Europrivacy.com
Privacy Audit and Certification

Schema di Certificazione Europrivacy™/® Specifiche Generali e Requisiti

Identificatore:	EP-CS.1
Versione:	77
Data:	4 gennaio 2024
Stato della pubblicazione:	**Riservato**
Siti web:	http://www.europrivacy.com
	www.eccpcenter.com
Contatto:	contact@europrivacy.com

Indice

1. Introduzione e riconoscimenti

Con l'evoluzione delle tecnologie dell'informazione e della comunicazione (ICT), la protezione dei dati è diventata una preoccupazione crescente per gli individui e le società. L'Unione Europea e i singoli Paesi hanno adottato normative e regolamenti formali per tutelare i diritti e le libertà fondamentali delle persone fisiche e, in particolare, il diritto alla protezione dei dati personali.

Lo Schema di Certificazione Europrivacy è stato sviluppato per valutare la conformità delle operazioni di trattamento dei dati personali da parte dei Titolari e dei Responsabili del trattamento agli obblighi del Regolamento generale europeo sulla protezione dei dati (GDPR), e per essere facilmente estendibile agli obblighi complementari in materia di protezione dei dati, come le normative nazionali e/o gli obblighi specifici settoriali.

I criteri Europrivacy sono stati approvati dal Comitato europeo per la protezione dei dati (EDPB) per fungere da sigillo formale europeo per la protezione dei dati applicabile alle attività di trattamento dei dati svolte dai Titolari o dai Responsabili del trattamento.

L'utilizzo della metodologia e dei criteri dello Schema di certificazione consente di ridurre i rischi per tutte le parti. Quando il trattamento dei dati personali è soggetto a uno stretto monitoraggio basato su requisiti chiari, i rischi per gli interessati, i Titolari e i Responsabili del trattamento sono ridotti.

Lo Schema di Certificazione e i suoi criteri sono stati concepiti per essere utilizzati:

a) come sigillo europeo per la protezione dei dati ai sensi dell'art. 42 del GDPR;
b) come meccanismo per i trasferimenti internazionali di dati da parte degli importatori di dati [1];
c) come meccanismo di certificazione conforme al GDPR e riconoscibile da altre giurisdizioni [2];
d) per gli audit interni e le certificazioni volontarie senza i benefici e i vantaggi di una certificazione ufficiale GDPR, a condizione che non vi sia alcun rischio di confusione con la regolare certificazione ai sensi del GDPR;
e) per documentare la conformità e ridurre i rischi di non conformità, senza necessariamente perseguire una certificazione formale.

Lo Schema di Certificazione Europrivacy è stato sviluppato con il supporto di progetti di ricerca europei co-fondati dalla Commissione europea e dal Ministero svizzero per la ricerca e l'istruzione. Lo Schema di Certificazione iniziale è stato sviluppato da Archimede Solutions SARL. Il ruolo e la funzione di Scheme Owner sono stati delegati al Centro europeo per la certificazione e la privacy (ECCP) in Lussemburgo. L'ECCP è incaricato di esaminare, migliorare e aggiornare lo Schema di certificazione con il supporto di un comitato internazionale di esperti in materia di protezione dei dati, sicurezza ICT e certificazione (di seguito denominato "Comitato internazionale di esperti Europrivacy").

Lo schema di certificazione è destinato principalmente a certificare la conformità del trattamento dei dati personali secondo la ISO/IEC 17065. È stato ottimizzato per sfruttare appieno la capacità dell'ISO/IEC 17065 di essere esteso a requisiti di certificazione complementari, come l'ISO/IEC 17021-1. Ove applicabile, Europrivacy può essere applicato anche a diversi ambiti di certificazione, a condizione che sia conforme alle normative applicabili e ai requisiti complementari.

[1] L'utilizzo di Europrivacy come meccanismo per il trasferimento internazionale dei dati ai sensi dell'art. 46 del GDPR è in attesa di approvazione da parte dell'EDPB. Gli importatori di dati non soggetti al GDPR devono adottare un adeguato strumento contrattualmente vincolante.
[2] Il riconoscimento formale in altre giurisdizioni può essere soggetto a requisiti complementari.

2. Ambito e scopo dello Schema di Certificazione

2.1. Ambito di applicazione del presente documento

Il presente documento presenta le specifiche e i requisiti generali dello Schema di certificazione Europrivacy (di seguito denominato "Schema di Certificazione"), comprese le politiche, i processi e le procedure che gli organismi di certificazione (di seguito denominati "Organismi di Certificazione") devono applicare e rispettare. Questo documento principale è completato da una serie di documenti complementari che forniscono informazioni più dettagliate e che fanno anch'essi parte dello Schema di Certificazione.

Le sezioni da 2 a 5 sono incentrate sulla panoramica generale di Europrivacy, comprese le definizioni e i riferimenti.

Le sezioni da 6 a 11 sono incentrate sul processo di certificazione, compresi i criteri.

Le sezioni da 12 a 17 sono incentrate sui requisiti organizzativi dell'Organismo di Certificazione.

Le sezioni 18-19 sono incentrate sulla gestione dello Schema di Certificazione, compresi l'accreditamento e la concessione di licenze.

2.2. Scopo e ambito della certificazione Europrivacy

Europrivacy è stato progettato per fornire un sistema di certificazione chiaro e completo sulla conformità del trattamento dei dati alle normative sulla protezione dei dati personali, con particolare attenzione al GDPR. Esso intende fornire un livello di garanzia indipendente, imparziale e ragionevole della conformità del trattamento dei dati al GDPR e ai corrispondenti diritti fondamentali degli interessati e, se del caso, a requisiti complementari, come le normative nazionali e i requisiti specifici del settore.

È stato progettato nel rispetto del diritto internazionale, dei principi ISO e dei requisiti dell'Organizzazione Mondiale del Commercio.

Lo Schema di Certificazione è stato studiato e strutturato per essere applicabile a diverse attività di trattamento dei dati svolte da Titolari e/o Responsabili del trattamento (di seguito "Richiedente"). È stato sviluppato con un'attenzione specifica ai rischi che emergono dall'uso di tecnologie innovative, come l'Internet delle Cose e l'Intelligenza Artificiale. La sua architettura consente di estendere i criteri fondamentali con requisiti complementari nazionali e specifici del settore.

Europrivacy è stato strutturato in modo da essere affidabile e conveniente per le PMI. Ove applicabile, integra e sfrutta altre certificazioni, come le ISO/IEC 27001 e 27701, al fine di evitare la duplicazione degli sforzi e dei costi di certificazione.

L'ambito della certificazione Europrivacy è soggetto ad alcune restrizioni:

- Il Richiedente deve aver designato un Responsabile della Protezione dei Dati – "DPO" (o una funzione equivalente che può essere esterna) incaricato di monitorare la conformità delle attività di trattamento dei dati da certificare;
- Il Richiedente deve avere un registro delle sue attività di trattamento dei dati personali;
- L'ECCP tiene un elenco di domini applicativi che sono esclusi dal campo di applicazione della regolare certificazione Europrivacy. In caso di dubbi sull'applicabilità della certificazione a domini specifici, il Richiedente o l'Organismo di Certificazione devono contattare l'ECCP.

La certificazione Europrivacy intende fornire un livello di garanzia indipendente, imparziale e ragionevole della conformità del trattamento dei dati al Regolamento generale europeo sulla protezione dei dati e, ove applicabile, ai requisiti complementari di protezione dei dati, come le normative nazionali o i requisiti specifici di un dominio, utilizzando le estensioni di certificazione (vedere la sezione 11.1).

2.2.1. Ambito normativo della certificazione

Lo Schema di Certificazione Europrivacy è stato progettato per rispondere ai requisiti del GDPR, in particolare:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Lo Schema di Certificazione si concentra sugli obblighi del GDPR la cui inosservanza potrebbe mettere a rischio i diritti e le libertà degli interessati, i loro dati personali o il Richiedente.

La consegna della certificazione GDPR in conformità agli articoli 42 e 43 del GDPR richiede la conformità con:

- le linee guida del EDPB, tra cui:
  - Linee guida 4/2018 sull'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del Regolamento generale sulla protezione dei dati (2016/679);
  - Linee guida 1/2018 sulla certificazione e sull'individuazione dei criteri di certificazione ai sensi degli articoli 42 e 43 del Regolamento 2016/679;
  - Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti;
- gli obblighi applicabili previsti dalle normative sulla protezione dei dati degli Stati membri dell'UE.

Sebbene lo Schema di Certificazione sia principalmente incentrato sulla conformità al GDPR, il Richiedente e l'Organismo di Certificazione possono concordare di estendere l'Ambito Normativo della certificazione aggiungendo requisiti complementari, quali:

- Direttive e regolamenti europei, come le direttive ePrivacy e NIS[3] ;
- Normativa nazionale sulla protezione dei dati;
- Requisiti specifici del dominio o ISO/IEC.

Indipendentemente dall'estensione, la certificazione deve sempre dimostrare la conformità ai requisiti del GDPR. L'estensione dell'Ambito Normativo deve essere chiaramente comunicata con il certificato, come previsto al punto 11.1.

Lo Schema di Certificazione è destinato ad essere adattato alle successive evoluzioni e aggiornamenti della normativa sopra citata, anche, ove applicabile, alla giurisprudenza e all'evoluzione dell'ambiente tecnologico.

2.2.2. Campo di applicazione materiale della certificazione

Lo schema di certificazione è stato studiato, sviluppato e specificato per fornire valutazioni complete, omogenee e sistematiche della conformità alla protezione dei dati. Sebbene **il suo obiettivo principale sia quello di certificare le operazioni di trattamento dei dati personali**, lo Schema di Certificazione è stato progettato per essere il più completo possibile, allineandosi ai requisiti ISO applicabili per la valutazione di prodotti, processi e servizi (ISO/IEC 17065), nonché alla ISO/IEC 17021-1, con particolare attenzione alla protezione dei dati.

In base al Target of Evaluation, gli Auditor devono applicare verifiche e controlli specifici e complementari specificati dallo Scheme Owner. Questo meccanismo consente di applicare lo Schema di Certificazione a diverse attività di trattamento dei dati, rispondendo ai requisiti specifici del settore e della tecnologia.

2.2.3. Ambito geografico della certificazione

L'ambito geografico dello Schema di Certificazione non è formalmente limitato e può essere utilizzato dai Richiedenti, ma:

a. I sigilli europei per la protezione dei dati consegnati ai sensi del GDPR a richiedenti situati al di fuori del SEE sono soggetti a requisiti complementari.[4]
b. I criteri di certificazione possono essere difficili e potenzialmente impossibili da soddisfare in paesi il cui contesto giuridico non garantisce un'adeguata protezione dei dati personali e dei diritti degli interessati.

[3] Direttiva (UE) 2002/58/CE e 2016/1148/CE del Parlamento europeo e del Consiglio.
[4] L'applicabilità di Europrivacy ai Richiedenti non appartenenti allo SEE è in fase di revisione da parte dell'EDPB, in attesa di una decisione.

2.2.4. Chiarezza dell'ambito e del Target of Evaluation della certificazione

L'Ambito Normativo della certificazione e i Target of Evaluation di ciascun certificato consegnato devono essere chiaramente specificati e designati. I certificati consegnati sono pubblicati nel Registro dei Certificati Europrivacy (di seguito "Registro") e possono essere facilmente accessibili e verificati grazie all'identificativo del certificato e all'indirizzo del sito web allegati a ciascun marchio di conformità.

2.3. Allineamento con il Regolamento europeo sulla protezione dei dati

2.3.1. Adattamento all'evoluzione della normativa sulla protezione dei dati personali

Poiché le normative sulla protezione dei dati sono in continua evoluzione, si prevede che lo Schema di Certificazione venga regolarmente aggiornato per tenere conto dell'evoluzione del contesto legale e della giurisprudenza in materia di protezione dei dati. Lo scopo è anche quello di consentire un processo di miglioramento continuo.

Lo Scheme Owner, supportato da un Comitato Internazionale di Esperti, è responsabile della revisione e dell'aggiornamento dello Schema di Certificazione.

2.3.2. Requisiti dello Schema di Certificazione

Lo Schema di Certificazione è stato progettato tenendo conto dei seguenti elementi:

a) deve essere accessibile alle micro, piccole e medie imprese;
b) è disponibile attraverso un processo trasparente;
c) chiarisce che la certificazione non riduce la responsabilità del Richiedente nell'adempimento dei suoi obblighi normativi in materia di protezione dei dati;
d) segue i criteri approvati dal Comitato europeo per la protezione dei dati e/o dall'Autorità competente per la protezione dei dati;
e) è conforme ai requisiti pertinenti delle norme ISO/IEC applicabili;
f) il Richiedente è tenuto a fornire all'Organismo di Certificazione tutte le informazioni e l'accesso alle proprie attività di trattamento necessarie per condurre la procedura di certificazione;
g) la Certificazione ha una durata massima di tre anni;
h) il rinnovo della certificazione è concesso a condizione che il Richiedente soddisfi le condizioni e i requisiti stabiliti per il suddetto rinnovo.

2.3.3. Requisiti degli Organismi di Certificazione

L'Organismo di Certificazione deve rispettare i requisiti di accreditamento e i regolamenti applicabili.

Secondo il GDPR, l'Organismo di Certificazione deve specificatamente:

a) **dimostrare un livello adeguato di competenza nella protezione dei dati**;
b) **dimostrare indipendenza e imparzialità**;
c) **rispettare i requisiti della norma ISO/IEC 17065**[5] per la consegna delle certificazioni, comprese procedure e strutture adeguate:
   - rilasciare, rivedere periodicamente e ritirare certificazioni, sigilli e marchi;
   - controllare che le entità certificate siano trasparenti nei confronti degli interessati e del pubblico;
   - gestire i reclami relativi a violazioni della certificazione e/o al modo in cui la certificazione è stata o viene attuata;
d) **rispettare i requisiti di accreditamento applicabili stabiliti dall'Autorità di Controllo competente**, quali:
   - dimostrare processi adeguati per la protezione dei dati durante il trattamento dei dati personali;
   - essere accreditati dall'Autorità di Controllo o di Accreditamento competente.

Gli organismi esterni, come i laboratori e gli Auditor, che svolgono parte delle attività di certificazione per conto di un Organismo di Certificazione devono dimostrare di possedere un'adeguata competenza in materia di protezione dei dati, nonché un'appropriata conoscenza dello Schema di Certificazione pertinente al loro lavoro.

[5] ISO/IEC 17065/2012 o posteriore (ultima versione disponibile).

Le Autorità di Controllo nazionali ed europee non hanno bisogno di una licenza formale, a condizione che rispettino le normative applicabili, i requisiti dello Schema di Certificazione e che utilizzino quest'ultimo con l'autorizzazione dello Scheme Owner.

2.4. Processo di miglioramento continuo

Per garantire un'efficace protezione dei dati è necessario tenere conto dell'evoluzione della normativa (giurisprudenza, pubblicazioni dell'EDPB, ecc.), dell'ambiente tecnologico (che può influire, ad esempio, sul rischio di deanonimizzazione dei dati) e degli insegnamenti tratti dalla pratica.

Lo Schema di Certificazione e le relative risorse, compresi i criteri, le verifiche e i controlli, possono essere rivisti e aggiornati ogni volta che è necessario attraverso un processo di miglioramento continuo per affrontare questi cambiamenti ed evitare l'emergere di lacune tra i requisiti dello Schema di Certificazione e i requisiti legali.

Inoltre, sfrutta l'esperienza degli Auditor e degli Esperti Tecnici che sono invitati a presentare suggerimenti di miglioramento allo Scheme Owner. I suggerimenti di miglioramento presentati vengono esaminati dal Comitato Internazionale di Esperti dello Scheme Owner e i miglioramenti approvati vengono rilasciati in versioni aggiornate. Tutti gli adattamenti devono contribuire a migliorare l'applicabilità e l'affidabilità del processo di certificazione e non indebolirlo.

Il disegno seguente riassume il processo:

Figura 1 Processo di miglioramento continuo del sistema di certificazione Europrivacy

2.5. Limiti intrinseci alla certificazione

2.5.1. Limitazione generale

Un certificato Europrivacy è il risultato finale di un processo di certificazione, che indica che la certificazione è stata eseguita secondo i requisiti e le procedure dello Schema di Certificazione di riferimento e che il Target of Evaluation certificato ha soddisfatto con successo i requisiti specificati dallo Schema di Certificazione per il Target of Evaluation durante il processo di valutazione e/o di audit, e che il Richiedente si è impegnato a rispettarli per la durata del Certificato.

Un processo di certificazione si basa sui risultati identificati dall'Auditor dopo aver seguito una metodologia chiaramente specificata e sistematica. Si basa su campioni analizzati e/o su audit mirati effettuati in un determinato periodo di tempo. Un certificato è un'indicazione professionale e imparziale di conformità verificata da una terza parte indipendente, ma non può garantire che il Target of Evaluation certificato sia e sarà privo di qualsiasi Non Conformità. La conformità legale rimane di esclusiva responsabilità del Richiedente, che deve costantemente garantire che il proprio Target of Evaluation certificato sia pienamente conforme ai requisiti dello Schema di Certificazione e alle normative applicabili in materia di protezione dei dati.

Una certificazione non è né una raccomandazione per l'uso di un prodotto, un processo, un servizio o un sistema di gestione, né una garanzia che esso sia totalmente privo di vulnerabilità sfruttabili.

