9 ANNEX A - ANALISI DELLA PANORAMICA DELLE CERTIFICAZIONI ESISTENTI

9.1 A.1 - ePrivacyseal

Ambito	Descrizione
Campo di applicazione e oggetto	ePrivacyseal certifica prodotti o servizi che sono in linea con il catalogo di criteri predefiniti del sistema ePrivacyseal.
Requisiti e base normativa	ePrivacyseal afferma che esso deriva i criteri dalla "normativa europea sulla tutela della privacy dei dati", alla quale si riferisce come "direttive UE applicabili in materia di protezione dei dati" e come regolamento generale dell'UE sulla protezione dei dati (GDPR). Inoltre, esistono una serie di criteri relativi al "comportamento pubblicitario online". Per quanto riguarda gli argomenti, i criteri coprono un'ampia gamma di aspetti, quali i principi del trattamento, i motivi per un trattamento lecito e i diritti degli interessati.
Processo di certificazione	Il processo di certificazione ePrivacySeal EU prevede cinque fasi: 1. Definizione degli obiettivi 2. Workshop 3. Ottimizzazione 4. Valutazione finale 5. Certificazione Le fasi 1-3 sono preparatorie al processo di valutazione ("valutazione finale"). Nell'ambito del workshop, gli esperti tecnici e legali esaminano il prodotto o servizio sulla base dei requisiti tecnici, organizzativi e legali di pertinenza. La fase di valutazione finale prevede una verifica da parte degli auditor effettuata sulla base del catalogo dei criteri di ePrivacy e delle raccomandazioni per il miglioramento. La fase finale del processo è la richiesta del certificato e la concessione della licenza sotto il marchio ePrivacyseal. ePrivacy prevede che i servizi di consulenza e audit siano forniti dalla ePrivacy GmbH, il conferimento del marchio di protezione dei dati personali avviene attraverso un'altra società, la ePrivacyseal GmbH.
Accreditamento dell'organismo di certificazione	La ePrivacy GmbH non prevede di essere essa stessa un organismo di certificazione accreditato dall'Ente nazionale di accreditamento della Germania, dove l'impresa si è stabilita.
Durata del processo	Non specificato
Monitoraggio post-certificazione	Non specificato
Periodo di validità della certificazione	Due anni, con possibile ri-certificazione
Risorse	Le informazioni relative ai costi dei servizi sono disponibili nei Termini e Condizioni della ePrivacy
Certificazioni rilasciate	ePrivacyseal EU è stato riconosciuto a 27 imprese (fino a settembre 2017)

9.2 A.2 - EuroPrise

Ambito	Descrizione

Campo di applicazione e oggetto	Oggetto dello schema sono i prodotti informatici quali hardware (ad es. un firewall hardware) e software (ad es. un'applicazione di database per un ospedale) e i servizi basati sull' informatica e il trattamento automatizzato dei dati (ad es. elaborazione dati commissionata, siti web). La valutazione di tale servizio include la valutazione delle live performances nel trattamento dei dati. Per valutazione si intende il prodotto al completo (ad esempio, un software) o una parte di prodotto. EuroPrise certifica inoltre i siti web e il "trattamento dei dati commissionati". L' obiettivo della certificazione è aumentare la trasparenza del mercato per i prodotti rilevanti ai fini della tutela della privacy e ampliare il mercato delle tecnologie di rafforzamento della tutela della privacy e accrescere la fiducia nelle tecnologie informatiche, certificando il rispetto delle norme europee sulla tutela della vita privata (Europrise 2017).
Requisiti e base normativa	Sono disponibili sul sito Internet di EuroPrise un elenco di criteri basato sulla direttiva 95/46/CE e sulla direttiva ePrivacy e un elenco di criteri basato sul GDPR e sulla direttiva ePrivacy. I criteri sono formulati come domande. Secondo EuroPrise: "*Not each and every question will be applicable to each and every product or service. The certification authority shall ensure that in any certification procedure the relevant criteria are applied and that all related questions are answered in a plausible manner, the appropriate granularity, and at a uniform and comparable level*". Non sono tuttavia disponibili informazioni sulla metodologia di valutazione nell'applicabilità di tali criteri.
Processo di certificazione	1. Gli esperti di EuroPrise valutano il prodotto o servizio in linea con i criteri di valutazione specificati per l'uso previsto, il quadro giuridico e l'ambiente tecnico del prodotto. Essi riferiscono i loro risultati in una relazione di valutazione. I criteri di valutazione comprendono: panoramica delle questioni fondamentali, legittimità del trattamento dei dati, misure tecnico-organizzative, diritti della persona interessata. 2. L' organismo di certificazione verifica i risultati della valutazione: L' organismo di certificazione verifica il rapporto di valutazione sotto il profilo della completezza, plausibilità e comparabilità con altre certificazioni. Il rapporto di certificazione viene pubblicato. Viene pubblicato inoltre, un breve rapporto pubblico che riassume i risultati della valutazione. 3. Assegnazione del marchio europeo sulla Privacy: L' organismo di certificazione compila un rapporto interno di certificazione, rilascia il sigillo e pubblica il breve rapporto di valutazione. La certificazione è rilasciata da EuroPrise Gmbh, l'unico ente che rilascia certificati ed effettua la valutazione della certificazione.
Accreditamento dell'organismo di certificazione	Nessuna informazione disponibile
Durata del processo	Non specificato
Monitoraggio post-certificazione	Non specificato
Periodo di validità della certificazione	Due anni, con possibile ri-certificazione

