	privata e l'elevato livello di conformità alla protezione dei dati". Lo scopo del sigillo non è solo quello di dimostrare la conformità dell'organizzazione certificata ai requisiti della legge britannica sulla protezione dei dati, ma anche quello di dimostrare il superamento dei requisiti legali "quando ci si occupa delle informazioni dei cittadini". L' ICO Privacy Seal mostrerà che l'organizzazione certificata è andata "al di là dell'obbligo di servizio". Gli operatori del sistema (diversi dall' ICO) si concentreranno su diversi settori, processi, prodotti o aree di conformità.
Requisiti e base normativa	Requisiti della legge britannica sulla protezione dei dati personali
Processo di certificazione	Le organizzazioni che desiderano richiedere un certificato di privacy ICO potranno quindi presentare una domanda ad un operatore del sistema interessato. Le organizzazioni riceveranno un certificato di privacy ICO "se possono dimostrare di soddisfare i criteri di valutazione dell'operatore dimostrando così di soddisfare i più elevati standard di protezione dei dati". Nonostante non sia direttamente coinvolto nel processo di assegnazione del certificato di privacy ICO, l'autorità di protezione dei dati manterrà i poteri sul funzionamento complessivo del processo di certificazione, come il potere di revocare l'approvazione a un operatore del sistema.
Accreditamento dell'organismo di certificazione	Organismo nazionale di accreditamento del Regno Unito (UKAS) e dovrà soddisfare ulteriori criteri stabiliti dall' ICO.
Durata del processo	Non specificato
Monitoraggio post-certificazione	Non specificato, solo l'intenzione dell'ICO di mantenere i poteri sul funzionamento complessivo del certificato.
Periodo di validità della certificazione	Non specificato
Risorse	Non specificato
Certificazioni rilasciate	Non applicabile (certificazione in fase di sviluppo)

9.5 A.5 – Certificazione basata su ISO/IEC 27001

Ambito	**Descrizione**
Campo di applicazione e oggetto	L' oggetto della certificazione può essere un unico processo di business (ad es. HR), un particolare servizio o l'intero processo di business di un'organizzazione. L'organizzazione certificata è in grado di identificare e mitigare i rischi per la sicurezza dell'informazione ai livelli desiderati, migliorare la fiducia nei propri servizi e gestire i processi di sicurezza dell'informazione.
Requisiti e base normativa	La norma ISO/IEC 27001 definisce i requisiti obbligatori per un sistema di gestione della sicurezza delle informazioni (ISMS).
Processo di certificazione	Il processo di certificazione comprende: 1. Un audit iniziale in due fasi, definito dalle norme ISO/IEC 17021 e ISO/IEC 27006, dove: 2. La fase 1 è dedicata alla revisione della documentazione dell'ISMS rispetto allo standard, e 3. La Fase 2: riesamina l'attuazione dell'ISMS all' interno del business e ne evidenzia l'adesione.