Come promemoria:

1) Il ruolo principale dello Scheme Owner è quello di mantenere e aggiornare lo schema di certificazione;
2) L'Organismo di Certificazione è responsabile della valutazione, dell'audit e della decisione di certificare il Target of Evaluation come conforme ai requisiti dello Schema di Certificazione;
3) Il Richiedente rimane l'unico responsabile della conformità del proprio trattamento dei dati personali alle normative sulla protezione dei dati.

Né l'Organismo di Certificazione né lo Scheme Owner sono responsabili per qualsiasi perdita o danno, di qualsiasi tipo e in qualsiasi modo, derivante dall'uso di un prodotto, di un processo, di un servizio o di qualsiasi altro elemento coperto da una certificazione.

Il certificato Europrivacy non libera il titolare del certificato dalle sue responsabilità legali, compresa l'eventuale non conformità alle normative applicabili in materia di protezione dei dati.

L'utilizzo dello Schema di Certificazione è subordinato all'accettazione dei Termini e condizioni generali di Europrivacy, disponibili online sul sito web di Europrivacy : https://europrivacy.com

2.5.2. Limitazioni specifiche del GDPR

La certificazione rilasciata ai sensi degli articoli 42 e 43 del GDPR deve essere conforme alla politica, alle linee guida e ai requisiti del Comitato europeo per la protezione dei dati, quali:

- Richiedere che l'ambito della certificazione si concentri sul trattamento dei dati personali.

2.5.3. Restrizioni all'uso non regolamentato dello Schema di Certificazione e dei Criteri

Europrivacy ha lo scopo di fornire certificazioni conformi ai requisiti del GDPR e alle normative nazionali applicabili in materia di protezione dei dati. I suoi criteri possono essere utilizzati come base per rilasciare certificazioni al di fuori dell'ambito di applicazione del GDPR, a condizione di evitare il rischio di confusione con le certificazioni GDPR. Ad esempio, i certificati rilasciati dovranno utilizzare un nome e un marchio di conformità diversi. Tali certificazioni saranno soggette a regole complementari che saranno specificate dallo Scheme Owner in un documento separato. Dovranno inoltre essere conformi alla normativa applicabile e ai diritti di proprietà intellettuale. Le certificazioni rilasciate al di fuori del GDPR non sono riconosciute come certificazioni GDPR.

3. Documenti di riferimento

3.1. Riferimenti normativi e prescrittivi

Lo Schema di Certificazione fa riferimento a diversi documenti, tra cui documenti di riferimento esterni, come gli standard ISO e le normative sulla protezione dei dati, nonché documenti di riferimento interni che completano e dettagliano ulteriormente lo Schema di Certificazione.

3.1.1. Documenti normativi complementari di Europrivacy

Lo Schema di Certificazione è integrato da diversi documenti gestiti dall'ECCP e dal suo Comitato Internazionale di Esperti, tra cui:

a) Termini e condizioni generali di Europrivacy;
b) Limitazioni del campo di applicazione della certificazione Europrivacy;
c) Linee guida Europrivacy sull'uso di Criteri, Verifiche e Controlli;
d) Elenco Europrivacy di Criteri, Verifiche e Controlli che gli Auditor devono utilizzare per le certificazioni Europrivacy;
e) Estensioni e adattamenti del sistema di certificazione Europrivacy (facoltativi);
f) Gestione delle competenze del personale coinvolto nelle certificazioni Europrivacy;
g) Regole e linee guida Europrivacy sull'uso di certificati, loghi e marchi di conformità;
h) Regole di comunicazione e marketing Europrivacy.

I documenti normativi sono integrati da una serie di documenti informativi, tra cui linee guida e modelli. Tutta la documentazione ufficiale e formale di Europrivacy viene mantenuta aggiornata e resa disponibile sul sito web di Europrivacy Community and Resources: https://community.europrivacy.com

3.1.2. Principali riferimenti normativi esterni

Ove applicabile, l'Organismo di Certificazione deve utilizzare i seguenti riferimenti normativi nell'applicazione dello Schema di Certificazione e del processo di certificazione:

- Regolamento europeo (UE) 2016/679 del Parlamento europeo e del Consiglio, noto anche come Regolamento generale sulla protezione dei dati (GDPR);
- Linee guida 4/2018 sull'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del Regolamento generale sulla protezione dei dati (2016/679);
- Linee guida 1/2018 sulla certificazione e sull'individuazione dei criteri di certificazione ai sensi degli articoli 42 e 43 del Regolamento (2016/679);
- Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti;
- ISO/IEC 17065, Valutazione della conformità - Requisiti per gli organismi che certificano prodotti, processi e servizi (e dove applicabile le sue integrazioni nazionali);
- ISO/IEC 17021-1, Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione dei sistemi di gestione;
- ISO/IEC 17030, Valutazione della conformità - Requisiti generali per i marchi di conformità di terzi;
- Le leggi nazionali complementari relative alla protezione dei dati applicabili al Target of Evaluation;
- Se richiesto dalla procedura di accreditamento nazionale, il Regolamento europeo (CE) 765/2008 del Parlamento europeo e del Consiglio che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

Ove incluso nel campo di applicazione della certificazione, può fare riferimento a norme complementari quali:

- Regolamenti nazionali;
- Direttive e regolamenti europei;
- Standard ISO, come ISO/IEC 27001 o 27701;
- Norme, standard e requisiti specifici del settore.

L'Organismo di Certificazione deve sempre considerare le versioni più recenti di queste norme al momento del processo di valutazione.

3.2. Regole e principi relativi ai documenti di riferimento

3.2.1. Versioni applicabili

Salvo diversa indicazione, tutti i riferimenti a un documento si intendono implicitamente riferiti alla sua ultima versione. Il rilascio di una nuova versione di un documento deve essere considerato come la sostituzione di tutte le versioni precedenti dello stesso documento alla data della sua pubblicazione, o alla fine del periodo di transizione se tale periodo è specificato.

I processi di certificazione e di audit devono utilizzare l'ultima versione disponibile dello Schema di Certificazione e dei relativi documenti alla data di inizio del processo di valutazione. Quando vengono rilasciate nuove versioni dei documenti durante un processo di valutazione, questo deve tenerne conto e, per quanto possibile, conformarsi alla nuova versione, ma è accettabile completare un processo di valutazione in corso secondo la versione ufficiale al momento in cui è iniziato.

3.2.2. Diffusione e controllo

I documenti normativi e informativi specifici dello Schema di Certificazione rimangono sotto il controllo dello Scheme Owner, assistito dal suo Comitato Internazionale di Esperti. Lo Scheme Owner rende disponibili i documenti rilevanti in formato elettronico agli Organismi di Certificazione autorizzati e a terzi.

I documenti di riferimento esterni sono gestiti in modo indipendente e devono essere consultati attraverso il sito web della fonte esterna corrispondente.

L'Organismo di Certificazione e i suoi Auditor hanno la responsabilità di verificare e garantire l'utilizzo della versione appropriata dei documenti.

3.2.3. Linguaggio di riferimento

Lo schema di certificazione è sviluppato e revisionato da esperti internazionali in materia di protezione dei dati. La sua lingua di riferimento è l'inglese. Tutti i documenti dello Schema possono essere tradotti in altre lingue. I documenti la cui traduzione è stata convalidata dallo Scheme Owner possono fungere da versioni ufficiali. Tuttavia, in tutti i casi di conflitto di interpretazione, farà fede la versione inglese.

4. Termini e definizioni

Nel presente Schema di Certificazione e in tutti i documenti ad esso relativi, vengono utilizzate le seguenti forme verbali:

Il termine "**deve**" indica un requisito;

"**dovrebbe**" indica una raccomandazione;

"**può**" indica l'autorizzazione;

"**potrebbe**" indica una possibilità o una capacità.

(Adottato da ISO/IEC 17065:2012)

4.1. Definizioni specifiche e uso contestuale di alcuni termini

Nel presente Schema di Certificazione, alcuni termini devono essere intesi come segue:

"Adattamento" si riferisce a regole e procedure complementari dello Schema di Certificazione specificate in un documento distinto per affrontare specifici Target of Evaluation.

Per "Richiedente" si intende il Cliente di un Organismo di Certificazione che richiede la certificazione o che partecipa a un processo di certificazione. Il Richiedente può essere inteso come ricompreso nella nozione di "Cliente" negli standard ISO. Il Richiedente sarà il Titolare o il Responsabile del trattamento dei dati personali del Target of Evaluation.

Per "Soggetto Controllato" si intende la parte o le parti dell'organizzazione del Richiedente che riceveranno il Team di audit.

Il "**Sistema di Gestione della Protezione dei Dati**" (DPMS) si riferisce alla parte del sistema di gestione complessivo, basato su un approccio al rischio d'impresa, utilizzato per stabilire, implementare, gestire, monitorare, rivedere, mantenere e migliorare la protezione dei dati in conformità alle normative applicabili in materia di protezione dei dati. Comprende il quadro delle risorse messe in atto da un Richiedente per proteggere i dati personali che tratta, tra cui *"struttura organizzativa, politiche, attività di pianificazione, responsabilità, pratiche, procedure, processi e risorse".* (Fonte: ISO/IEC 27000)

Le "**Normative sulla protezione dei dati**" al plurale e scritte in minuscolo si riferiscono sia alle norme europee che a quelle nazionali complementari applicabili.

Per "**Esame**" si intende la visita o la valutazione a distanza dei locali in cui viene effettuato o gestito il trattamento dei dati, al fine di verificare e determinare se i requisiti specificati nei Criteri sono soddisfatti. Può includere osservazioni visive e domande poste alle parti interessate coinvolte nell'elaborazione dei dati.

"**Estensione**" si riferisce a un insieme di criteri complementari specificati per valutare la conformità a normative complementari, come altre normative nazionali sulla protezione dei dati o altri regolamenti o direttive europee.

Il termine "**Ispezione**", utilizzato nel presente Schema di certificazione, si riferisce all'esame come sopra definito.

"**Ambito Normativo**" si riferisce agli obblighi legali e normativi rispetto ai quali vengono effettuate la valutazione e la certificazione.

Per "**Target of Evaluation**" si intende il trattamento dei dati da valutare e certificare in un determinato processo di certificazione. Il Target of Evaluation deve essere chiaramente specificato e la sua eventuale certificazione deve essere chiaramente comunicata e facilmente comprensibile per gli interessati.

"**Test**" e **"Prove"** si riferiscono all'esecuzione di un trattamento o di una procedura al fine di verificare e determinare se i requisiti specificati nei Criteri sono effettivamente soddisfatti . Per impostazione predefinita, i test vengono eseguiti in loco, ma, se del caso, possono essere eseguiti a distanza o in laboratorio.

4.2. Definizioni generali

Salvo diversa definizione, i termini utilizzati nello Schema di Certificazione devono essere intesi secondo le definizioni applicabili fornite dal GDPR, dalle linee guida dell'European Data Protection Board (EDPB) e da altre fonti normative pertinenti, come l'ISO. In caso di conflitto di interpretazione, le definizioni dell'EDPB prevarranno su qualsiasi altra definizione.

L'elenco seguente presenta i termini e le definizioni più rilevanti relativi a questo documento.

Accreditamento: *"Attestazione da parte di un organismo nazionale di accreditamento che un organismo di valutazione della conformità soddisfa i requisiti stabiliti dalle norme armonizzate e, se del caso, qualsiasi requisito aggiuntivo, compresi quelli stabiliti nei pertinenti schemi settoriali, per svolgere una specifica attività di valutazione della conformità."* (Fonte: Linee guida EDPB 4/2018)

Informazioni anonime: *"Informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.."* (Fonte: Considerando 26 del GDPR)

Certificato: *"Una dichiarazione di conformità".* (Fonte: Linee guida EDPB 1/2018)

Certificazione: *"La valutazione e l'attestazione imparziale da parte di terzi che il soddisfacimento dei criteri di certificazione è stato dimostrato."* (Fonte: Linee guida EDPB 4/2018)

Organismo di Certificazione: "*Un organismo terzo di valutazione della conformità che gestisce un meccanismo di certificazione.***"** (Fonte: Linee guida EDPB 4/2018)

Schema di certificazione: *"Un sistema di certificazione relativo a determinati prodotti, processi e servizi a cui si applicano gli stessi requisiti specificati, regole specifiche e procedure."* (Fonte: Linee guida EDPB 4/2018)

Verifiche e controlli: requisiti specifici rispetto ai quali viene valutato il Target of Evaluation.

Consenso: si riferisce a una *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."* (Fonte: GDPR, articolo 4). Il consenso richiede che "l*'interessato dia liberamente il proprio consenso al trattamento dei dati, dopo essere stato informato in modo sufficiente e chiaro sul modo in cui i suoi dati saranno utilizzati."* (Fonte: GDPR, articoli 13 e 14)

Criteri o Criteri di certificazione: *"I criteri rispetto ai quali viene effettuata una certificazione (valutazione di conformità)".* (Fonte: Linee guida EDPB 4/2018) Europrivacy integra i suoi criteri fondamentali formali con controlli e verifiche complementari.

Trattamento transfrontaliero "significa sia:

A) il trattamento dei dati personali che avviene nel contesto delle attività di stabilimenti in più di un paese del Titolare o del Responsabile del trattamento, qualora il Titolare o il Responsabile del trattamento sia stabilito in più di un paese; oppure
B) il trattamento di dati personali che avviene nel contesto delle attività di un unico stabilimento di un Titolare o di un Responsabile del trattamento nell'Unione, ma che incide o rischia di incidere sostanzialmente sugli interessati in più di uno Stato membro." (Fonte: GDPR, articolo 4)

Violazione dei dati: *"Una violazione della sicurezza che comporta la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati."* (Fonte: GDPR, articolo 34)

Titolare del trattamento: *"La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;"* (Fonte: GDPR, articolo 4)

Esportatore di dati: si riferisce al Titolare o al Responsabile del trattamento che trasferisce i dati a un altro Titolare o Responsabile del trattamento situato in un altro Paese che non è soggetto alla stessa normativa sulla protezione dei dati.

Importatore di dati: si riferisce al Titolare o al Responsabile del trattamento che riceve i dati da un altro Titolare o Responsabile del trattamento situato in un altro Paese che non è soggetto alla stessa normativa sulla protezione dei dati.

Minimizzazione dei dati: *"L'obbligo per il Titolare del trattamento di raccogliere solo i dati strettamente necessari per eseguire la funzionalità richiesta dall'interessato. In altre parole, i dati raccolti devono essere adeguati, pertinenti e non eccessivi rispetto alle finalità per cui sono trattati, al fine di evitare un trattamento dei dati non necessario e potenzialmente illegale.*" (Fonte: GDPR, articolo 5, paragrafo 1, lettera c)

Portabilità dei dati: Il diritto degli interessati di recuperare e trasferire i propri dati personali per altri usi o ad altri fornitori di servizi. È definito dal GDPR come *"il diritto dell'interessato di ricevere i dati personali che lo riguardano, forniti a un Titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico e, ove tecnicamente fattibile, il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui sono stati forniti i dati personali". Il diritto alla portabilità si applica solo se il trattamento è effettuato con mezzi automatizzati e si basa: a) sul consenso dell'interessato; b) o su un contratto di cui l'interessato è parte; c) o è necessario adottare misure su richiesta dell'interessato prima di stipulare un contratto*." (Fonte: GDPR, articolo 20)

Responsabile del trattamento: Ai sensi dell'articolo 2, lettera e), del regolamento (CE) n. 45/2001, per incaricato del trattamento si intende *"una persona fisica o giuridica, un'autorità pubblica, un'agenzia o qualsiasi altro organismo che tratta dati personali per conto del responsabile del trattamento".* L'elemento essenziale è quindi che il Responsabile del trattamento agisca solo "*per conto del Titolare del trattamento*" e sotto le istruzioni di quest'ultimo. Si noti che, ai sensi dell'art. 28 del GDPR, "il Responsabile del trattamento non può agire per conto del Titolare del trattamento". 28, *"il Responsabile del trattamento non può ingaggiare un altro Responsabile del trattamento senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. In caso di autorizzazione generale scritta, il Responsabile del trattamento dovrà informare il Titolare del trattamento di qualsiasi modifica prevista in merito all'aggiunta o alla sostituzione di altri Responsabili del trattamento, consentendo così al Titolare del trattamento di opporsi a tali modifiche."*

Trattamento dei dati: *"Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione."* (Fonte: GDPR, articolo 4, n. 2)

Autorità di Controllo (DPA): Un'autorità pubblica indipendente incaricata di monitorare l'applicazione del regolamento sulla protezione dei dati e la tutela dei diritti degli interessati. Nello SEE, le autorità per la protezione dei dati sono definite "Autorità di Controllo".

Responsabile della protezione dei dati (DPO): Un esperto in materia di privacy dei dati che lavora in modo indipendente per garantire che un'entità aderisca alle politiche e alle procedure stabilite dal GDPR (fonte: Glossario del EDPS). Il Responsabile della protezione dei dati è la persona incaricata di: informare e consigliare il Titolare (o il Responsabile del trattamento) sulle questioni relative alla protezione dei dati; monitorare la conformità al GDPR; sensibilizzare e formare il personale coinvolto nelle operazioni di trattamento dei dati; collaborare con l'Autorità di Controllo. (Fonte: articolo 39 del GDPR)

Conservazione dei dati: La conservazione dei dati si riferisce al fatto che i Titolari o i Responsabili del trattamento conservano i dati personali per determinati scopi.

Interessato: Qualsiasi *"persona fisica identificata o identificabile a cui si riferiscono i dati".* (Fonte: Articolo 4, n. 1, del GDPR)

Trasferimento dei dati: Il trasferimento di dati personali si riferisce alla trasmissione/comunicazione di dati a un destinatario in qualsiasi modo.