Risorse	Costi per la valutazione da parte degli esperti e onorari per la certificazione da parte degli organismi di certificazione. I costi della valutazione sono negoziati tra il richiedente e l'esperto. I costi per la certificazione sono fissati dall'organismo di certificazione.
Certificazioni rilasciate	Dal 2008 a settembre 2017: 68 Certificazioni (incluse le ri-certificazioni)

9.3 A.3 – CNIL Labels

Ambito	Descrizione
Campo di applicazione e oggetto	La certificazione può riguardare qualsiasi persona fisica o giuridica la cui procedura o prodotto corrisponda ad una delle norme pubblicate dalla CNIL nella Gazzetta ufficiale.
Requisiti e base normativa	I requisiti sono attualmente definiti in 4 standard: 1. Procedure di audit relative al trattamento dei dati personali: Il certificato di audit sulla privacy rilasciato dal CNIL *non si applica direttamente al trattamento effettuato*. Questo si applica alla procedura di audit utilizzata per verificare che tali processi siano conformi alla legge francese sulla protezione dei dati. La procedura descrive le varie fasi e i processi in base ai quali tale audit deve essere preparato, attuato e completato. Questo Include anche i requisiti riguardanti l'organizzazione che esegue l'audit e gli auditor stessi. Può essere rilasciato per l'elaborazione delle procedure di audit svolte dai fornitori di servizi (società di consulenza, avvocati, ecc.) o da organizzazioni (in questo caso si parla di internal audit). Il certificato di riservatezza del CNIL viene consegnato agli audit legali e tecnici. 2. Corsi di formazione sulla protezione dei dati: Il certificato CNIL può essere consegnato per i corsi di formazione interna ad un'organizzazione, sia per i corsi di formazione in aula che per e-learning, purché rispondano ai requisiti dello standard. 3. Cassette di sicurezza digitali: differiscono da uno spazio di memorizzazione in quanto i dati ivi memorizzati (documenti e alcuni metadati) sono accessibili solo al detentore della cassetta di sicurezza e a qualsiasi persona che abbia ricevuto mandato. I fornitori di servizi che forniscono una cassetta di sicurezza digitale (operatori) o ne propongono una agli utenti (fornitori) possono richiedere il sigillo di riservatezza. La richiesta può quindi essere presentata congiuntamente dall'operatore e dal suo cliente (fornitore). 4. Le procedure di governance dei dati personali sono tutte le misure, le regole e le best practices per la gestione dei dati personali di un'organizzazione. CNIL verifica la conformità della richiesta di certificazione dell'Organizzazione a 25 requisiti, tutti cumulativi, nella norma relativa a tre tematiche: organizzazione interna della gestione dei dati personali; procedura di verifica della conformità del trattamento con la Legge; gestione dei reclami e degli incidenti (CNIL 2017). 5. Il CNIL riconosce che un prodotto o una procedura è conforme alle disposizioni della legge francese sulla protezione dei dati personali. Essa non intende esentare i suoi titolari dalle formalità amministrative (CNIL 2017)
Processo di certificazione	La procedura consiste nelle seguenti fasi:

	1. Domanda: il richiedente invia la domanda mediante un modulo disponibile sul sito web della CNIL. Esso deve fornire tutti gli elementi atti a dimostrare che la sua procedura o il suo prodotto sono conformi ai requisiti della norma. 2. Valutazione dell'ammissibilità: CNIL dispone di 2 mesi per analizzare l'ammissibilità di una domanda. In caso contrario, essa è considerata ammissibile. 3. Esame da parte dell'unità Privacy Seals del CNIL in cui possono aver luogo scambi tra la divisione Privacy Seals e il richiedente per chiarire alcuni punti della domanda. 4. Valutazione della conformità da parte del comitato di certificazione: Quando l'esame da parte della Privy Seals Unit è completato, questo viene presentato al comitato di certificazione, che svolge l'analisi legale, sviluppa le raccomandazioni e pianifica le azioni correttive. 5. Presentazione e garanzia del marchio di riservatezza: La decisione di rilasciare il certificato di riservatezza viene presa dall'Autorità per la protezione dei dati personali riunita in seduta plenaria. 6. Notifica e pubblicazione: La decisione viene inviata al richiedente, accompagnata da loghi personalizzati a nome del titolare del marchio di protezione dei dati personali, nonché dalle norme per l'utilizzo del marchio, e viene pubblicata poi sul sito web Légifrance (CNIL 2017) della CNIL.
Accreditamento dell'organismo di certificazione	Non applicabile (I certificati sono rilasciati solo dalla CNIL, non vi sono organismi di certificazione coinvolti)
Durata del processo	L' esame della domanda di certificazione avviene in due fasi: l'ammissibilità della domanda e l'esame. Il CNIL dispone di 2 mesi per analizzare l'ammissibilità di una domanda. Il periodo di esame varia. Il certificato di riservatezza deve essere consegnato entro 6 mesi dal ricevimento degli ultimi elementi necessari per soddisfare i requisiti della norma.
Monitoraggio post-certificazione	Il CNIL può verificare in qualsiasi momento e con qualsiasi mezzo che il prodotto o la procedura certificati siano conformi alle condizioni definite nella norma. CNIL può ritirare un certificato di privacy. Sul suo sito Internet, il CNIL tiene un elenco aggiornato dei prodotti e delle procedure certificati, con l'identità dei propri titolari.
Periodo di validità della certificazione	3 anni, con possibilità di ri-certificazione/rinnovo
Risorse	Non viene corrisposta alcuna tassa al CNIL per il rilascio del sigillo. Tuttavia, il richiedente potrebbe dover dedicare risorse organizzative per conformarsi agli standard e adattare le proprie pratiche.
Certificazioni rilasciate	CNIL ha rilasciato 91 certificazioni (incluse le ri-certificazioni) fino a settembre 2017

9.4 A.4 – ICO Privacy Seal

Ambito	Descrizione
Campo di applicazione e oggetto	Nel 2015, il commissario britannico per l'informazione ha annunciato la sua intenzione di introdurre un certificato nazionale di privacy, quale timbro di approvazione "che dimostri la buona prassi in materia di tutela della vita

	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.

