Attività	Descrizione	Fatto
Implementazione di Misure di Sicurezza Adeguate	È fondamentale adottare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio. Questo include la protezione da accessi non autorizzati, perdite di dati, e danneggiamenti accidentali o illeciti. Ad esempio, l'implementazione di sistemi di autenticazione multi-fattore, crittografia dei dati sensibili, e il monitoraggio continuo delle infrastrutture IT possono rafforzare significativamente la sicurezza.	☐
Formazione e Consapevolezza del Personale	La sicurezza dei dati dipende significativamente dalla consapevolezza e dalla formazione del personale che gestisce e lavora con dati sensibili. È essenziale che tutto il personale sia formato regolarmente sulle migliori pratiche di sicurezza dei dati e sulle procedure da seguire in caso di violazione dei dati.	☐
Piani di Risposta agli Incidenti e Ripristino	Ogni organizzazione deve avere un piano di risposta agli incidenti ben definito e testato regolarmente. Questo dovrebbe includere procedure per il rilevamento rapido di un'incursione e per il ripristino tempestivo dei servizi e dei dati compromessi. Il piano di ripristino dovrebbe anche coprire il backup regolare dei dati e i protocolli di disaster recovery.	☐
Comunicazione Tempestiva delle Violazioni	Il GDPR richiede che le violazioni dei dati personali siano notificate all'autorità di controllo competente entro 72 ore dalla scoperta, a meno che la violazione non presenti un rischio per i diritti e le libertà degli individui. Le organizzazioni devono garantire che i canali di comunicazione interni supportino una rapida raccolta e comunicazione delle informazioni relative alla violazione.	☐
Valutazione e Aggiornamento Regolari:	Le misure di sicurezza e le politiche di protezione dei dati devono essere regolarmente vagliate e aggiornate in risposta ai cambiamenti nel panorama delle minacce e all'evoluzione delle tecnologie. Questo include l'aggiornamento dei sistemi operativi e delle applicazioni per correggere eventuali vulnerabilità note.	☐
Nomine 28 GDPR:	Quando si lavora con partner o fornitori terzi, è vitale stabilire chiaramente le responsabilità in materia di protezione dei dati. Gli accordi contrattuali devono specificare le aspettative e le responsabilità in materia di sicurezza dei dati e conformità normativa.	☐
Audit e Monitoraggio Continuo	Le organizzazioni dovrebbero condurre audit regolari della sicurezza dei dati e utilizzare sistemi di monitoraggio continuo per rilevare attività sospette o non autorizzate in tempo reale. Questo può aiutare a prevenire o limitare il danno di eventuali violazioni.	☐