Trattamento ad alto rischio: Attività di trattamento dei dati personali la cui natura costituisce un rischio maggiore per i diritti e la libertà delle persone fisiche, trattando categorie particolari di dati personali o dati

relativi a condanne penali, o rivolgendosi specificamente a dati personali di minori di età, o che può comportare un rischio elevato per i diritti e la libertà delle persone fisiche.

Marchio di conformità (o sigillo): *"Un sigillo o un marchio può essere utilizzato per indicare il completamento della procedura di certificazione. Un sigillo o un marchio si riferisce comunemente a un logo o a un simbolo la cui presenza (oltre al certificato) indica che il Target of Evaluation della certificazione è stato valutato in modo indipendente nell'ambito di una procedura di certificazione ed è conforme ai requisiti specificati, indicati in documenti normativi come regolamenti, standard o specifiche tecniche."* (Fonte: Linee guida EDPB 1/2018)

Meccanismo: *"Un elemento software che esegue compiti di controllo e gestione"* (Fonte: ISO/IEC 12087-1)

Dato personale: *"Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."* (Fonte: GDPR, articolo 4)

Violazione dei dati personali: *"Una violazione della sicurezza che comporta la distruzione accidentale o illecita, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati."* (Fonte: GDPR, articolo 4)

Privacy: La privacy è la capacità di un individuo di essere lasciato solo, fuori dalla vista del pubblico, e di controllare le informazioni che lo riguardano. Il diritto alla privacy è sancito dalla Dichiarazione universale dei diritti dell'uomo (articolo 12), dalla Carta europea dei diritti fondamentali (articolo 7) e dalla Convenzione europea dei diritti dell'uomo (articolo 8). (Fonte: Glossario EDPS). Il concetto di privacy si sovrappone ma non coincide con quello di protezione dei dati personali. Il concetto di protezione dei dati ha una portata diversa, in quanto si riferisce a qualsiasi dato personale, compresi i dati personali resi disponibili al pubblico. La protezione dei dati personali si riferisce anche a un insieme di diritti degli interessati.

Rischio per la privacy: effetto dell'incertezza sulla privacy. Nel contesto del GDPR, i rischi per la privacy sono principalmente legati alla protezione dei dati personali e al loro potenziale impatto sui diritti e le libertà degli interessati.

Procedura: "*modo specifico per svolgere un'attività o un processo*" (Fonte: ISO 30000)

Pseudonimizzazione: *"Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato, senza l'uso di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile."* (Fonte: GDPR, articolo 4) La pseudonimizzazione può servire nella minimizzazione dei dati, ad esempio per garantire che, durante il trattamento dei dati personali, l'identità degli interessati sia limitata e accessibile solo a coloro che ne hanno una necessità legittima.

Finalità: s**i** riferisce allo scopo per cui vengono trattati i dati personali.

Destinatario: *"Una persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento."* (Fonte: GDPR, articolo 4)

Periodo di conservazione: *"Periodo di tempo durante il quale i dati personali sono conservati dal Titolare o dal Responsabile del trattamento". Secondo il principio della "limitazione della conservazione", i dati personali possono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario per le finalità per le quali i dati personali sono trattati. I dati personali possono essere conservati per periodi più lunghi nella misura in cui saranno trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ai sensi dell'articolo 89, paragrafo 1, fatta salva l'attuazione delle misure tecniche e organizzative adeguate richieste dal presente regolamento per salvaguardare i diritti e le libertà dell'interessato."* (Fonte: GDPR, articolo 5)

Scheme Owner: *"Un'organizzazione identificabile che ha stabilito i criteri e i requisiti di certificazione rispetto ai quali deve essere valutata la conformità."* (Fonte: Linee guida EDPB 4/2018)

Categorie Particolari di Dati: *"Le Categorie Particolari di Dati sono dati personali particolarmente sensibili e che richiedono un livello di protezione più elevato". Comprendono qualsiasi dato che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, compresi i dati genetici, i dati biometrici al fine di identificare in modo univoco una persona fisica, i dati relativi alla salute o i dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica*." (Fonte: GDPR, articolo 9)

5. Principi generali e linee guida per la certificazione

5.1. Scopo della certificazione

Lo Schema di Certificazione **mira a fornire a tutte le parti la certezza** che un Target of Evaluation Certificato sia conforme ai requisiti dello Schema di Certificazione e, più in generale, al GDPR e alle normative nazionali complementari applicabili in materia di protezione dei dati. Di conseguenza, l'Organismo di Certificazione mira a mantenere la fiducia nei propri processi attraverso forti principi di imparzialità, competenza (comprese le competenze in materia di protezione dei dati), responsabilità, apertura, riservatezza, reattività ai reclami e ai ricorsi, nonché un approccio basato sul rischio.

5.2. Valori fondamentali e principi chiave

5.2.1. Creare fiducia e sicurezza

Gli Auditor devono sempre tenere presente che Europrivacy è stato concepito per creare fiducia e sicurezza che l'Target of Evaluation sia conforme ai requisiti applicabili.

5.2.2. Integrità

Gli Auditor e il personale dell'Organismo di Certificazione coinvolti in un processo di certificazione devono svolgere il proprio lavoro con onestà, diligenza e responsabilità. Devono applicare i requisiti dello Schema di Certificazione con professionalità e imparzialità.

5.2.3. Indipendenza

Gli Auditors devono essere indipendenti dall'attività oggetto di revisione ogniqualvolta sia possibile e devono in ogni caso agire in modo libero da pregiudizi e conflitti di interesse.

5.2.4. Imparzialità

Gli Organismi di Certificazione devono garantire l'imparzialità nei loro processi di certificazione e rimanere equi e imparziali in tutti i loro rapporti. Le decisioni di un Organismo di Certificazione devono basarsi su prove oggettive di conformità (o di non conformità) e devono garantire che le sue decisioni non siano influenzate da altri interessi o da altre parti. (Maggiori dettagli nella Sezione 13)

5.2.5. Approccio basato sull'evidenza

I risultati e le conclusioni dell'audit devono basarsi sulle evidenze pertinenti ai criteri di audit. Le prove devono essere registrate e verificabili.

5.2.6. Presentazione veritiera

I risultati, le conclusioni e i rapporti dell'audit devono riflettere in modo veritiero e accurato le attività di audit. La loro comunicazione deve essere veritiera, accurata, obiettiva, tempestiva, chiara e completa.

5.2.7. Riservatezza

L'Organismo di Certificazione e lo Scheme Owner devono adottare procedure e attuare una politica efficace per proteggere la riservatezza delle informazioni acquisite in relazione al processo di certificazione. Gli Auditor e tutto il personale dell'Organismo di Certificazione dovranno tutelare la riservatezza delle informazioni raccolte.

Tutti i documenti o le informazioni condivisi dall'Organismo di Certificazione e/o dallo Scheme Owner con il Richiedente devono essere protetti e gestiti come riservati da quest'ultimo, a meno che tali documenti o informazioni non siano esplicitamente destinati a essere resi pubblici. (Maggiori dettagli nella Sezione 15)

5.2.8. Apertura

L'Organismo di Certificazione deve rispettare il principio ISO di apertura fornendo un adeguato accesso pubblico a informazioni chiare sui propri processi e procedure di certificazione.

Tuttavia, si impegnerà sempre a preservare e proteggere le informazioni riservate, come le informazioni relative al Richiedente e i documenti condivisi come informazioni riservate.

5.2.9. Condizioni di non discriminazione

Le politiche e le procedure dell'Organismo di Certificazione devono essere non discriminatorie. L'Organismo di Certificazione deve rendere i propri servizi accessibili a tutti i Richiedenti le cui attività rientrano nell'ambito delle sue operazioni e per le quali dispone delle risorse necessarie e adeguate.

La decisione di accettare o rifiutare un Richiedente si baserà sulle disposizioni dello Schema di Certificazione. L'Organismo di Certificazione può rifiutare di accettare una domanda o di mantenere un contratto di certificazione da parte di un Richiedente quando esistono ragioni obiettive e proporzionate. Esempi di motivi ragionevoli che un Organismo di Certificazione può prendere in considerazione per tale decisione sono:

- Richiedente che partecipa ad attività illegali;
- Richiedente con una storia di ripetute non conformità con lo Schema di Certificazione e/o con le normative sulla protezione dei dati;
- Il Richiedente si affida pesantemente a Responsabili del trattamento dei dati che non possono essere controllati e/o che si trovano in paesi con normative o politiche di protezione dei dati personali troppo deboli;
- Il Richiedente è impegnato in controversie legali relative alla protezione dei dati;
- Richiedente che costituisce un rischio di discredito per lo Schema di Certificazione;
- Richiedente la cui conformità sarebbe troppo complessa o difficile da valutare e certificare;
- La mancanza o l'assenza di risorse necessarie o di disponibilità da parte dell'Organismo di Certificazione per fornire una valutazione affidabile del Target of Evaluation.

5.2.10. Indirizzare le tecnologie emergenti

Europrivacy è stato progettato per includere i rischi legati alle tecnologie emergenti e per sfruttare le tecnologie più avanzate a supporto dei processi di certificazione.

5.2.11. Miglioramento continuo

Lo schema di certificazione Europrivacy è stato progettato per applicare e beneficiare di una metodologia di miglioramento continuo.

5.2.12. Salvaguardia dei valori fondamentali e dei principi chiave

In caso di sospetto fondato di influenza indebita, che potrebbe mettere a repentaglio il mantenimento dei principi sopra citati, è necessario informare il Comitato Esecutivo dell'Organismo di Certificazione. Se la questione non viene risolta dall'Organismo di Certificazione, lo Scheme Owner deve essere informato con le relative prove dell'influenza indebita.

6. Criteri di valutazione

I criteri di valutazione devono essere applicati in conformità all'ultima versione dei requisiti dello Schema di Certificazione Europrivacy. Essi devono essere applicati dall'Organismo di Certificazione:

a) **tenendo conto dei diritti degli interessati e dei rischi potenziali per i loro dati personali**;
b) **in modo coerente e omogeneo**;
c) **in modo verificabile e controllabile**;
d) **tenendo in considerazione:**
   - le dimensioni dell'organizzazione;
   - la natura dell'attività di trattamento dei dati;
   - i rischi identificati per i dati e gli interessati.

6.1. Sintesi dei principali criteri di valutazione

L'Organismo di Certificazione deve rispettare e applicare i criteri applicabili indicati negli articoli 42 e 43 del GDPR.

I criteri di valutazione, le verifiche e i controlli dettagliati di Europrivacy mirano a valutare i seguenti aspetti del Target of Evaluation:

a) l'identificazione dei dati personali trattati, compresa l'identificazione di eventuali categorie speciali di dati, se applicabile;
b) il rispetto dei requisiti per le informazioni sul trattamento dei dati fornite agli interessati, tra cui:
   - facilità di accesso e comprensibilità;
   - scopo chiaro per la raccolta dei dati personali;
   - informativa sulla privacy del Titolare del trattamento;
   - i diritti degli interessati, compresi i diritti di accesso, rettifica o cancellazione dei dati personali, di opposizione al trattamento dei dati, di richiesta di limitazione di tale trattamento, di revoca del consenso e di portabilità dei dati;
   - informazioni sul Titolare del trattamento e, se del caso, sui Responsabili del trattamento;
c) la liceità del trattamento e, se del caso, la conformità ai requisiti del "consenso preventivo informato", compresa una chiara indicazione delle finalità della raccolta dei dati, o in alternativa l'esistenza di altre basi giuridiche per il trattamento dei dati personali (come un mandato legale conferito a una pubblica amministrazione);
d) il rispetto dei requisiti relativi ai minori di età;
e) il rispetto del principio di minimizzazione dei dati personali fin dalla progettazione e per impostazione predefinita;
f) il rispetto del principio di trasparenza previsto dal GDPR, che richiede che qualsiasi informazione e comunicazione relativa al trattamento dei dati personali sia facilmente accessibile e comprensibile e che venga utilizzato un linguaggio chiaro e semplice.
g) l'analisi del flusso dei dati personali, comprese le questioni relative al Responsabile del trattamento e al trasferimento transfrontaliero dei dati, assicurando che:
   - i dati personali siano adeguatamente protetti quando vengono trasferiti in un paese terzo (ad esempio, sulla base di decisioni di adeguatezza, garanzie appropriate, ecc.);
   - i Titolari o i Responsabili del trattamento non stabiliti nell'UE forniscano garanzie adeguate per ricevere dati personali da organizzazioni con sede nell'UE;
h) il ciclo di vita dei dati personali e la minimizzazione dei periodi di conservazione dei dati personali;
i) l'effettiva attuazione dei diritti degli interessati, tra cui:
   - il diritto di accesso, rettifica o cancellazione dei dati personali;
   - il diritto di opporsi al trattamento dei dati o di chiederne la limitazione;
   - il diritto degli utenti di revocare il proprio consenso;
   - il diritto alla portabilità dei dati;
j) la presenza e la conformità della raccolta indiretta di dati, come i cookie e/o la profilazione automatizzata;
k) l'attuazione di misure idonee a salvaguardare i diritti e le libertà degli interessati e i loro legittimi interessi nel contesto del processo decisionale individuale automatizzato;

l) la sicurezza e l'effettiva protezione e integrità dei dati raccolti, come ad esempio:
- l'uso di soluzioni di backup;
- l'uso di soluzioni di firewalling e antivirus;
- utilizzo di meccanismi di controllo dell'accesso ai dati (fisici o remoti) definiti in base a ruoli e responsabilità;
- l'uso di protocolli di crittografia affidabili;
- l'uso di meccanismi di autenticazione affidabili;
- l'utilizzo di un approccio alla protezione dei dati da parte della progettazione;

m) l'attuazione da parte del Titolare di misure tecniche e organizzative adeguate per la protezione dei dati, tra cui:
- ruoli e responsabilità chiare;
- designazione di un responsabile della protezione dei dati (DPO) con:
  - qualificazione adeguata;
  - autonomia d'azione e accesso alla direzione;
  - efficacia dell'azione (dimostrazione della sua attività e azione);
  - coinvolgimento in tutte le questioni relative alla protezione dei dati personali;
- che qualsiasi persona fisica che agisca sotto la sua autorità non tratti i dati se non su istruzione del Titolare;
- procedura per registrare tutte le violazioni dei dati in un registro interno e per informare gli organi di controllo senza ritardi ingiustificati/entro 72 ore dal momento in cui si viene a conoscenza di una violazione dei dati personali (a meno che non sia improbabile che si verifichi un rischio per l'interessato);
- procedura di comunicazione della violazione dei dati personali agli interessati senza indebito ritardo, qualora la violazione possa comportare un rischio elevato per i diritti/le libertà delle persone fisiche;
- ove applicabile, come nel caso di trattamenti di dati potenzialmente rischiosi, la valutazione d'impatto sulla protezione dei dati (DPIA) effettuata con il DPO e la consultazione delle autorità di controllo prima del trattamento dei dati se la DPIA ha indicato un rischio elevato;
- che i Responsabili del trattamento (e, se del caso, i loro rappresentanti) conservino registri delle attività di trattamento;

n) per i Titolari del trattamento non stabiliti nell'UE, l'obbligo di designare per iscritto un rappresentante stabilito in uno degli Stati membri dell'UE;
- in caso di utilizzo di Responsabili del trattamento, le procedure e gli accordi in essere che consentono al Titolare del trattamento di assicurarsi che i Responsabili del trattamento forniscano garanzie sufficienti per attuare misure tecniche e organizzative adeguate, tra cui:
- l'esistenza di un contratto scritto e di obblighi contrattuali con tutti i Responsabili del trattamento, che copra gli obblighi del Responsabile del trattamento;
- che il Responsabile del trattamento metta in atto misure tecniche e organizzative adeguate per garantire un'appropriata sicurezza del trattamento;
- che il Responsabile del trattamento non potrà collaborare con un altro Responsabile del trattamento senza la preventiva autorizzazione scritta del Titolare del trattamento;
- che il Responsabile del trattamento non tratterà i dati personali se non su istruzione del Titolare del trattamento;
- che il Responsabile del trattamento (e i suoi rappresentanti) collaborino con le autorità di vigilanza;
- che il Responsabile del trattamento si assicuri che qualsiasi persona fisica che agisca sotto la sua autorità non tratti i dati se non dietro istruzioni del Titolare;
- che il Responsabile del trattamento informi il Titolare del trattamento senza indebito ritardo dopo essere venuto a conoscenza di una violazione dei dati personali;
- che il Responsabile del trattamento si atterrà alle condizioni stabilite nel Capo V del GDPR per garantire che i dati personali siano adeguatamente protetti quando vengono trasferiti in un paese terzo;
- che il Responsabile del trattamento sarà responsabile dei danni causati da un trattamento non conforme qualora non abbia rispettato gli obblighi del GDPR specificamente rivolti ai

Responsabili del trattamento (vedi sopra) o abbia agito al di fuori o in contrasto con le istruzioni legittime del Titolare;

o) Se inclusi nell'ambito normativo **concordato, requisiti e criteri normativi complementari nazionali e/o specifici del settore**.

6.2. Elenco dettagliato di criteri, controlli e verifiche

I suddetti criteri sono tradotti in elenchi dettagliati di criteri, verifiche e controlli mantenuti dallo Scheme Owner e resi disponibili alle Autorità di Vigilanza e alle terze parti autorizzate.

L'elenco dei criteri, delle verifiche e dei controlli sarà utilizzato dagli Organismi di Certificazione per valutare sistematicamente la conformità del trattamento dei dati nel Target of Evaluation.