	4. Verifiche di sorveglianza condotte nel primo e nel secondo anno al fine di verificare la continua conformità dell'organizzazione allo standard, 5. Un audit di ri-certificazione nel terzo anno prima della scadenza della certificazione. La certificazione potrà essere successivamente rinnovata per successivi periodi triennali (ENISA 2013). 6. Il certificato può essere revocato o sospeso se la revisione annuale lo giustifica. L'ente certificante sospende la certificazione nei casi in cui, ad esempio, il sistema di gestione certificata del cliente ha persistentemente o gravemente mancato di soddisfare i requisiti di certificazione, inclusi i requisiti per l'efficacia del sistema di gestione, il cliente certificato non consente di effettuare audit di sorveglianza o ri-certificazione alle frequenze richieste o il cliente certificato ha volontariamente richiesto una sospensione (ENISA 2013).
Accreditamento dell'organismo di certificazione	ISO indirizza i propri clienti ad enti di certificazione accreditati, che hanno acquisito una competenza indipendente e riconosciuta da parte di un Organismo di Accreditamento. Gli organismi di certificazione accreditati devono essere in grado di offrire una certificazione conforme alla norma ISO/IEC 17021-1, che contiene principi e requisiti per la competenza, la coerenza e l' imparzialità degli organismi che forniscono audit e certificazione di tutti i tipi di sistemi di gestione e alla norma ISO/IEC 27006 che stabilisce i requisiti per gli organismi che forniscono audit e certificazione dei sistemi di gestione della sicurezza delle informazioni (documento di criteri per l' accreditamento, peer assessment o altri processi di audit) (ISO 2017).
Durata del processo	La durata della procedura di certificazione nel suo complesso dipende dall'ambito della certificazione. Secondo uno studio passato, il periodo di tempo necessario alle imprese oggetto dell'indagine per prepararsi alla certificazione variava tra i 3 e i 18 mesi, la maggior parte delle imprese ha richiesto dai 6 ai 12 mesi per completare la preparazione. Il processo di certificazione in sé non ha superato la settimana.
Monitoraggio post-certificazione	Dipende dall' organismo che fornisce la certificazione
Periodo di validità della certificazione	3 anni
Risorse	Non specificato
Certificazioni rilasciate	Nel 2015 sono stati rilasciati in tutto il mondo 27536 certificati, tenendo conto solo di quelli rilasciati da organismi di certificazione accreditati (ISO 2015).

9.6 A.6 – Certificazione basata su ISO/IEC 27018

Ambito	Descrizione
Campo di applicazione e oggetto	Il codice di condotta ISO/IEC 27018:2014 stabilisce gli obiettivi di controllo, i controlli e le linee guida comunemente accettati per l'attuazione di misure volte a proteggere le informazioni personali (PII) in conformità ai principi di riservatezza contenuti nella norma ISO/IEC 29100 per l'ambiente di cloud computing pubblico. Specifica le linee guida basate sulla norma ISO/IEC 27002, tenendo conto dei requisiti normativi per la protezione della PII che potrebbero essere applicabili nel contesto

	dell'ambiente o degli ambienti a rischio per la sicurezza dell'informazione di un fornitore di servizi pubblici in-the-cloud.
Requisiti e base normativa	I controlli riguardano le politiche di sicurezza dell'informazione, le organizzazioni per la sicurezza delle informazioni, la sicurezza delle risorse umane, la gestione degli asset, il controllo degli accessi, la crittografia, la sicurezza fisica e ambientale, la sicurezza delle operazioni, la sicurezza delle comunicazioni, l'acquisizione dello sviluppo e la manutenzione del sistema, le relazioni con i fornitori, la gestione degli incidenti relativi alla sicurezza dell'informazione, la gestione della continuità, il rispetto dei requisiti legali e contrattuali. In ANNEX A sono previsti nuovi controlli, classificati in base ai principi di riservatezza della norma ISO/IEC 29100.
Processo di certificazione	Vedere tabella ISO/IEC 27001
Accreditamento dell'organismo di certificazione	Vedere tabella ISO/IEC 27001
Durata del processo	Vedere tabella ISO/IEC 27001
Monitoraggio post-certificazione	Vedere tabella ISO/IEC 27001
Periodo di validità della certificazione	Vedere tabella ISO/IEC 27001
Risorse	Vedere tabella ISO/IEC 27001
Certificazioni rilasciate	Vedere tabella ISO/IEC 27001

9.7 A.7 – Sistema PrivacyMark

Ambito	**Descrizione**
Campo di applicazione e oggetto	Il sistema PrivacyMark è gestito da JIPDEC, un'organizzazione Giapponese senza scopo di lucro che ha l'obiettivo di sviluppare e proporre meccanismi e infrastrutture quadro per garantire la sicurezza e la protezione, nonché l'uso delle informazioni informatiche e digitali.
Requisiti e base normativa	Il Sistema PrivacyMark è basato sullo standard tecnico JISQ15001 riguardante la protezione delle informazioni personali nei sistemi di gestione. I requisiti del JISQ15001:2006 riguardano: a. i requisiti generali, b. la politica di protezione dei dati personali, c. il piano (specifica dei dati personali, leggi e linee guida stabilite dallo Stato, ruoli, responsabilità, ecc.), d. l'attuazione e il funzionamento (principi di acquisizione, utilizzo e fornitura dei dati personali, controlli appropriati, diritti delle persone), e. la documentazione, f. il meccanismo di reclamo, g. le ispezioni, h. le azioni correttive e preventive.
Processo di certificazione	La valutazione della conformità del richiedente ai requisiti della norma è costituita da due componenti principali: una valutazione della documentazione e una valutazione in loco. L'obiettivo della valutazione

