

2 GDPR come riferimento per gli Audit Interni

L'intero processo di un **Audit interno** deve focalizzare l'attenzione sugli adempimenti dei requisiti del GDPR e sull'applicazione delle Misure tecniche ed organizzative all'interno dell'Organizzazione e all'esterno di questa nell'ipotesi di trattamenti affidati a responsabili esterni.

Requisito	Adempimenti di verifica Audit	Riferimento articoli regolamento
Registro dei trattamenti	<ul style="list-style-type: none"> ▪ Compilazione registro dei trattamenti ▪ Aggiornamento registro dei trattamenti 	Art. 30
Sicurezza del trattamento (Valutazione rischi)	<ul style="list-style-type: none"> ▪ Compilazione del documento di valutazione dei rischi ▪ Aggiornamento documento di valutazione dei rischi 	Art. 32
Documento di valutazione di impatto privacy	<ul style="list-style-type: none"> ▪ Verifica dell'obbligo della valutazione di impatto ▪ Nomina DPO ▪ Compilazione del documento di valutazione di impatto ▪ Aggiornamento del documento di valutazione di impatto 	Art. 35
Consultazione preventiva	<ul style="list-style-type: none"> ▪ Verifica dell'obbligo della consultazione preventiva ▪ Inoltro della richiesta di parere ▪ Esecuzione delle prescrizioni segnalate dal Garante ▪ Controllo sulle prescrizioni eseguite 	Art. 36
Procedura data breach	<ul style="list-style-type: none"> ▪ Individuazione di un ufficio responsabile ▪ Preparazione di un protocollo azioni (anche per i responsabili esterni) ▪ Esecuzione di misure tecniche e organizzative inserite nel protocollo ▪ Verifica di sussistenza cause di esonero ▪ Preparazione di invio delle notificazioni (iniziali ed integrative) al Garante ▪ Preparazione per l'esecuzione delle prescrizioni del Garante ▪ Realizzazione modulo di invio di comunicazione agli interessati ▪ Presenza del registro della violazione dei dati 	Art. 33,34
Accordo con contitolari	<ul style="list-style-type: none"> ▪ Documento che stabilisce un accordo di contitolarità ▪ Misure organizzative e tecniche previste dall'accordo ▪ Punto di contatto unico nei confronti degli interessati 	Art. 26
Contratto di responsabile esterno	<ul style="list-style-type: none"> ▪ Mappa dell'esternalizzazione dei trattamenti ▪ Contratti con i responsabili esterni ▪ Misure normative, tecniche e organizzative previste dai contratti ▪ Controlli del responsabile esterno programmati ed eseguiti ▪ Patto di riservatezza con i dipendenti del responsabile esterno ▪ Stesura di modifiche e sottoscrizione delle clausole aggiuntive/sostitutive 	Art. 28
Contratto con sub responsabili	<ul style="list-style-type: none"> ▪ Mappatura della sub esternalizzazione dei trattamenti ▪ Stesura di apposite clausole nei contratti con i responsabili esterni ▪ Procedure selettive pianificate ed eseguite previste nelle clausole contrattuali ▪ Controlli pianificati ed eseguiti per il tramite del responsabile esterno ▪ Mappatura della sub esternalizzazione dei trattamenti ▪ Clausole nei contratti con i responsabili esterni ▪ Procedure pianificate ed eseguite selettive previste nelle clausole contrattuali ▪ Controlli pianificati ed eseguiti per il tramite del responsabile esterno 	Art. 28
Atto di nomina e disciplinare	<ul style="list-style-type: none"> ▪ Mappatura delle nomine esistenti e mantenimento di centri apicali interni 	Art. 5
Nomina dipendenti e collaboratori	<ul style="list-style-type: none"> ▪ Mappatura delle posizioni dei soggetti interni che trattano i dati 	Art. 29