Ogni criterio, verifica e controllo applicabile deve essere sufficientemente completato e documentato con prove adeguate per valutare la conformità al requisito.

Criteri, Controlli e Applicabilità delle Verifiche

I criteri, le verifiche e i controlli di Europrivacy sono differenziati individualmente e collegati a categorie distinte per determinare e facilitare la loro applicabilità.

Una colonna indica se i criteri, le verifiche e i controlli sono applicabili a:

- **C** Titolari del trattamento
- **P** Responsabili del trattamento
- **CP** Titolari e Responsabili del trattamento

Al fine di affrontare la proporzionalità e di differenziare i trattamenti di dati ad alto rischio da quelli regolari, un'altra colonna differenzia i criteri, le verifiche e i controlli nelle seguenti categorie:

- **A** **Obbligatorio per impostazione predefinita per tutti i processi di certificazione**.
- **B** Non è richiesto per la certificazione di semplici trattamenti, **ma è obbligatorio per la certificazione di qualsiasi trattamento ad alto rischio, definita come trattamento che:**
  - tratta **categorie particolari di dati personali** o dati relativi a condanne penali, oppure;
  - **si rivolge** specificamente **ai dati personali di minori di età**, oppure;
  - è suscettibile di comportare un **rischio elevato per i diritti e la libertà delle persone fisiche**[6].
- **E** **Esenzioni**: per determinare se una deroga a un criterio può essere giustificata.

Un'altra colonna specifica se i criteri, le verifiche e i controlli sono:

- **S** **Specifico** per ogni trattamento di dati (cioè la liceità di un trattamento di dati);
- **G** **Generico** e comune a diversi trattamenti di dati (ad esempio, qualificazione adeguata del DPO).

Inoltre, nei Criteri fondamentali, un'altra colonna specifica se il criterio è richiesto per certificare gli Importatori di dati con sede al di fuori dello Spazio Economico Europeo (SEE) che non sono direttamente soggetti al GDPR ma che intendono utilizzare la certificazione come meccanismo per il trasferimento internazionale dei dati[7], dove:

- **R** indica che il criterio **è richiesto** per gli importatori di dati con sede al di fuori dello SEE;
- **NR** indica che il criterio **non è richiesto** per gli importatori di dati con sede al di fuori dello SEE.

I criteri, le verifiche e i controlli possono essere soggetti a **clausole di condizionalità** che iniziano con il termine "**SE**" e terminano con il termine "**ALLORA:**". Se la condizione non è soddisfatta, i requisiti associati non sono applicabili e possono essere saltati.

Ogni controllo e verifica può contenere e combinare più requisiti, che sono collegati tra loro con le parole "E" e "O" per chiarire la loro relazione. L'uso di "E" tra due o più condizioni richiede che tutte le condizioni siano soddisfatte; l'uso di "O" richiede che almeno una delle condizioni sia soddisfatta.

[6] L'Organismo di certificazione terrà conto delle relative linee guida dell'EDPB in materia.
[7] I Richiedenti non appartenenti allo SEE sono soggetti al GDPR quando raccolgono direttamente i dati personali nello SEE (art. 3 GDPR).

6.2.1. Criteri fondamentali e verifiche e controlli complementari

Europrivacy è stato progettato per fornire un processo di certificazione omogeneo e coerente applicabile a diverse categorie di attività di trattamento. Oltre agli obblighi fondamentali del GDPR, i Target of Evaluation possono essere soggetti a normative nazionali complementari o specifiche del settore. Di conseguenza, i criteri fondamentali di Europrivacy sono integrati da requisiti contestuali per tenere conto delle normative nazionali applicabili al Richiedente e delle specificità del trattamento.

Criteri fondamentali di Europrivacy

L'elenco dei criteri fondamentali di Europrivacy costituisce la spina dorsale di tutti i processi di certificazione e deve essere applicato dagli auditor dell'Organismo di Certificazione a ogni singolo Target of Evaluation.

Requisiti complementari

Europrivacy tiene conto di tre serie di requisiti complementari relativi a:

- **Normativa nazionale**: valutata attraverso il National Obligations Compliance Assessment Report (NOCAR) e/o criteri nazionali complementari Estensioni;
- **Requisiti di sicurezza**: valutati attraverso le verifiche e i controlli delle misure tecniche e organizzative (TOM) o attraverso la norma ISO/IEC 27001;
- **Requisiti specifici della tecnologia e del dominio**: valutati attraverso le Verifiche e i Controlli Contestuali Complementari.

L'applicabilità di questi requisiti complementari è determinata da fattori oggettivi, quali: l'ubicazione del Richiedente per i requisiti nazionali e la natura del trattamento nel Target of Evaluation per i requisiti tecnologici e specifici del dominio.

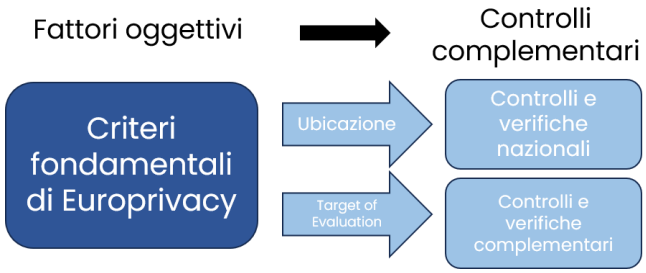

Figura 2 Verifiche e controlli complementari determinati da fattori oggettivi

Relazione tra i requisiti fondamentali e quelli complementari

I criteri fondamentali di Europrivacy richiedono di valutare la conformità del Target of Evaluation con i requisiti complementari applicabili.

La figura seguente illustra la base normativa dello Schema di Certificazione e la complementarità tra i Criteri Fondamentali di Europrivacy e i requisiti complementari.

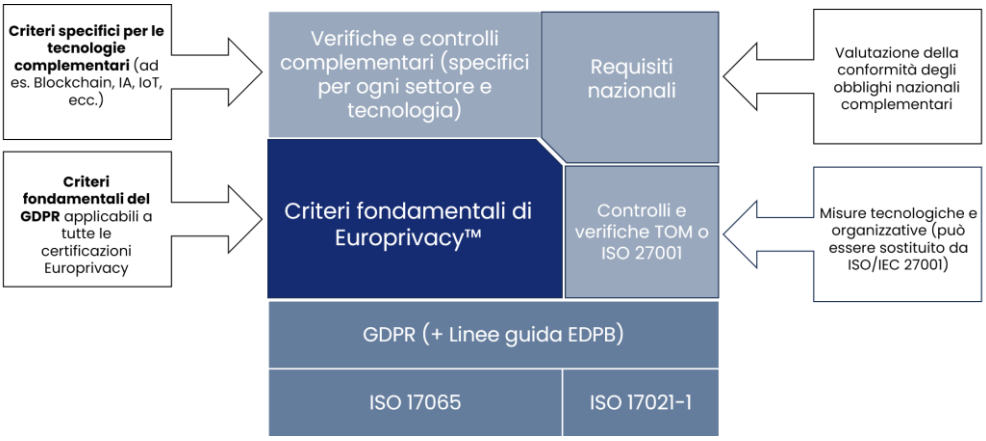

Figura 3 Criteri fondamentali di Europrivacy e controlli e verifiche complementari

6.2.2. Requisiti nazionali e normativi complementari

Il Richiedente che presenta la domanda dallo Spazio Economico Europeo (SEE) deve richiedere a un esperto con adeguate competenze legali di **valutare la conformità del suo Target of Evaluation con gli obblighi nazionali complementari del Paese di applicazione** che superano gli obblighi regolari previsti dal GDPR. I risultati della valutazione dovranno essere riportati in una relazione scritta: il ***National Obligations Compliance Assessment Report*** **(NOCAR)**. In assenza di un NOCAR, l'Organismo di Certificazione può in alternativa eseguire una valutazione di conformità del Target of Evaluation all'obbligo nazionale applicabile nel Paese di applicazione, soggetta allo stesso livello di requisiti del NOCAR. Lo Scheme Owner mette a disposizione risorse online, tra cui elenchi di requisiti nazionali complementari identificati. Questi elenchi di requisiti nazionali devono essere presi in considerazione dall'esperto quando esegue la valutazione.

La Certificazione Europrivacy può essere estesa per indirizzare normative complementari sulla protezione dei dati non appartenenti all'UE, così come normative complementari dell'UE. In tal caso, i requisiti e i criteri complementari possono essere specificati e forniti attraverso apposite "estensioni" dello Schema di Certificazione Europrivacy (cfr. sezione 11.1).

6.2.3. Requisiti delle misure tecniche e organizzative complementari

La certificazione Europrivacy richiede l'adozione di adeguate misure tecniche e organizzative per proteggere i dati trattati e conservati.

Per valutare l'adeguatezza della sicurezza del trattamento dei dati sono stati specificati i Controlli e le Misure Tecniche e Organizzative Complementari. Tali verifiche e controlli integrano i Criteri Fondamentali e sono obbligatori, ad eccezione del caso in cui il Target of Evaluation sia il seguente:

a) è coperto da una certificazione ISO/IEC 27001 valida; e
b) non esegue alcun trattamento di dati ad alto rischio.

6.2.4. Requisiti complementari contestuali e specifici del dominio

Le Verifiche e i Controlli Contestuali Complementari contengono vari sottoinsiemi di controlli e verifiche corrispondenti a tecnologie o domini applicativi specifici. L'Organismo di Certificazione deve applicare e valutare tutti i sottoinsiemi di verifiche e controlli applicabili alle attività di trattamento incluse nel Target of Evaluation.

6.2.5. Sviluppo di controlli e verifiche complementari

Lo Scheme Owner fornisce elenchi complementari di verifiche e controlli, nonché un meccanismo per integrare le verifiche e i controlli predefiniti con altri complementari.

Ogni verifica e controllo deve essere:

- **Adeguato** per valutare la conformità al corrispondente requisito legale;
- **Auditabile**, garantendo che il requisito possa essere efficacemente valutato e dimostrato;
- **Obiettivo e fattuale**, concentrandosi su fatti e prove verificabili per ridurre al minimo la soggettività della valutazione;
- **Formulazione chiara** per evitare qualsiasi ambiguità o margine di interpretazione;
- **Applicabile in modo omogeneo**, cercando di renderlo applicabile con la stessa rilevanza alle diverse attività di trattamento dei dati e ai diversi responsabili del trattamento;
- **Efficiente** per fornire una valutazione affidabile della conformità, senza inutili carichi di lavoro;
- **Neutrale** (come definito da ISO), garantendo che possa essere utilizzato dal Richiedente stesso, dall'Organismo di Certificazione, così come da una seconda o terza parte.

Processo e requisiti per la specificazione di nuovi controlli e verifiche

Al fine di sviluppare verifiche e controlli complementari, l'Organismo di Certificazione deve:

1. Verificare innanzitutto, nell'archivio documentale dello Scheme Owner, se sono disponibili adeguati elenchi complementari di verifiche e controlli per valutare questi requisiti;
2. Se questi requisiti normativi complementari non sono adeguatamente coperti dalle verifiche e dai controlli esistenti, l'Organismo di Certificazione può (A) escludere il requisito complementare

dall'Ambito Normativo, oppure (B) analizzare questa/e norma/e aggiuntiva/e per identificare ed estrarre i requisiti complementari;

3. In caso di B, dovrà compilare il modello messo a disposizione dallo Scheme Owner per elencare i requisiti pertinenti e specificare le verifiche e i controlli corrispondenti;
4. Invia il nuovo elenco di verifiche e controlli complementari allo Scheme Owner;
5. Quando esegue la valutazione, applica l'elenco delle verifiche e dei controlli al Target of Evaluation;
6. La società deve riportare il risultato della valutazione complementare nella sezione corrispondente della valutazione di conformità globale.

Il modello può essere utilizzato anche dalle autorità europee o nazionali per la protezione dei dati per comunicare allo Scheme Owner i requisiti complementari e le verifiche e i controlli.

Lo Scheme Owner si occupa di raccogliere, rivedere e condividere queste verifiche e controlli aggiuntivi con altri organismi di certificazione, al fine di garantire la coerenza.

6.2.6. Elenchi di criteri, controlli e verifiche

I criteri, le verifiche e i controlli obbligatori sono:

- *"A - Application and Target of Evaluation – Preliminary Checks and Controls "*, per convalidare l'adeguatezza della domanda e del suo Target of Evaluation;
- *"G - GDPR Core Criteria"*, per valutare la conformità ai requisiti fondamentali di protezione dei dati;
- *"C - Complementary Contextual Checks and Controls "*, per valutare la conformità ai requisiti complementari specifici del dominio e della tecnologia;
- *" Technical and Organisational Measures Checks and Controls "*, per valutare le misure in atto per la sicurezza dei dati trattati (può essere sostituita da una certificazione ISO/IEC 27001 se il Target of Evaluation non include trattamenti di dati ad alto rischio);
- *"S - Complementary Surveillance Checks and Controls "*, da utilizzare negli audit di sorveglianza e nelle ricertificazioni.

Quando una verifica e un controllo sono pertinenti e applicabili al Target of Evaluation, devono essere applicati. L'esclusione di controlli e verifiche deve essere giustificata.

L'Allegato 1 fornisce una visione sintetica dei criteri applicabili in base all'ubicazione e all'attività del Richiedente per il rilascio di una certificazione ai sensi degli Art. 42 e 43 del GDPR.

Se del caso, l'Organismo di Certificazione può prendere in considerazione verifiche e controlli complementari, purché consentano di valutare meglio la conformità del Target of Evaluation alle normative applicabili in materia di protezione dei dati.

Europrivacy è supportato da documenti informativi e liste di controllo complementari per facilitare e migliorare il processo di certificazione, tra cui:

- *"D - Documentation checklist for Europrivacy certification "*, per facilitare la preparazione e la revisione della documentazione;
- Profili *"N - National Data Protection Obligations "* che elencano i principali requisiti complementari di protezione dei dati per paese, a supporto della preparazione del National Obligations Compliance Assessment Report (NOCAR);
- Liste di controllo complementari, come la *"P - Policy Checklist"* per verificare la completezza delle politiche e delle procedure in vigore;
- Modelli (ad esempio, dichiarazione del DPO, NOCAR, inventari dei dati trattati, dei responsabili del trattamento, dei luoghi di conservazione dei dati, ecc.).

7. Processo di riferimento per la certificazione del trattamento dei dati

La certificazione Europrivacy è volontaria e il ruolo dell'Organismo di Certificazione è quello di verificare, attraverso il processo di certificazione, se il trattamento dei dati da certificare soddisfa i requisiti di certificazione.

Prima di richiedere la certificazione, il Richiedente deve lavorare sulle proprie attività di trattamento dei dati rendendole conformi alle normative sulla protezione dei dati applicabili. Il Richiedente è incoraggiato a documentare la conformità del proprio trattamento dei dati con la normativa sulla protezione dei dati, nonché con i criteri e i requisiti di Europrivacy prima del processo. L'uso di strumenti di autovalutazione e di società di consulenza qualificate può contribuire ad accelerare il processo di certificazione. L'ECCP mette a disposizione dei Richiedenti, degli studi legali e delle società di consulenza una serie di risorse per preparare le certificazioni Europrivacy.

Il processo di riferimento per la certificazione dell'elaborazione dei dati si basa sul modello e sui requisiti della ISO/IEC 17065. Il processo di valutazione è incentrato sul Target of Evaluation.

La certificazione può essere concessa per un periodo massimo di 3 anni. La ricertificazione può essere concessa in base all'esito delle attività di monitoraggio.

Il processo di riferimento per la certificazione del trattamento dei dati prevede le seguenti fasi:

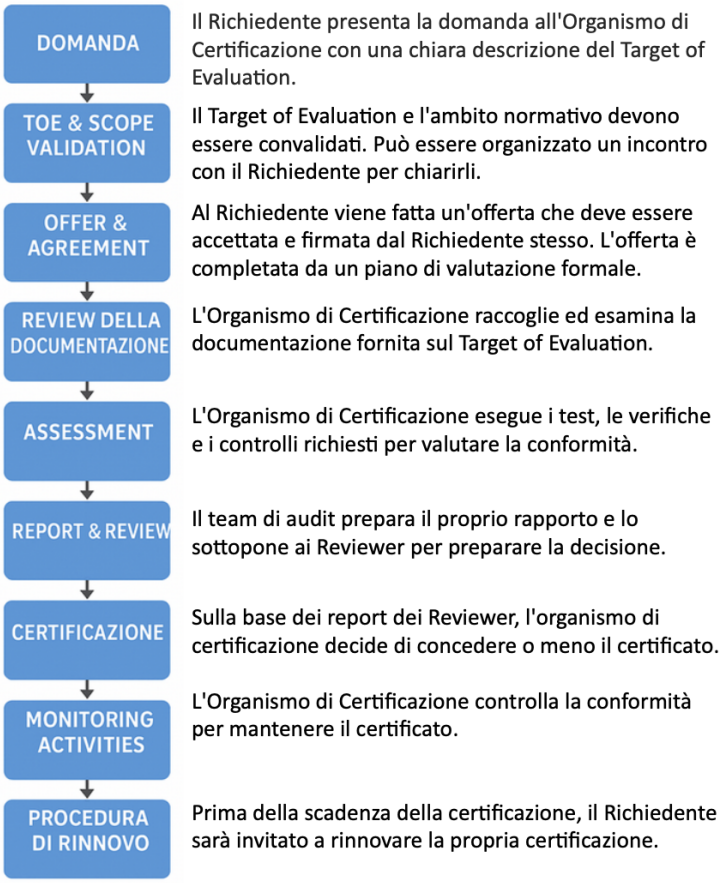

Figura 4 Processo di certificazione di riferimento

7.1. Modello di processo adattabile

7.1.1. Panoramica del modello di processo adattabile

Sebbene l'obiettivo principale dello Schema di Certificazione Europrivacy sia la valutazione del trattamento dei dati personali, esso è stato concepito per essere il più completo possibile. È adattabile a diversi ambiti, come i sistemi di gestione della protezione dei dati, che sono soggetti a requisiti aggiuntivi e a procedure di accreditamento specificate in appositi adattamenti (cfr. sezione 11).