	complessiva è quello di decidere se il sistema di gestione della protezione delle informazioni personali (PMS) del richiedente gestisce adeguatamente i rischi connessi al trattamento delle informazioni personali. Il Sistema PrivacyMark collabora con un totale di 1.246 valutatori, di cui 305 sono lead assessor. Esistono diciotto organismi di valutazione e tre organismi di formazione.
Accreditamento dell'organismo di certificazione	Non specificato
Durata del processo	Non specificato
Monitoraggio post-certificazione	Non specificato
Periodo di validità della certificazione	Due anni, con possibilità di ri-certificazione
Risorse	La struttura tariffaria del Sistema PrivacyMark tiene conto della scala di business del richiedente (piccolo, medio, grande) e se la richiesta riguarda una prima applicazione piuttosto che un rinnovo del PrivacyMark.
Certificazioni rilasciate	Entro il 2017, 21.307 certificazioni hanno ottenuto il marchio PrivacyMark, incluse le ri-certificazioni.

9.8 A.8 – Certificazione Privacy by Design della Ryerson University & Deloitte Canada

Ambito	Descrizione
Campo di applicazione e oggetto	I'obiettivo dichiarato è quello di "far progredire l'operatività della Privacy by Design" e di aiutare le aziende e le organizzazioni che stanno lavorando per integrare la Privacy by Design nei loro processi quotidiani. La certificazione valuta: sistemi IT, "accountable business practices" e infrastruttura di rete.
Requisiti e base normativa	I criteri si basano sui 7 principi fondamentali della Privacy By Design: 1. Proattivo non reattivo; preventivo non correttivo 2. Privacy come impostazione predefinita 3. Privacy integrata nel design 4. Funzionalità completa - somma positiva, non somma zero 5. Sicurezza end-to-end - Protezione completa del ciclo di vita 6. Visibilità e trasparenza – Keep it Open 7. Rispetto della privacy dell'utente - Keep it User-Centric L' elenco dei criteri e le relative attività di controllo sono disponibili online. La Certificazione Privacy by Design non significa conformità alle leggi sulla privacy dell'Ontario.
Processo di certificazione	Il processo inizia con l'applicazione dell'organizzazione interessata. Il "Privacy and Big Data Institute" esamina l'applicazione e trasmette le informazioni a Deloitte Canada per iniziare la valutazione. La ricorrente stipula un accordo separato con la Deloitte Canada. Deloitte Deloitte "esamina i prodotti, i servizi e/o le offerte certificate, conduce colloqui ed esamina i processi operativi. Deloitte pubblicherà quindi un rapporto basato sulla metodologia di valutazione e sulla tecnica della scorecard sviluppata esclusivamente per la Privacy by Design Certification che esamina l'aderenza dell'organizzazione alla Privacy by Design". In seguito al

	rapporto di Deloitte, il Privacy by Design Centre of Excellence emette una decisione sul rilascio della certificazione. L'Organizzazione cui viene concessa la Certificazione sulla Priivacy by Design, può utilizzare il relativo certificato, chiamato "Certification Shield".
Accreditamento dell'organismo di certificazione	Non Specificato
Durata del processo	Non Specificato
Monitoraggio post-certificazione	Annuale. Le certificazioni devono essere rinnovate annualmente per essere mantenute aggiornate. Il rinnovo richiede un'attestazione da parte dell'Organizzazione attestante che non vi è stata alcuna modifica che abbia influito sulla certificazione da loro rilasciata. Inoltre, viene applicata una tassa di rinnovo.
Periodo di validità della certificazione	Tre anni
Risorse	Non Specificato
Certificazioni rilasciate	7 certificazioni dal 2015 al settembre 2017.