cosa succede alla fabbrica se la licenza viene revocata.

EVIDENZE DA RICEVERE

- ☐ Procedura di esportazione con i formati
- ☐ Prova di esportazione su un campione
- ☐ Dichiarazione sui formati aperti

Ricevuta il _____ • Valutazione: adeguata • da integrare • non adeguata

Modulo di risposta del fornitore

Compilato dal fornitore e firmato. Ogni risposta rimanda a un documento allegato; una risposta senza allegato vale come non data. Yempik compila questo modulo per i propri clienti prima di qualunque proposta.

Fornitore

Referente

Data

01 Clausole

Notifica incidenti entro _____ ore (clausola n. _____)

Divieto di addestramento sui dati del cliente: sì · no (clausola n. _____)

Uscita e restituzione entro _____ giorni, formati _____

Legge applicabile _____ · foro _____

02 Evidenze

Certificazione _____ · ente _____ · scadenza _____ · perimetro _____

Ultimo test di sicurezza: data _____ · esito _____ · allegato n. _____

Registro delle operazioni: dove _____ · chi lo legge _____ · conservazione _____ mesi

03 Dipendenze di secondo livello

SUBFORNITORE	RUOLO	PAESE	DATI TRATTATI

Esecuzione dei modelli: nel perimetro del cliente · cloud dedicato in UE · cloud pubblico (paese _____)

Dati a riposo in _____ · dati in transito _____

04 Sostituibilità

Cosa viene restituito: dati · regole · configurazioni · registro · altro _____

Formati _____ · tempi _____ giorni · costo _____

Cambio di modello senza perdere il contesto: sì · no · come _____

Firma del fornitore _____ · Firma del responsabile sicurezza dell'azienda _____