Sebbene lo Schema di Certificazione possa essere applicato a un'ampia varietà di attività di trattamento dei dati, la sua applicazione per le certificazioni ai sensi degli articoli 42 e 43 del GDPR deve essere rigorosamente conforme alla politica, alle direttive e alle restrizioni stabilite dal Comitato europeo per la protezione dei dati.

7.1.2. Applicazioni combinate

Lo Schema di Certificazione Europrivacy può essere esteso per includere obblighi complementari in materia di protezione dei dati specificati nelle estensioni (vedere la sezione 11). In questi casi, il processo di certificazione deve essere considerato come un unico processo di certificazione piuttosto che una certificazione doppia o combinata.

7.1.3. Richiedenti e applicabilità

Il processo di certificazione è aperto a soggetti pubblici e privati che agiscono in qualità di Titolari o Responsabili del trattamento. Ai sensi degli articoli 42 e 43 del GDPR, la certificazione è applicabile solo alle operazioni di trattamento dei dati personali da parte di Titolari e Responsabili del trattamento e può essere soggetta a restrizioni stabilite dal Comitato europeo per la protezione dei dati.

7.2. Attività di pre-certificazione

7.2.1. Application Process

Il processo di richiesta deve raccogliere le informazioni necessarie per determinare il Target of Evaluation della certificazione e deve essere adeguatamente documentato.

Il Richiedente deve essere il Titolare o il Responsabile del trattamento dei dati che rientrano nel Target of Evaluation della certificazione.

In linea di principio, il Richiedente deve compilare e presentare un modulo di domanda firmato dal suo o dai suoi legali rappresentanti. In alternativa, la richiesta può essere effettuata mediante un incontro diretto tra un legale rappresentante del Richiedente e l'Organismo di Certificazione.

Il processo di richiesta deve raccogliere e documentare informazioni su:

a) il Richiedente, compresa la sua denominazione legale, l'indirizzo, il sito web e il dominio di attività;
b) la descrizione delle attività di trattamento dei dati;
c) il campo di applicazione normativo e il Target of Evaluation della certificazione;
d) se del caso, informazioni sulle normative complementari nazionali o specifiche di settore in materia di protezione dei dati applicabili al Target of Evaluation;
e) la/e persona/e di contatto autorizzata/e;
f) se è stata fornita una consulenza per il Target of Evaluation e, in caso affermativo, da chi.

Inoltre, come richiesto dalle linee guida EDPB, il Target of Evaluation deve essere descritto in dettaglio nella fase di candidatura con:

- **Interfacce e trasferimenti ad altri sistemi e organizzazioni;**
- **Protocolli utilizzati e altre garanzie pertinenti;**
- **Identificazione di tutti i Responsabili del trattamento dei dati coinvolti con i relativi compiti e responsabilità.**

Una volta che l'Organismo di Certificazione e i Richiedenti sono coperti da adeguate clausole contrattuali di riservatezza, l'Application deve essere completata con copie delle clausole contrattuali pertinenti tra il Richiedente e i suoi Responsabili del trattamento.

Oltre alle informazioni fornite dal Richiedente, l'Organismo di Certificazione può raccogliere informazioni complementari da aggiungere alla Domanda con indicazioni documentate della fonte.

7.2.2. Impegno preliminare del Richiedente

Firmando il modulo di richiesta, il Richiedente si impegna a rispettare i Termini e le Condizioni Generali di Europrivacy allegati allo Schema di Certificazione. Si impegna inoltre a rispettare e facilitare il processo di certificazione fornendo le informazioni richieste, il supporto e l'accesso necessario agli Auditor.

7.2.3. Chiarire e specificare il Target of Evaluation

Il Target of Evaluation deve essere specificato e controllato con cura. Il Richiedente e l'Organismo di certificazione devono:

a) specificare il Target of Evaluation:
   a. nominarlo con un titolo chiaro;
   b. descrive il trattamento;
   c. illustrare i flussi di dati personali in un diagramma o in un disegno, compresa l'identificazione dei flussi di dati personali con i trattamenti esterni;
   d. identificare le categorie di dati trattati nell'ambito del Target of Evaluation;
   e. identificare e descrivere tutte le operazioni e i sistemi di trattamento relativi al Target of Evaluation;
   f. indicare quando inizia e termina il trattamento;
   g. se del caso, identificare e descrivere le interfacce dell'elaborazione dei dati nel Target of Evaluation con un trattamento indipendente;
   h. specificare i protocolli utilizzati e altre misure di garanzia pertinenti;
b) giustificare l'esclusione del trattamento dei dati interdipendenti dal Target of Evaluation;
c) elencare tutti i Responsabili del trattamento dei dati coinvolti nel Target of Evaluation, con una descrizione dei loro compiti, delle loro responsabilità e delle relative clausole contrattuali;
d) se applicabile, identificare:
   a. qualsiasi contitolare;
   b. i destinatari dei dati o le categorie di destinatari;
   c. trasferimento dei dati a paesi terzi o a organizzazioni internazionali;
e) determinare se eventuali **requisiti complementari, come le norme nazionali e specifiche del settore, devono essere affrontati dalla certificazione**.

Deve essere chiarito il ruolo del Richiedente come Titolare o Responsabile del trattamento del Target of Evaluation. Nel caso in cui i Richiedenti agiscano in qualità di contitolari, le implicazioni per il Target of Evaluation e la certificazione devono essere analizzate attentamente.

La specifica finale del Target of Evaluation e dell' Ambito Normativo rimane sotto il controllo dell'Organismo di Certificazione e deve essere allineata con la capacità dell'Organismo di Certificazione di valutare efficacemente la conformità degli elementi inclusi nel campo di applicazione. L'Organismo di Certificazione può decidere di adattare il Target of Evaluation e l'Ambito Normativo nel corso del processo di certificazione.

L'Organismo di Certificazione deve garantire di poter valutare adeguatamente il Target of Evaluation.

L'Organismo di Certificazione deve garantire che il Target of Evaluation sia adeguatamente specificato per trasmettere informazioni chiare agli interessati. Deve evitare qualsiasi certificazione fuorviante o eccessiva ampiezza del Target of Evaluation. Deve rifiutare qualsiasi Target of Evaluation che sia ambiguo, fuorviante o che rischi di essere mal interpretato dagli interessati o da terzi.

7.2.4. Chiarimento dell'Ambito Normativo

Al momento di specificare il Target of Evaluation, il Richiedente e l'Organismo di Certificazione devono valutare e determinare se le normative complementari nazionali o specifiche per il settore della protezione dei dati devono essere incluse nell'Ambito Normativo della certificazione prevista.

Deve prendere in considerazione il rischio potenziale di un'interpretazione errata da parte dell'interessato, nonché il contesto, come le aspettative specifiche del settore e dell'ambito applicativo in materia di protezione dei dati.

L'Ambito Normativo della certificazione deve essere chiaramente specificato.

7.2.5. Revisione e convalida dell'Application

L'Organismo di Certificazione deve esaminare le informazioni ricevute attraverso il Processo di Richiesta per garantire che:

a) il modulo di domanda è completo;
b) le informazioni sul Richiedente e sul Target of Evaluation sono sufficienti per prendere una decisione e valutare l'impegno richiesto per il processo di certificazione;
c) il Target of Evaluation sia ben definito e si tenga conto di tutti gli altri aspetti che influenzano l'attività di certificazione (tempo necessario per completare l'audit, lingua, condizioni di sicurezza, minacce all'imparzialità, ecc.);
d) esiste una comprensione e un accordo reciproco tra l'organismo di certificazione e l'organizzazione richiedente in merito al Target of Evaluation;
e) l'Ambito normativo da utilizzare sia adeguato per evitare qualsiasi certificazione fuorviante;
f) siano disponibili i mezzi per svolgere tutte le attività di valutazione e di audit e, in particolare, che l'Organismo di Certificazione abbia accesso alle competenze tecniche e giuridiche adeguate per la certificazione richiesta;
g) i controlli e le verifiche di Europrivacy sono adeguati per valutare il Target of Evaluation.

La certificazione ai sensi dell'articolo 43 del GDPR richiede che la domanda e le specifiche del Target of Evaluation siano conformi a una serie di requisiti specifici. Per convalidare la conformità a tali requisiti, **l'Organismo di Certificazione deve applicare l'apposito elenco di verifiche e controlli Europrivacy per convalidare l'Applicazione e il Target of Evaluation**[8].

7.2.6. Verifica rapida e chiarimenti con il Richiedente

Se pertinente, l'Organismo di Certificazione deve proporre un incontro o una teleconferenza per chiarire il Target of Evaluation previsto. L'incontro può anche servire a comprendere meglio il contesto e le specificità del trattamento dei dati coinvolti, a determinare la fattibilità della certificazione, a valutare meglio lo sforzo di certificazione, nonché a discutere e concordare il processo di certificazione previsto.

7.2.7. Determinazione dei criteri e della metodologia di valutazione

Come richiesto dall'EDPB, l'Organismo di Certificazione deve identificare i metodi di valutazione del Target of Evaluation e farvi riferimento nell'accordo di certificazione con il Richiedente.

Gli Organismi di Certificazione devono disporre di metodi di valutazione coerenti per Target of Evaluation comparabili, quali:

- Un metodo per valutare la necessità e la proporzionalità del trattamento dei dati rispetto alla finalità e al consenso dell'interessato.
- Un metodo per valutare la completezza della valutazione dei rischi da parte del Titolare del trattamento e dei suoi Responsabili del trattamento.
- Un metodo per valutare i rimedi, le garanzie e le procedure per garantire la protezione del trattamento dei dati personali nel Target of Evaluation.

L'Organismo di Certificazione deve garantire una documentazione appropriata e accessibile dei propri metodi e risultati.

L'Organismo di Certificazione determina i criteri Europrivacy e la metodologia di valutazione applicabile al Target of Evaluation.

[8] "A - Application and Target of Evaluation – Preliminary Checks and Controls"

L'Accordo di certificazione deve fare riferimento ai criteri di certificazione Europrivacy, che sono obbligatori. Dovrà chiarire se per la valutazione della conformità del Target of Evaluation saranno utilizzati ulteriori requisiti normativi, come le normative nazionali e specifiche del settore.

7.2.8. Valutazione dei rischi e dei requisiti del personale

Una volta chiarito l'Ambito Normativo, l'Organismo di Certificazione deve identificare i principali rischi in termini di protezione dei dati, nonché l'impegno di lavoro necessario per valutare, verificare e certificare il Target of Evaluation. Dovrà valutare se dispone del personale e delle risorse necessarie per eseguire il processo di certificazione.

7.2.9. Decisione sull'Application

Dopo aver esaminato la domanda, l'Organismo di Certificazione decide se accettarla o rifiutarla. Esso valuterà se è in grado di fornire una certificazione affidabile del Target of Evaluation.

In caso di decisione negativa, informerà il Richiedente con spiegazioni in merito alla sua decisione e potrà raccomandare altri Organismi di certificazione qualificati.

Se la decisione è positiva, determina le competenze necessarie per eseguire il processo di certificazione secondo la revisione e prepara un'offerta.

7.3. Offerta

7.3.1. Stimare il tempo e l'impegno necessari per la valutazione

L'Organismo di Certificazione deve stimare il tempo di audit previsto necessario per garantire che tutte le aree di interesse delle attività di trattamento dei dati siano adeguatamente valutate con l'intensità necessaria. Deve tenere conto dei seguenti fattori:

a) il numero di criteri applicabili al Target of Evaluation;
b) la potenziale inclusione di criteri complementari Estensioni per valutare la conformità a norme e regolamenti complementari;
c) l'estensione geografica del Target of Evaluation e il numero di siti da ispezionare.

Lo Scheme Owner fornisce risorse e strumenti per aiutare a stimare l'impegno e il tempo necessari.

7.3.2. Preparazione dell'offerta

Una volta presa la decisione di accettare l'Application, l'Organismo di Certificazione dovrà preparare un'Offerta scritta che contenga almeno:

a) l'Ambito Normativo proposto, gli obiettivi e i criteri per la certificazione;
b) informazioni sull'intero processo di certificazione, tra cui:
   - metodologia utilizzata per certificare e mantenere la certificazione;
   - un link al sito web ufficiale del sistema di certificazione;
c) i termini e le condizioni, tra cui:
   - gli obblighi del Richiedente indicati nello Schema di Certificazione;
   - il chiarimento dei ruoli e delle responsabilità delle varie parti;
d) una stima dei costi (o almeno un modello di costo e un'indicazione del costo orario) dei servizi;
e) una clausola di riservatezza che si applica di default a tutti i documenti scambiati con il Richiedente, compresa l'Offerta stessa;
f) al fine di semplificare il processo amministrativo, l'Organismo di Certificazione può anche decidere di presentare una proposta iniziale di Programma di Certificazione come parte dell'Offerta al Richiedente.

7.3.3. Presentazione dell'offerta

L'offerta presentata deve essere limitata nel tempo con una scadenza precisa.

Se il Richiedente è d'accordo con le condizioni, dovrà sottoscrivere l'Offerta e/o i relativi contratti di certificazione e procedere ai pagamenti nei tempi indicati.

Se il Richiedente non firma l'accordo o non paga la fattura di apertura entro la scadenza, l'Offerta può essere considerata rifiutata. L'Organismo di Certificazione sarà libero di assumere altri impegni e non avrà più alcun

obbligo di seguire l'Offerta presentata, tranne se richiesto dalla legge. Non avrà inoltre alcun obbligo di accettare una nuova domanda.

7.3.4. Accettazione dell'offerta

L'accettazione formale dell'Offerta da parte del Richiedente sarà formalizzata dalle firme autorizzate dei firmatari designati del Richiedente e dalla loro accettazione formale dei termini e delle condizioni proposti.

Se l'Offerta richiede un pagamento iniziale prima dell'inizio del processo di certificazione, l'accordo sarà considerato completo solo dopo che il Richiedente avrà effettuato il pagamento necessario.

7.3.5. Fatture e pagamenti

I risultati degli Audit possono avere un impatto sul processo di certificazione, sul numero di ore di lavoro richieste e sul costo finale della certificazione. Gli Organismi di Certificazione devono informare i Richiedenti di qualsiasi deviazione prevista rispetto all'offerta iniziale.

Il Richiedente si impegna a pagare in tempo utile tutte le fatture inviate dall'Organismo di Certificazione per il processo di certificazione. L'Organismo di Certificazione può sospendere o annullare il processo di certificazione in caso di mancato pagamento o di eccessivo ritardo nel pagamento da parte del Richiedente.

7.4. Composizione del Audit Team e funzioni associate

Parallelamente alla presentazione dell'Offerta, o al più tardi nel momento in cui il Richiedente accetta l'Offerta, l'Organismo di Certificazione deve prendere le disposizioni necessarie per il processo di valutazione. Dovrà assegnare almeno un Lead Auditor e un Project Manager (che può essere la stessa persona del Lead Auditor) e identificare i membri complementari del Team di Audit, se necessario, compresi gli Auditor complementari e gli Esperti Tecnici.

I Reviewer non fanno parte del team di audit e possono essere identificati in una fase successiva.

Come specificato nelle linee guida EDPB per la certificazione, la valutazione può essere "effettuata da esperti esterni riconosciuti dall'organismo di certificazione".

7.4.1. Qualifiche richieste

Il team di audit deve riunire le competenze e le capacità necessarie per eseguire l'audit e applicare lo Schema di Certificazione al Target of Evaluation selezionato. In particolare, ogni team deve comprendere:

- Competenza nella normativa sulla protezione dei dati;
- Conoscenza e comprensione adeguate dei requisiti del sistema di certificazione Europrivacy;
- Competenze tecniche adeguate per analizzare l'adeguatezza delle misure tecniche e organizzative adottate per proteggere i dati trattati.

Gli Auditor devono aver completato con successo il corso di valutazione Europrivacy e superato il relativo esame sul sito web dell'Europrivacy Online Academy (https://academy.europrivacy.com).

La selezione del gruppo di audit deve rispettare i requisiti specifici relativi alle qualifiche specificati nella sezione sulla gestione del personale e delle risorse (cfr. sezione 14) e nel documento "Gestione delle competenze del personale coinvolto nel processo di certificazione Europrivacy".

7.4.2. Composizione complessiva del team di certificazione

Un team di certificazione può essere composto da diversi ruoli e funzioni, tra cui:

Come parte del team di audit formale:

- Lead Auditor;
- Additional Auditors (facoltativi);
- Esperti Tecnici e/o Legali (facoltativo, se gli Auditor hanno competenze adeguate per la valutazione del Target of Evaluation).

Funzioni aggiuntive che integrano l'Audit Team:

- Project Manager;
- Reviewer.

Le funzioni di Project Manager e Lead Auditor possono essere combinate e svolte da un'unica persona, oppure assegnate a due persone distinte.

La presenza di coadiutori è facoltativa.

Possono essere incluse funzioni aggiuntive, come le Guide fornite dal Richiedente e gli Observer.

