ATHLANTIC
compliance & certifications

AUDIT
2nd PART

COME VERIFICHI LA COMPLIANCE AL GDPR DEI TUOI FORNITORI ?

La scelta di un fornitore, specialmente se dovrà essere designato **Responsabile Esterno al trattamento dei dati personali** - come previsto dall'art. 28 del GDPR - implica una valutazione preliminare all'assegnazione dell'incarico, in termini di protezione dei dati personali.
Una valutazione positiva implicherà la **qualifica del fornitore**, che potrà essere inserito nelle attività di business con la tranquillità di aver affidato i propri dati ad un fornitore adeguato per ciò che concerne la protezione dei dati personali.

AUDIT

L'audit è uno strumento idoneo per verificare la **compliance rispetto al Regolamento Europeo sulla Protezione dei Dati Personali** (Reg. EU 2016/679 – GDPR).
Il Titolare del trattamento è così in grado di dimostrare fattivamente che la gestione dei dati affidati ai Responsabili Esterni sia in linea con le norme del Regolamento in materia di protezione dei dati personali, anche in termini di **Accountability**.
Durante l'Audit saranno verificati gli aspetti **formali**, **sostanziali** e afferenti alla **sicurezza delle informazioni** dell'organizzazione del Responsabile Esterno.

REPORT AUDIT

Al termine dell'attività, verrà rilasciato al Titolare il Report di Audit con l'indicazione del **livello di adeguatezza** delle misure di protezione dei dati personali del fornitore.
Nel Report di Audit saranno, inoltre, indicate le eventuali non conformità riscontrate, in modo che il titolare possa richiedere al fornitore le necessarie azioni correttive ai fini della compliance.

MODALITA' SVOLGIMENTO AUDIT

L'audit sarà condotto secondo quanto previsto dalle linee guida **ISO19011:2018** - ***Guidelines for Auditing Management Systems***.
L'attività si svolgerà con il Titolare o del Responsabile Esterno, in collaborazione con il DPO (Data Protection Officer) - ove presente - e con il personale referente dei sistemi informativi delle rispettive organizzazioni, al fine di verificare l'adeguatezza dell'organizzazione rispetto alla protezione dei dati personali.
L'auditor sottoporrà il fornitore ad una serie di domande, finalizzate a rilevare il livello di adeguatezza delle misure tecnico-organizzative implementate per garantire la protezione dei dati personali.
L'audit, in funzione delle specifiche esigenze del titolare, potrà essere svolto con l'ausilio di uno o più dei seguenti strumenti :

- **Due Diligence Checklist**, con l'acquisizione delle risposte fornite.
- **Audit Remoto**, con verifica della plausibilità delle risposte fornite.
- **Audit On-Site**, con verifica delle risposte fornite e rilievo delle evidenze in merito alle effettive misure adottate dal fornitore.

In tutti i casi, sulla base delle risposte/evidenze raccolte può essere definito un **livello di accettazione** per la qualifica del fornitore.

IL TEAM DI AUDIT

L'attività di audit sarà condotta dal team multidisciplinare di Athlantic, così composto:

- Ingegnere certificato Lead Autor ISO 27001 per la valutazione degli aspetti tecnico-organizzativi.
- Avvocato con competenze specifiche in materia di protezione dei dati per la valutazione degli aspetti legali.

In funzione delle necessità del cliente potranno essere aggiunti al team ulteriori professionisti con specializzazioni mirate al caso specifico.

GDPR COMPLIANCE