Contratti con fornitori

Best Practice

Nel seguito sono elencati alcuni quesiti principali da porre ai vostri fornitori, quale base per l’elaborazione dei contratti per fornitori. In questo ambito dovete considerare nei vostri contratti (indipendentemente dal fornitore) i seguenti elementi chiave, segnatamente per adempiere le esigenze in materia di cibersicurezza e di protezione dei dati.

1. Obbligo di proteggere da ciberattacchi i propri mezzi informatici (dunque tutti i sistemi e tutte le reti IT) conformemente allo stato attuale della tecnica e in maniera adeguata ai rischi.
2. Obbligo di utilizzare metodi di crittografia moderni, sottoposti a manutenzione e conformi agli standard industriali, per proteggere dati sensibili in transito tra sistemi nonché dati sensibili a riposo in supporti di dati e backup online.
3. Obbligo di trasparenza degli accessi, per garantire la tracciabilità riguardo a chi accede a quali dati o sistemi e quando.
4. Obbligo di notificare (entro un determinato numero di ore / giorni) a un organo prestabilito i ciberattacchi, le violazioni della protezione dei dati e i punti di vulnerabilità dell’organizzazione, affinché sia possibile reagire rapidamente e in maniera adeguata agli eventi in materia di sicurezza.
5. Obbligo di ovviare immediatamente, a proprie spese (costi materiali, ore di lavoro ed eventualmente anche spese per fornitori di prestazioni esterni), ai punti di vulnerabilità individuati.
6. Obbligo del fornitore di osservare, nell’elaborazione di dati, i requisiti e le direttive sanciti nella legge federale sulla protezione dei dati (LPD). Va segnatamente menzionato che devono essere rilevati ed elaborati unicamente dati necessari per l’adempimento del compito.
7. Obbligo di tenere un elenco delle tipologie di dati sensibili destinati a essere elaborati da applicazioni.
8. Obbligo di rappresentare graficamente in un diagramma costantemente aggiornato come i dati sensibili giungono nei sistemi del fornitore e dove vengono infine salvati.
9. Obbligo di comunicare regolarmente le informazioni che il fornitore detiene sull’organizzazione nonché di distruggerli se non più necessari.
10. Definizione dei *service level agreement* (SLA) per l’approntamento delle prestazioni (p. es. definizione di concreti criteri prestazionali e standard qualitativi che il fornitore deve soddisfare, definizione dei criteri di valutazione delle prestazioni e delle conseguenze in caso di mancato adempimento degli standard).
11. Disciplinamento del ricorso a subfornitori/subappaltatori: se il fornitore è ricorso a subfornitori/subappaltatori, esigete che quest’ultimi e i collaboratori da esso impiegati sottostiano ai medesimi standard in materia di cibersicurezza e di protezione dei dati valevoli per il fornitore principale. Inserite una clausola in virtù della quale il ricorso a ulteriori subfornitori/subappaltatori o modifiche concernenti i subfornitori/subappaltatori sottostanno alla previa autorizzazione della vostra organizzazione.
12. Obbligo di tenere un elenco di subfornitori (imprese terze) che hanno accesso ai dati dei clienti. Tale elenco deve poter essere consultato in qualsiasi momento su richiesta.
13. Eventualmente, obbligo di documentare a ritmo semestrale la propria cibersicurezza, per garantire le esigenze a livello di compliance e l’efficacia delle misure di sicurezza (da concretizzare eventualmente nei contratti sotto forma di audit di sicurezza; possono essere menzionati in dettaglio i requisiti da soddisfare nel quadro degli audit sullo stato delle misure di cibersicurezza [p. es. audit svolti da un’impresa indipendente e riconosciuta]; possono essere previsti obblighi del fornitore in materia di verbalizzazione, sorveglianza e conservazione per mezzo di sistemi di sorveglianza, al fine di riconoscere attività sospette o potenziali violazioni in materia di sicurezza nonché redazione di un *incident response plan* comprendente direttive chiare per la notificazione, le misure di contenimento e l’analisi di eventi in materia di sicurezza).
14. Eventualmente, clausole contrattuali in materia di responsabilità, in virtù delle quali il fornitore è responsabile dei danni diretti, dei danni indiretti e dei danni conseguenti risultanti dalla mancata osservanza degli obblighi contrattuali nonché definizione di pene convenzionali in caso di violazione degli obblighi contrattuali in materia di cibersicurezza e protezione dei dati.
15. Eventualmente, obbligo di contrarre un’assicurazione di responsabilità civile e/o un’assicurazione in materia di cibersicurezza per i danni provocati dalla mancata osservanza di obblighi, da aspetti legati alla protezione dei dati o da violazioni della protezione dei dati.

\* \* \* \* \*