L'Organismo di Certificazione deve garantire che i Lead Auditor e i Reviewer abbiano un livello adeguato di competenza in materia di protezione dei dati per valutare e convalidare le conclusioni del processo di certificazione.

La figura seguente riassume le funzioni chiave dell'organismo di certificazione per il processo di audit:

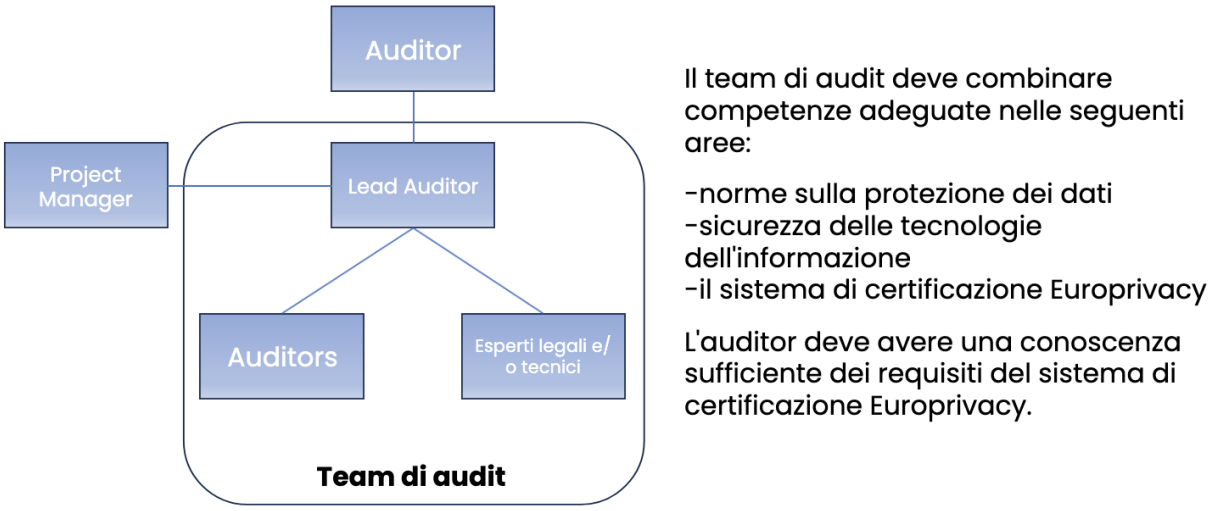

Figura 5 Struttura dell'ordinario Audit Team periodico

7.4.3. Project Manager

Il Project Manager sarà il contatto principale del Richiedente ed è responsabile del monitoraggio delle attività relative al processo di certificazione del Richiedente. Il Project Manager dovrà garantire che:

- tutti i documenti contrattuali richiesti siano firmati e ritirati;
- tutte le informazioni necessarie per il processo di certificazione sono raccolte dal Richiedente;
- il piano di revisione e le relative riunioni siano adeguatamente organizzate;
- il rapporto di audit viene completato, rivisto e condiviso con il Richiedente;
- tutte le informazioni, la documentazione e i rapporti pertinenti siano archiviati nel sistema di gestione della protezione dei dati dell'organismo di certificazione;
- tutte le fatture e i pagamenti siano correttamente compilati;
- se del caso, il certificato viene consegnato e pubblicato nel Registro online.

L'Organismo di Certificazione può decidere di trasferire alcuni o tutti questi compiti al Lead Auditor.

7.4.4. Lead Auditor

Dopo l'accettazione dell'Offerta, l'Organismo di Certificazione designerà un Lead Auditor la cui responsabilità principale sarà quella di coordinare ed eseguire l'audit, nonché di produrre il rapporto di audit da presentare ai Reviewer.

Il Lead Auditor deve possedere una conoscenza completa delle specifiche e dei requisiti dello Schema di Certificazione, completando con successo la propria qualifica di auditor tramite l'Europrivacy Online Academy: https://academy.europrivacy.com.

7.4.5. Auditors

Ulteriori Auditor possono unirsi al Team di Audit sotto l'autorità del Lead Auditor. Essi devono avere un'adeguata conoscenza dello Schema di Certificazione e soddisfare i requisiti specificati dallo Schema di Certificazione, completando con successo la qualifica di auditor tramite l'Europrivacy Online Academy: https://academy.europrivacy.com.

7.4.6. Esperti Tecnici e Legali

Gli Esperti Tecnici e Legali possono integrare un Audit Team fornendo competenze aggiuntive. Quando eseguono un audit, agiscono sotto l'autorità del Lead Auditor e si concentrano sulla loro missione specifica.

L'Organismo di Certificazione dovrà informare preventivamente il Richiedente del coinvolgimento degli Esperti Tecnici nelle attività di certificazione.

7.4.7. Valutatori

I membri dell'Audit Team possono fungere da valutatori per allenare e valutare il Lead Auditor e/o i membri dell'Audit Team. I Valutatori possono essere designati dallo Scheme Owner e/o dall'Organismo di certificazione e/o dall'autorità nazionale competente. I valutatori lavoreranno e si comporteranno come normali Auditor o Esperti Tecnici nel processo di certificazione per il Richiedente. Riferiranno le loro osservazioni, chiarimenti e raccomandazioni di miglioramento all'Audit Team e, se del caso, all'Organismo di Certificazione e/o allo Scheme Owner.

7.4.8. Observer

Gli Observer possono essere invitati a partecipare all'Audit Team. Gli Observer possono essere membri dell'organizzazione del Richiedente, consulenti, personale dell'ente di accreditamento, personale dell'Autorità di Controllo, rappresentanti dello Scheme Owner, autorità di regolamentazione o altre persone la cui partecipazione sia giustificata.

Gli Observer sono tenuti a rispettare gli obblighi di riservatezza prima di partecipare all'audit.

Quando un Organismo di Certificazione prevede di invitare Observer a un audit, deve informare preventivamente il Richiedente, in modo che questi abbia la possibilità di opporsi a tale presenza.

L'Observer non avrà alcun coinvolgimento diretto nel processo di audit e certificazione. Se gli Observer individuano una non conformità allo Schema di Certificazione da parte del Team di Audit, devono comunicare le loro osservazioni al Lead Auditor e/o al Team di Audit nel contesto di un debriefing strettamente bilaterale.

7.4.9. Guide

Quando si effettuano audit in loco, gli Auditor devono essere accompagnati da una Guida, a meno che non sia stato concordato diversamente dal Lead Auditor e dal soggetto controllato.

Il compito della Guida è quello di agevolare il lavoro degli Auditor facilitando loro l'accesso a locali, dipendenti, documenti, informazioni e qualsiasi altra risorsa ritenuta rilevante dagli Auditor per il processo di certificazione. La Guida può essere incaricata di:

a) organizzare e pianificare le visite e i colloqui;
b) garantire la sicurezza dei membri del Audit Team;
c) testimoniare dell'audit per conto del Richiedente;
d) fornire chiarimenti o informazioni su richiesta di un Auditor.

Il soggetto controllato deve assicurarsi che la Guida abbia l'autorità e le competenze adeguate per svolgere il proprio compito.

L'Audit Team deve garantire che le Guide non influenzino o interferiscano nel processo di audit o nel risultato dell'audit.

7.4.10. Traduttori e interpreti

Possono essere necessari traduttori e interpreti e ciò può avere un impatto sulla durata dell'audit. L'Organismo di certificazione deve selezionare traduttori e interpreti imparziali e non in grado di influenzare indebitamente l'audit.

7.4.11. Reviewer

La funzione principale del Reviewer (o dei Reviewer) è quella di esaminare il rapporto e i risultati dell'Auditor e di prendere una decisione sulla certificazione. La funzione di Reviewer deve essere svolta da una persona o da un gruppo di persone (ad esempio, un comitato) che non sono state coinvolte nel processo di valutazione. I Reviewer possono fungere da Lead Auditor o da Auditor in altri processi di certificazione, ma non nel processo di certificazione oggetto della loro revisione.

Il/i Reviewer/s deve/devono essere impiegato/i o avere un contratto con l'Organismo di Certificazione o con un'entità sotto il controllo organizzativo dell'Organismo di Certificazione. I Reviewer non direttamente impiegati dall'Organismo di certificazione devono soddisfare gli stessi requisiti di idoneità previsti per i dipendenti dell'Organismo di Certificazione.

7.5. Utilizzo della certificazione preventiva di parti del Target of Evaluation

Secondo l'EDPB, le certificazioni precedenti di parti del Target of Evaluation possono essere considerate nel processo di certificazione, ma il loro riconoscimento deve richiedere almeno:

- **La disponibilità del rapporto di certificazione completo, oppure**
- **Informazioni adeguate per valutare le attività di certificazione precedenti e i relativi risultati.**

La ISO/IEC 17065 richiede che l'Organismo di Certificazione utilizzi solo *"i risultati della valutazione relativi alla certificazione completata prima della richiesta di certificazione".*[9] **È consentito riutilizzare le evidenze documentate**.

7.6. Assessment Plan

L'Organismo di Certificazione deve determinare un Assessment Plan adeguato alle specificità del Target of Evaluation. Dovrà tenere conto di potenziali requisiti aggiuntivi, quali obblighi specifici del dominio e/o nazionali inclusi nel campo di applicazione normativo della certificazione richiesta.

L'Assessment Plan deve specificare:

a) Il Target of Evaluation;
b) La composizione e i ruoli nel Certification Team;
c) Una pianificazione generale provvisoria delle attività di valutazione.

7.7. Obbligo di informare l'Autorità per la protezione dei dati

Prima di iniziare il processo di certificazione, un Organismo di Certificazione che opera in un altro Stato membro dello Spazio Economico Europeo deve informare l'Autorità di Controllo competente.

[9] Vedi clausola 7.4.5 ISO/IEC 17065

8. Valutazione della conformità e rendicontazione

8.1. Assessment Activities

Il Target of Evaluation deve essere valutato rispetto ai requisiti e ai criteri specificati nello Schema di Certificazione, entro i limiti del Target of Evaluation e dell'Ambito Normativo concordati. Ogni criterio applicabile al Target of Evaluation deve essere valutato.

La valutazione della conformità può comprendere attività quali l'esame della documentazione e dei file, il campionamento, le prove, l'esame, i colloqui e gli audit, a seconda dei casi. La valutazione dei criteri deve essere effettuata in conformità alle Linee guida Europrivacy sull'uso di criteri, verifiche e controlli.

L'Organismo di Certificazione dovrà svolgere le attività di valutazione utilizzando le proprie risorse interne e dovrà gestire le risorse esterne in conformità all'Assessment Plan. La valutazione sarà effettuata da un gruppo di audit con adeguate competenze legali e tecniche.

8.2. Revisione della documentazione

8.2.1. Accesso alla documentazione

L'Organismo di Certificazione deve avere accesso alla documentazione, ai file e ai registri necessari per valutare la conformità del Target of Evaluation. Ove applicabile, la documentazione e le prove possono essere raccolte per via elettronica e rese disponibili in un archivio online protetto.

È accettabile che, per motivi di sicurezza, alcuni documenti siano accessibili solo in loco dal Richiedente (ad esempio, la configurazione del firewall). Tuttavia, la **documentazione e le prove possono essere conservate e archiviate dall'Organismo di Certificazione in base alle necessità**.

L'ECCP fornisce un elenco di riferimento della documentazione a cui l'Organismo di Certificazione deve accedere per il processo di certificazione. Può essere utilizzato dal Richiedente per raccogliere e facilitare l'accesso alla documentazione richiesta.

8.2.2. Revisione della documentazione preliminare

Prima di iniziare la valutazione formale, il Project Manager o il Lead Auditor deve assicurarsi che **tutta la documentazione richiesta esista e sia accessibile all'Audit Team**. Un elenco di riferimento della documentazione richiesta è reso disponibile dallo Scheme Owner e può essere adattato dall'Organismo di Certificazione.

L'esame iniziale della documentazione non ha lo scopo di valutare la conformità del Target of Evaluation, ma deve verificare che il progetto sia conforme:

- **il DPO ha una competenza adeguata**, che deve essere verificata prima di convalidare i documenti forniti dall'RPD;
- **i documenti siano chiaramente identificabili** con date e/o numero di versione;
- la **documentazione sia completa e sufficiente per il processo di valutazione**.

Se la documentazione appare insufficiente, il Richiedente deve essere informato e la pianificazione del processo di valutazione deve essere discussa e riconfermata dall'Organismo di Certificazione e dal Richiedente.

8.3. Procedura di test

L'Organismo di Certificazione può eseguire prove per valutare la conformità delle lavorazioni ai requisiti dello Schema di Certificazione. Il riferimento ai Test o alle Prove nei mezzi di verifica suggeriti non si riferisce, né richiede, l'utilizzo di laboratori di prova.

La dimostrazione della conformità alla ISO/IEC 17025 non è richiesta dall'Organismo di Certificazione, ma se i test sono affidati a un laboratorio di prova esterno, quest'ultimo deve rispettare i requisiti della ISO/IEC 17025.

8.3.1. Uso dei campioni

L'Organismo di Certificazione può utilizzare campioni rappresentativi per valutare la conformità ai requisiti.

Per garantire che gli approcci di campionamento rimangano significativi e affidabili nel processo di certificazione, l'Auditor deve:

a) stabilire gli obiettivi del piano di campionamento;
b) selezionare la dimensione e la composizione della popolazione da campionare;
c) selezionare un metodo di campionamento;
d) determinare la dimensione del campione;
e) condurre l'attività di campionamento;
f) compilare, valutare, riferire e documentare i risultati.

Gli Auditors possono utilizzare sia il campionamento basato sul giudizio che il campionamento statistico.

Quando si applica un approccio di campionamento basato sul giudizio, la dimensione del campione deve includere almeno una voce per ogni cifra del numero totale di voci in esame, con una dimensione minima del campione di tre voci.

Quando si applica un approccio di campionamento statistico, l'Auditor può adattare la percentuale del livello di confidenza accettabile al livello di rischio e di impatto associato in caso di non conformità. Per impostazione predefinita, l'Auditor dovrebbe utilizzare almeno un livello di confidenza del 95% con un margine di errore massimo del 5%.

8.3.2. Prove tecniche

Ogniqualvolta sia pertinente, deve essere eseguita una serie di test tecnici per identificare eventuali vulnerabilità relative alla protezione dei dati e/o per eseguire le verifiche e i controlli richiesti dallo Schema di Certificazione (ad esempio, Vulnerability Assessments, Penetration Test). Il processo sarà gestito da Esperti Tecnici o laboratori con le competenze richieste. Gli esperti tecnici e i laboratori agiscono sotto la supervisione del Lead Auditor che può richiedere test e risultati specifici.

8.4. Esami e valutazioni in loco

8.4.1. Principi d'esame

Per esame si intende la visita o la valutazione a distanza dei locali in cui viene eseguito o gestito il trattamento, al fine di verificare e determinare se i requisiti specificati nei Criteri sono soddisfatti. L'esame può comprendere, a titolo esemplificativo, osservazioni visive, richieste di dimostrazioni e domande rivolte ai soggetti coinvolti nell'elaborazione dei dati.

8.4.2. On-site Assessment and Audits – Principi generali

In base al Target of Evaluation, possono essere richieste valutazioni in loco (dette anche "Audit"). Le valutazioni in loco possono utilizzare tecnologie per l'esame a distanza.

L'Organismo di Certificazione deve organizzare valutazioni in loco ogni qualvolta ve ne sia una chiara necessità o quando il Lead Auditor ritiene che tale azione sia necessaria per esprimere un parere affidabile sulla conformità del Target of Evaluation.

La decisione di effettuare valutazioni in loco dovrebbe essere comunicata al Richiedente nelle prime fasi del processo, in linea di principio con l'Assessment Plan, dopo che la domanda è stata elaborata e tutti i documenti necessari sono stati rivisti. Tuttavia, la decisione di effettuare le valutazioni in loco può essere presa in una fase successiva, ad esempio dopo che i test iniziali e i risultati della valutazione sono stati consegnati al Lead Auditor.

I criteri di audit sono quelli specificati nello Schema di Certificazione, compreso l'elenco delle verifiche e dei controlli dettagliati in base ai quali viene determinata la conformità.

Le prove dell'Audit devono essere costituite da registrazioni, dichiarazioni di fatti e altre informazioni relative ai criteri e devono essere verificabili.

8.4.3. Preparazione dell'On-site Assessment

Il Project Manager assegnerà un Lead Auditor qualificato o un Team di Audit per eseguire la valutazione o l'audit in loco. L'Organismo di Certificazione deve assicurarsi che la qualifica del Audit Team sia adeguata al tipo di attività svolta dal Richiedente.

Il Lead Auditor deve inviare l'Audit Plan al rappresentante del Richiedente almeno due settimane prima della valutazione o dell'audit per la conferma e l'accettazione. L'Audit Plan deve menzionare un elenco preliminare di requisiti, risorse e documenti che il Richiedente deve preparare per l'audit in loco.

8.4.4. On-site Assessment Process

Le fasi della valutazione o dell'audit in loco devono includere quanto segue:

a) una riunione di apertura, durante la quale il Lead Auditor presenta:
   - il piano di valutazione/audit, compresi gli obiettivi, l'ambito e i punti principali da verificare;
   - una sintesi delle prove e dei risultati delle fasi precedenti;
b) l'analisi e la valutazione della documentazione;
c) l'identificazione delle fonti di informazione rilevanti;
d) la raccolta di informazioni mediante campionamento, test, esami e verifiche appropriati, comprese, se del caso, visite in loco e colloqui con i dipendenti;
e) stabilire le prove di valutazione/audit delle fasi precedenti;
f) la valutazione delle informazioni e delle prove raccolte rispetto ai requisiti dello Schema di Certificazione;
g) la formulazione dei risultati della valutazione/audit;
h) l'esame dei risultati e delle evidenze della valutazione/audit per formulare le conclusioni della valutazione o dell'audit;
i) una riunione di chiusura, in cui il Lead Auditor presenta la valutazione o le conclusioni dell'audit.

8.4.5. On-site Assessment Summary Report

L'Organismo di Certificazione deve preparare un rapporto formale di sintesi della valutazione o dell'audit per presentare i risultati e le conclusioni della valutazione o dell'audit, nonché per fornire informazioni su eventuali Non Conformità identificate.

8.4.6. Multi-site Assessment

Il Target of Evaluation può riguardare il trattamento dei dati personali distribuito su più siti sotto il controllo effettivo del Richiedente. L'Organismo di Certificazione deve stabilire se sono necessarie valutazioni su più siti per dimostrare la conformità ai criteri.

Quando è richiesta una valutazione su più siti, l'Organismo di Certificazione può applicare un campionamento per sito tra i siti che svolgono attività di elaborazione dati simili. Il campionamento del sito è applicabile solo se il Richiedente dispone di un controllo e di un monitoraggio efficaci sui siti interessati.

I siti saranno selezionati tenendo conto di:

a) il livello di rischio per i dati trattati;
b) la diversità dei siti;

E dove applicabile:

a) risultati di audit precedenti;
b) reclami segnalati.

Inoltre, ove applicabile, almeno il 25% dei siti sarà selezionato a caso.

Il numero minimo di siti da valutare sarà proporzionale alla radice quadrata del numero di siti, con il seguente rapporto:

- Verifica iniziale: radice quadrata semplice, arrotondata al numero intero inferiore.
- Audit di sorveglianza: 60% del risultato della radice quadrata arrotondato al numero intero immediatamente inferiore.
- Ri-certificazione: 80% del risultato della radice quadrata arrotondato al numero intero inferiore.

Quando si esegue una valutazione su più siti, la riduzione del tempo di audit in loco per ogni sito campionato può essere ridotta al 50% del tempo di audit normale.

8.5. Utilizzo dei risultati di audit di altri organismi di certificazione

Nel caso in cui l'Organismo di Certificazione tenga conto della certificazione già concessa al Richiedente da un altro Organismo di Certificazione, dovrà ottenere e conservare prove sufficienti, quali rapporti e documentazione sulle azioni correttive relative a qualsiasi Non Conformità. L'Organismo di Certificazione deve giustificare e registrare qualsiasi adeguamento al programma di audit esistente e seguire l'attuazione delle azioni correttive relative a precedenti Non Conformità.

8.6. Valutazione della conformità

8.6.1. Strumenti di valutazione suggeriti

I Criteria menzionano i mezzi di valutazione suggeriti. **A seconda del Target of Evaluation, possono essere applicabili diversi mezzi di valutazione e possono essere necessari più mezzi di valutazione**. Ad esempio, la valutazione della procedura per il diritto dell'Interessato di richiedere l'accesso ai Dati personali può essere effettuata verificando come tali richieste sono state gestite dal Richiedente. Tuttavia, se il Richiedente non ha ancora ricevuto alcuna richiesta, una revisione della documentazione delle regole, delle politiche e delle procedure del Richiedente e/o la verifica dell'efficacia della procedura sarebbero valide alternative.

L'Auditor deve utilizzare i mezzi di valutazione più efficienti e raccogliere prove sufficienti per determinare con un elevato livello di fiducia la conformità o la non conformità di ciascun Criterio applicabile.

Secondo la ISO/IEC 17007, *"dovrebbe essere lasciato agli utenti del documento normativo decidere quale attività di valutazione della conformità (se esiste) sarà utilizzata, chi effettuerà la valutazione della conformità e in quali condizioni"*. **Per ogni criterio, l'Auditor deve utilizzare uno o più mezzi di valutazione, fino a raccogliere prove sufficienti per determinare se i requisiti sono soddisfatti**.

Per impostazione predefinita, si consiglia il seguente ordine di priorità:

a. esame della documentazione, compreso l'esame di fascicoli e registri;
b. interviste;
c. esami;
d. test;
e. altri mezzi di verifica, a condizione che siano efficienti e affidabili.

L'ordine di priorità può essere adattato quando un mezzo di valutazione non è applicabile o quando un ordine diverso può aumentare l'efficienza e l'affidabilità della valutazione. L'uso di altri mezzi di verifica deve essere registrato e giustificato.

I colloqui saranno effettuati come parte della valutazione del Target of Evaluation.

Maggiori dettagli sulla valutazione dei criteri sono forniti nelle Linee guida Europrivacy sull'uso di criteri, verifiche e controlli , nonché nella sezione FAQ del sito web di Europrivacy Resources and Community: https://community.europrivacy.com

8.6.2. Registrazione delle prove

Per valutare lo stato di un Criterio, dei Controlli e delle Verifiche, gli Auditor devono raccogliere e registrare evidenze chiare che dimostrino la conformità o la non conformità al requisito.

L'Organismo di Certificazione deve essere in grado di dimostrare che le sue conclusioni sono basate su prove evidenti.

8.6.3. Risultati e stato dei Criteri, delle Verifiche e dei Controlli

La maggior parte dei controlli e delle verifiche sono valutati e determinati in base a una delle seguenti categorie di stato:

Codice di stato	Significato/Spiegazione
?	**Informazioni mancanti/non so**
OK	Conformità: Il requisito è stato **verificato** e risulta essere conforme. Non sono state identificate Non Conformità.
OK+	Buone pratiche che vanno oltre la semplice conformità
Obs	**Osservazione**
Min NC	È stata identificata una **Non Conformità Minore** (non critica).
Maj NC	È stata identificata una **Non Conformità Maggiore** (critica).
NA	Il controllo non è applicabile alla certificazione in questione

Figura 6 Categorie di stato per i risultati

Quando i controlli sono considerati non applicabili, il motivo deve essere giustificato e documentato.

8.6.4. Qualificazione delle Non-Conformità

Se la valutazione di un Criterio (o di un Controllo e Verifica) porta a identificare un "non soddisfacimento di un requisito", ciò costituisce una Non Conformità.

Tutte le Non Conformità devono essere elencate con un numero di identificazione distinto e devono essere chiaramente descritte con il riferimento alla norma specifica e ai requisiti non rispettati. Ciascuna di esse dovrà essere qualificata come Non Conformità "Minore" o "Maggiore".[10]

Non-Conformità "Maggiori"

Una Non Conformità Maggiore è una Non Conformità che viola la conformità delle attività di trattamento nel Target of Evaluation con i requisiti fondamentali di protezione dei dati, i diritti degli interessati o i requisiti dello Schema di Certificazione Europrivacy, come indicato nel presente documento.

Qualsiasi Non Conformità in cui il Richiedente viola i propri obblighi legali, come specificato nel GDPR, costituisce una Non Conformità Maggiore.

Non-Conformità "Minori"

Una Non Conformità Minore è una Non Conformità non critica che non si qualifica come Non Conformità Maggiore.

Osservazioni

Il processo di valutazione può portare all'individuazione di situazioni che non costituiscono una formale Non-Conformità ai requisiti valutati, ma che possono essere considerate al limite o non ottimali. In tal caso, il Valutatore deve qualificare lo stato come "Osservazione" e annotare i risultati e le preoccupazioni.

8.6.5. Impatto delle Non-Conformità

È vietato consegnare una certificazione in uno dei seguenti casi:

- **In presenza di una qualsiasi Non-Conformità Maggiore non chiusa;**
- **In presenza di più di cinque Non-Conformità Minori in attesa di verifica;**
- **Se la certificazione potrebbe essere fuorviante per terzi e per gli interessati.**

[10] La differenziazione deve essere conforme alla ISO/IEC 17021-1.

In caso di Non-Conformità Minori rimanenti, il Richiedente deve presentare un piano di correzione e impegnarsi a risolvere le Non-Conformità Minori identificate prima del successivo Audit di Sorveglianza.

Nel caso in cui siano state identificate delle Non-Conformità Minori e sia stato accettato un piano d'azione correttivo dall'Organismo di Certificazione, quest'ultimo è autorizzato a rinviare la rivalutazione di un massimo di 5 Non-Conformità Minori per le quali sarà richiesta l'evidenza della conformità solo entro il successivo Audit di Sorveglianza.

Per qualsiasi Non Conformità Maggiore, l'Organismo di Certificazione deve aver **rivisto, accettato e verificato la correzione** e le azioni correttive per considerarla risolta e chiusa.

Per qualsiasi Non-Conformità Minore, l'Organismo di Certificazione deve aver **esaminato, accettato e verificato la correzione** per considerarla risolta e chiusa, oppure deve aver **accettato il piano di azioni correttive del Richiedente** da valutare e convalidare all'audit successivo.

Le Non-Conformità Minori identificate in una precedente valutazione e non affrontate dal Richiedente possono essere riqualificate dall'Organismo di Certificazione come "Non-Conformità Maggiori".

Se durante il processo di valutazione sono emerse Non-Conformità che impediscono la certificazione, e se il Richiedente esprime interesse a continuare il processo di certificazione, l'Organismo di Certificazione dovrà:

a) fornire informazioni sui compiti di valutazione aggiuntivi necessari per verificare che le Non-Conformità da correggere siano state corrette;
b) concordare con il Richiedente il ritardo necessario (che non dovrebbe superare i 6 mesi) per correggere le Non-Conformità identificate.

Se il Richiedente accetta il completamento dei compiti di valutazione aggiuntivi e, **se del caso, per garantire l'affidabilità della valutazione di conformità, il processo di valutazione deve essere ripetuto per completare i compiti di valutazione aggiuntivi**, in conformità ai requisiti della ISO/IEC 17065. Le prove documentate possono essere riutilizzate.

8.6.6. Correction Action Plan

Se il Richiedente esprime interesse a proseguire il processo di certificazione, deve essere elaborato un Piano d'Azione Correttivo come segue:

L'Organismo di Certificazione comunicherà al Richiedente l'elenco delle Non-Conformità identificate e il modo in cui queste si riferiscono ai requisiti della certificazione.

Il Richiedente deve preparare e proporre un Piano d'Azione Correttivo con azioni correttive per ogni Non-Conformità identificata, che fornisca la motivazione della Non-Conformità (ad esempio, un'analisi delle cause). Il Piano d'azione correttivo deve elencare le potenziali Non-Conformità e classificarle in base al loro grado di gravità (Non-Conformità "Maggiore" o "Minore"). Le azioni appropriate da intraprendere e le modalità di applicazione devono essere dettagliate. Le azioni correttive proposte dal Richiedente devono essere appropriate e complete per il proseguimento del processo di certificazione; in caso contrario, l'Organismo di Certificazione chiederà al Richiedente di proporre nuove azioni correttive.

Il Piano d'azione correttivo deve essere completato dal Richiedente entro un periodo di tempo concordato che non deve superare i 6 mesi.

8.6.7. Conseguenze del persistere delle Non-Conformità

La conseguenza del persistere delle Non-Conformità sulla certificazione è definita in base alla natura e alla gravità della Non-Conformità, nonché al suo verificarsi e al rischio di frode.

Le misure appropriate relative al piano di correzione possono essere:

a) Continuazione della certificazione in base alle condizioni;
b) Riduzione del campo di applicazione della certificazione;
c) Sospensione o ritiro della certificazione.

8.7. Report di Valutazione

Al termine delle attività di valutazione, il Lead Auditor è responsabile della generazione di un Report di Valutazione per il Richiedente.

Il Report di Valutazione **può identificare aree di miglioramento, ma non deve raccomandare soluzioni specifiche** per evitare la fornitura di consulenza.

Il Rapporto deve *"descrivere il modo in cui i requisiti sono stati soddisfatti e, se non sono stati inizialmente soddisfatti, descrivere le correzioni e le azioni correttive e la loro adeguatezza, fornendo così le ragioni per la concessione e il mantenimento della certificazione". Ciò include la descrizione della decisione individuale per la concessione, il rinnovo o il ritiro di un certificato. Dovrebbe fornire le ragioni, le argomentazioni e le prove risultanti dall'applicazione dei criteri e le conclusioni, i giudizi o le deduzioni dai fatti o dalle premesse raccolte durante la certificazione."* (EDPB)

Il Report deve contenere un resoconto accurato, conciso e chiaro della valutazione, al fine di informare il Richiedente e consentire una decisione di certificazione consapevole. Esso deve includere:
informazioni di identificazione, tra cui:

a) il nome dell'Organismo di Certificazione;
   - il nome del Richiedente;
   - l'indirizzo del Richiedente;
   - il nome del rappresentante del Richiedente;
b) una dichiarazione di esclusione di responsabilità, indicando che la revisione contabile si basa su un campione delle informazioni disponibili;
c) se del caso, informazioni sul piano di revisione:
   - il tipo di audit (iniziale/di sorveglianza/di ricertificazione/speciale);
   - i criteri di audit;
   - gli obiettivi dell'audit;
   - il Target of Evaluation, in particolare l'identificazione delle unità organizzative o funzionali o dei processi sottoposti ad audit e il momento dell'audit;
   - se applicabile, l'indicazione di audit combinati, congiunti o integrati;
d) informazioni su potenziali deviazioni:
   - qualsiasi deviazione dal piano di audit e le relative motivazioni;
   - qualsiasi questione significativa che abbia un impatto sul programma di audit;
e) le informazioni sulla composizione del Audit Team;
f) se del caso, le date e i luoghi delle attività di audit;
g) la valutazione e i risultati dell'audit:
   - risultati con riferimento alle prove pertinenti che descrivono il modo in cui i requisiti sono soddisfatti;
   - **Se i requisiti non erano inizialmente soddisfatti, descrizione delle correzioni e delle azioni correttive e loro adeguatezza;**[11]
   - conclusioni, coerentemente con i requisiti del tipo di revisione;
   - se applicabile, cambiamenti significativi che riguardano il sistema di gestione del Richiedente;
   - eventuali problemi irrisolti, se identificati;
h) ove applicabile, le osservazioni e le raccomandazioni formulate dall'Audit Team;
i) ove applicabile, la valutazione di come il Richiedente gestisce la propria certificazione e il proprio marchio di conformità;
j) ove applicabile, il rapporto sulle azioni correttive intraprese dal Richiedente per risolvere le Non Conformità precedentemente identificate;
k) una dichiarazione sulla conformità e l'efficacia della protezione dei dati con una sintesi delle prove relative a:
   - la capacità del sistema di gestione di proteggere efficacemente i dati personali;
   - l'audit interno e la revisione delle misure tecniche e organizzative in vigore;

[11] Si raccomanda vivamente di raccogliere informazioni sulle cause profonde delle Non-Conformità identificate.

l) una conclusione sull'adeguatezza del Target of Evaluation;
m) la conferma che gli obiettivi dell'audit sono stati raggiunti.

Il Report di Valutazione deve confermare formalmente che:

a) il campo di applicazione normativo e il Target of Evaluation sono sufficientemente chiari da evitare qualsiasi rischio di comprensione fuorviante della certificazione;
b) il Richiedente e i suoi rappresentanti sono stati trasparenti e collaborativi nel processo di certificazione;
c) i dati personali del Target of Evaluation sono:
   - trattati in modo lecito, equo e trasparente nei confronti dell'interessato;
   - raccolti per scopi specifici, espliciti e legittimi;
   - non vengano ulteriormente trattati in modo incompatibile con tali finalità;
   - adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati;
   - accurati e, se necessario, aggiornati;
   - conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati personali sono trattati;
   - trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da un trattamento non autorizzato o illegale e dalla perdita, dalla distruzione o dal danno accidentali, utilizzando misure tecniche o organizzative adeguate.

La proprietà e i diritti d'autore del Report di Valutazione sono di proprietà dell'Organismo di Certificazione.

8.7.1. Informazioni per il rilascio della certificazione iniziale

Al termine del processo di valutazione, il Lead Auditor preparerà e fornirà le seguenti informazioni al/ai Reviewer/s che esaminerà i risultati e preparerà la decisione:

a) il Report di Valutazione;
b) *"commenti sulle Non-Conformità e, se del caso, la correzione e le azioni correttive intraprese dal Richiedente";*
c) *conferma delle informazioni fornite all'Organismo di Certificazione utilizzate per l'esame della domanda;*
d) *la conferma del raggiungimento degli obiettivi di audit*;
e) *una raccomandazione se concedere o meno la certificazione, insieme a eventuali condizioni od osservazioni*".[12]

8.7.2. Valutazione delle conclusioni

Per ogni audit, il Lead Auditor deve riassumere le sue conclusioni utilizzando la seguente gradazione:

A. **Conformità con lo Schema di Certificazione**: ciò consentirà di norma al Richiedente di beneficiare di una certificazione e di un'etichettatura formale Europrivacy;
B. **Conformità allo Schema di Certificazione, con aree di miglioramento**: ciò consentirà normalmente al Richiedente di beneficiare di una certificazione e di un'etichettatura Europrivacy formale, con l'impegno di affrontare e migliorare le aree di criticità identificate. L'inadempienza nell'affrontare le aree di miglioramento può comportare il mancato mantenimento della certificazione al successivo audit di sorveglianza;
C. **Non conformità da correggere prima della certificazione**: richiede che il Richiedente affronti le Non-Conformità prima che possa essere concessa una potenziale certificazione e fornisca un piano credibile di rimedio;
D. **Esistenza di un numero eccessivo di Non-Conformità:** questo porterà normalmente a un rifiuto formale della certificazione e alla fine del processo di certificazione. In tutti i casi, non è possibile concordare la certificazione senza aver risolto le Non-Conformità come richiesto.

[12] Vedere la clausola 9.5.3.1 della ISO/IEC 17021:2015.

9. Processo di revisione, decisione e pubblicazione

9.1. Processo di revisione

9.1.1. Obbligo di documentare i risultati prima della revisione

I Lead Auditor devono documentare le attività di valutazione, le prove e i risultati prima di presentare il loro rapporto per la revisione.

9.1.2. Processo di revisione

L'Organismo di Certificazione deve disporre di un processo per condurre una revisione efficace prima di prendere una decisione per la concessione della certificazione, l'espansione o la riduzione del campo di applicazione della certificazione, il rinnovo, la sospensione o il ripristino, o il ritiro della certificazione. L'Organismo di Certificazione deve verificare che:

a) le informazioni fornite dal Team di Audit sono sufficienti a soddisfare i requisiti e a coprire l'Ambito Normativo della certificazione;
b) per ogni Non-Conformità Maggiore, ha rivisto e concordato le azioni correttive;
c) per qualsiasi Non-Conformità minore rimanente, ha esaminato e accettato il piano di azioni correttive del Richiedente.

Se la revisione e la decisione di certificazione sono completate da persone diverse, le raccomandazioni per una decisione di certificazione devono essere documentate.

9.2. Decisione di certificazione

9.2.1. Requisiti e processo chiave della decisione di certificazione

Una volta completato il processo di revisione, l'Organismo di Certificazione deve prendere una decisione formale sulla certificazione. **Come richiesto dall'ISO, *"l'Organismo di Certificazione sarà responsabile e manterrà l'autorità per le sue decisioni relative alla certificazione"*;**[13] *"dovrà assegnare ad almeno una persona il compito di prendere la decisione di certificazione sulla base di tutte le informazioni relative alla valutazione, al suo riesame e a qualsiasi altra informazione pertinente".*[14] L'Organismo di Certificazione può anche delegare questa competenza al/i Reviewer.

L'Organismo di Certificazione deve garantire che:

- le **persone o i comitati che prendono le decisioni formali sulla certificazione**[15] **sono diversi da quelli che hanno effettuato gli** audit;
- la persona o le persone nominate per condurre la decisione di certificazione **abbiano un'adeguata competenza e comprensione dei** requisiti **dello Schema di Certificazione**;
- l'individuo o gli individui nominati per condurre la decisione di certificazione **sono *"impiegati da, o sotto contratto con l'Organismo di Certificazione***"[16].

9.2.2. Decisioni

Le decisioni sono prese dall'Organismo di Certificazione e possono portare a:

a) concedere o rifiutare la certificazione;
b) ampliare o ridurre il campo di applicazione della certificazione;
c) sospendere o ripristinare la certificazione;
d) revocare la certificazione o il rinnovo della stessa.

Il periodo di validità di un certificato non deve superare i tre anni, rinnovabili tramite ricertificazione.

[13] Sezione 7.6.1 della norma ISO/IEC 17065:2012.
[14] Sezione 7.6.2 della norma ISO/IEC 17065:2012.
[15] Come la concessione, il rifiuto, l'ampliamento o la riduzione del campo di applicazione, la sospensione o il ripristino della certificazione, il ritiro o il rinnovo della certificazione.
[16] O con un'entità sotto il controllo organizzativo dell'Organismo di certificazione che abbia requisiti equivalenti.

L'Organismo di Certificazione deve registrare e documentare le proprie decisioni di certificazione, comprese le richieste di informazioni complementari.

9.3. Consegna della certificazione senza o prima dell'Accreditamento

La certificazione formale GDPR richiede che l'Organismo di Certificazione ottenga l'accreditamento formale o l'accordo dell'Autorità di Controllo ai sensi dell'art. 43 del GDPR, in conformità alle linee guida dell'EDPB.

Tranne nei casi vietati dalla legge, l'Organismo di Certificazione può avviare ed eseguire le valutazioni prima di ricevere l'accreditamento formale o l'accordo. Tuttavia, la consegna di certificati formali ai sensi dell'art. 43 del GDPR richiede l'accordo o l'accreditamento da parte dell'autorità nazionale competente.

Le certificazioni volontarie rilasciate al di fuori dell'ambito di applicazione dell'Art. 43 del GDPR devono essere chiaramente differenziate ed evitare qualsiasi rischio di confusione con le certificazioni formali del GDPR.

9.4. Trasferimento dei Certificati

I certificati attivi possono essere trasferiti a un altro Organismo di Certificazione nel corso della loro validità attraverso la seguente procedura:

a) Il Richiedente deve compilare il modulo di richiesta del nuovo Organismo di Certificazione;
b) Il Richiedente deve fornire al nuovo Organismo di Certificazione l'accesso a tutta la documentazione pertinente del suo attuale ciclo di certificazione;
c) Il nuovo Organismo di Certificazione dovrà riesaminare la documentazione acceduta ed eseguire un audit di sorveglianza o di ricertificazione al fine di prendere una decisione sulla certificazione.

Il trasferimento deve rispettare la durata e la frequenza degli audit di sorveglianza del certificato trasferito.

9.5. Sospensione, revoca o riduzione del campo di applicazione della certificazione

9.5.1. Obbligo di rispettare le decisioni delle autorità

Comr richiesto dall'Art. 58 del GDPR, *"l'Organismo di Certificazione accetta le decisioni e gli ordini dell'Autorità di Controllo competente di revocare o non rilasciare certificazioni a un Richiedente se i requisiti per la certificazione non sono o non sono più soddisfatti".*

9.5.2. Procedura per la sospensione, la revoca e l'adattamento del campo di applicazione

L'Organismo di Certificazione deve disporre di una procedura trasparente per la sospensione o il ritiro dei certificati, o per il potenziale adattamento dell'Ambito Normativo e/o del Target of Evaluation. Ciò si applica in situazioni in cui un Richiedente non mantiene in modo persistente e grave la conformità ai requisiti dello Schema di Certificazione o si impegna in altre azioni, come violazioni contrattuali o attività che rischiano di ingannare terze parti. Esempi di motivi validi per sospendere, ritirare o modificare il campo di applicazione di un certificato sono, a titolo esemplificativo e non esaustivo:

a) il trattamento dei dati certificati del Richiedente non soddisfa in modo persistente o pieno i requisiti di certificazione, come ad esempio:
   - non aver affrontato adeguatamente le Non-Conformità identificate;
   - misure tecniche e organizzative insufficienti per la protezione dei dati personali;
b) le azioni o l'inazione irragionevole del Richiedente impediscono l'esecuzione degli audit di sorveglianza o di ricertificazione secondo la frequenza richiesta o come previsto;
c) Violazione dei termini dell'accordo di certificazione firmato, come ad esempio:
   - mancato pagamento di quote o fatture;
   - uso improprio del marchio di certificazione e/o del riferimento alla certificazione;
d) Il Richiedente richiede volontariamente la sospensione temporanea;
e) Prove ricevute che potrebbero influenzare lo stato del certificato, come ad esempio:

- prove di non conformità del trattamento certificato;
- prove di misure tecniche e organizzative non efficaci in caso di incidenti gravi.

9.5.3. Gestione della sospensione della certificazione

In caso di sospensione della certificazione, l'Organismo di Certificazione incarica una o più persone di formulare e comunicare al Richiedente le azioni necessarie per porre fine alla sospensione e ripristinare la certificazione in conformità allo Schema di Certificazione.

Queste persone devono avere una conoscenza e una comprensione sufficienti dei requisiti dello Schema di Certificazione e delle questioni in gioco per gestire il processo e risolvere la sospensione se vengono intraprese le azioni necessarie.

In caso di sospensione, la certificazione del trattamento del Richiedente è temporaneamente invalida.

L'Organismo di Certificazione deve specificare un termine entro il quale il Richiedente deve affrontare e risolvere il problema che ha causato la sospensione. Nella maggior parte dei casi, la sospensione non supera i sei mesi e può essere adattata.

Se il problema che ha causato la sospensione viene risolto dal Richiedente, la certificazione viene ripristinata. Tuttavia, se il problema non viene risolto dal Richiedente nei tempi stabiliti dall'Organismo di Certificazione, quest'ultimo ridurrà il campo di applicazione della certificazione o ritirerà la certificazione.

9.5.4. Adattamento e Riduzione dell'ambito di certificazione

Quando un Richiedente certificato ha persistentemente o gravemente mancato di soddisfare i requisiti di certificazione per parti specifiche del Target of Evaluation o dell'Ambito Normativo, l'Organismo di Certificazione può prendere in considerazione la possibilità di modificarli e ridurli al fine di escludere le parti che non soddisfano i requisiti, a condizione che:

a) qualsiasi riduzione sarà in linea con i requisiti di Europrivacy;
b) il Target of Evaluation e l'Ambito Normativo modificati non devono essere fuorvianti e devono essere sufficientemente coerenti e comprensibili per i terzi e per il pubblico.

9.5.5. Obbligo di aggiornare i documenti e le informazioni di certificazione

Se una certificazione viene terminata, sospesa o ritirata, ripristinata o ridotta nel campo di applicazione, l'Organismo di Certificazione deve:

a) intraprendere le azioni specificate dallo Schema di Certificazione;
b) **se necessario, informare l'Autorità di Controllo competente e/o l'autorità nazionale di accreditamento**[17];
c) garantire che la decisione sia comunicata chiaramente al Richiedente;
d) chiedere al Richiedente di conformarsi alla decisione e di adeguare di conseguenza la sua comunicazione;
e) apportare tutte le modifiche e gli aggiornamenti necessari ai documenti formali di certificazione, alle informazioni pubbliche, alle autorizzazioni all'uso dei marchi, ecc.
f) aggiornare il Registro dei certificati Europrivacy.

Il lavoro svolto dall'Organismo di Certificazione per conformarsi allo Schema di Certificazione sarà a carico del Richiedente.

9.5.6. Cessazione

L'Organismo di Certificazione può decidere di interrompere il processo di certificazione in casi quali:

a) non sono state soddisfatte le condizioni per eseguire un processo di certificazione affidabile;
b) il Richiedente ha fornito informazioni fuorvianti o non ha collaborato;
c) il Richiedente e l'Organismo di Certificazione decidono congiuntamente di interrompere il processo di certificazione.

[17] In caso di ritiro o sospensione, l'Organismo di Certificazione dovrà anche fornire le motivazioni della sua decisione.

In caso di cessazione, anche prematura, l'Organismo di Certificazione dovrà completare il lavoro relativo alla decisione (come ad esempio la segnalazione, la registrazione e la documentazione della decisione, l'aggiornamento del Registro online, ecc.) e il Richiedente deve coprire i relativi costi giustificati.

9.6. Notifica e documentazione della certificazione

9.6.1. Obbligo di informare l'Autorità di Controllo ai sensi dell'articolo 43

"L'articolo 43(1) richiede agli organismi di certificazione di informare la propria Autorità di Vigilanza prima di rilasciare o rinnovare le certificazioni, per consentire all'Autorità di Vigilanza competente di esercitare i propri poteri correttivi *ai sensi dell'articolo 58(2), lettera h). Inoltre, l'articolo 43, paragrafo 5, prevede che gli organismi di certificazione* ***forniscano all'Autorità di Controllo competente le ragioni della concessione o del ritiro della certificazione richiesta".*** Più in generale, secondo gli articoli 42 e 43 del GDPR, ***"l'Organismo di certificazione è tenuto a fornire all'Autorità di Controllo le informazioni (...) necessarie per monitorare l'applicazione del meccanismo di certificazione."*** (Linee guida EDPB 1/2018)

9.6.2. Notifica della decisione di certificazione

L'Organismo di Certificazione deve notificare al Richiedente la decisione di concedere o meno la certificazione.
Se la certificazione non viene concessa, deve identificare e informare il Richiedente delle ragioni della decisione.

9.6.3. Requisiti preliminari alla consegna della documentazione di certificazione

Prima di rilasciare la documentazione di certificazione, l'Organismo di Certificazione deve assicurarsi che:

a) il processo di certificazione è stato documentato e registrato dall'Organismo di Certificazione;
b) è stata presa la decisione di concedere o estendere l'ambito della certificazione;
c) i requisiti di certificazione sono stati soddisfatti, compreso il pagamento della tassa per il certificato allo Scheme Owner;
d) l'accordo di certificazione è stato completato e firmato dal Richiedente.

Prima di consegnare una certificazione, i Richiedenti devono aver accettato espressamente di conformarsi ai requisiti dello Schema di Certificazione e alle Condizioni Generali di Europrivacy.

Una volta soddisfatte le condizioni di cui sopra, l'Organismo di Certificazione dovrà:

a) registrare la certificazione nel Registro dei Certificati di Europrivacy;
b) trasmettere la documentazione di certificazione al proprio Richiedente.

9.6.4. Contenuto della documentazione di certificazione

La documentazione di certificazione deve identificare quanto segue:

a) **il nome e l'indirizzo del** Richiedente **certificato**;
b) **il nome e l'identificazione del Target of Evaluation certificato**, compresi la versione e/o il modello, se applicabile;
c) una **breve descrizione del Target of Evaluation**, che includa:
   - il tipo di attività di trattamento;
   - se pertinente, l'ambito geografico della certificazione;
d) se il Richiedente agisce in qualità di **Titolare del trattamento, di Responsabile del trattamento o di Contitolare del trattamento**;
e) se del caso, il nome **del/i contitolare/i del trattamento**;
f) ove applicabile, qualsiasi Estensione o Adattamento applicato alla certificazione;
g) le **date di rilascio e di scadenza**, comprese, se del caso, le date di espansione o riduzione del campo di applicazione della certificazione, o di rinnovo della certificazione;
h) **la** data **di scadenza**;
i) un **codice di identificazione univoco** del certificato;
j) **il logo o il marchio di conformità Europrivacy**, a condizione che il suo utilizzo non sia fuorviante o ambiguo;

k) il riferimento alla **versione dello Schema di Certificazione** (data di revisione o numero di versione) utilizzata per la certificazione;
l) il **nome e l'indirizzo dell'**Organismo **di Certificazione**;
m) il **nome, il titolo e la firma della persona o delle persone che hanno preso la decisione di certificazione** o che hanno presieduto l'organo che ha preso la decisione.
n) se applicabile, un mezzo per distinguere i documenti rivisti da eventuali documenti obsoleti precedenti.

La documentazione di certificazione può assumere la forma di un certificato, come specificato nella Sezione 15.6.4, a condizione che includa i contenuti sopra menzionati.

Lo Scheme Owner può richiedere una copia elettronica del documento di certificazione consegnato e firmato.

9.7. Registro dei Certificati Europrivacy

***"Gli Organismi di Certificazione accreditati devono rendere pubblico in modo permanente e continuo quale certificazione è stata effettuata su quale base (o meccanismi o schema di certificazione), per quanto tempo le certificazioni sono valide in quale quadro e condizioni."* (EDPB)**

Per essere valido, un certificato Europrivacy deve essere registrato e pubblicato nel Registro ufficiale online dei certificati Europrivacy, gestito dallo Scheme Owner. L'Organismo di Certificazione deve registrare e aggiornare le informazioni nel Registro ufficiale.

9.7.1. Informazioni pubbliche incluse nel Registro dei certificati Europrivacy

Il Registro dei certificati Europrivacy rilasciati conterrà almeno le seguenti informazioni sull'avvenuta certificazione:

a) il nome del Richiedente;
b) il nome del Target of Evaluation e, se del caso, il suo modello e/o versione;
c) la descrizione del Target of Evaluation e le potenziali esclusioni dall'ambito;
d) il riferimento allo schema di certificazione e ai criteri (compresa la versione) in base ai quali è stata certificata la conformità;
e) i metodi di valutazione e i test condotti per la valutazione dei criteri (valutazione in loco, revisione della documentazione, test tecnici, ecc.;
f) la sintesi dei risultati della valutazione;
g) l'identificazione dell'Organismo di Certificazione;
h) la data di emissione, rinnovo e cessazione del certificato;
i) la durata di validità del certificato.

Nel Registro possono essere memorizzate informazioni aggiuntive per supportare il processo di convalida da parte dell'Autorità di Controllo e per migliorare lo Schema di Certificazione.

9.7.2. Informazioni private fornite allo Scheme Owner

Su richiesta, l'Organismo di Certificazione fornirà allo Scheme Owner le seguenti informazioni:

a) una copia dei rapporti di certificazione in formato pdf;
b) un file pdf del documento di certificazione con la firma della/e persona/e autorizzata/e;
c) il numero di ore di lavoro addebitate al Richiedente per la valutazione;
d) se, considerando le dimensioni e la complessità del Target of Evaluation, il tempo di audit calcolato fosse sufficiente e adeguato per completare una valutazione pienamente affidabile;
e) suggerimenti per migliorare lo Schema di Certificazione e/o l'elenco delle verifiche e dei controlli.

9.7.3. Informazioni aggiuntive che devono essere conservate dall'Organismo di Certificazione

L'Organismo di Certificazione deve mantenere tutta la documentazione relativa alla certificazione effettuata *"completa, comprensibile, aggiornata e idonea all'audit"*, incluso quanto segue:

a) il modulo di domanda e le informazioni;
b) l'accordo contrattuale per la certificazione;
c) se applicabile, i programmi di audit;

d) la giustificazione della determinazione del tempo del revisore;
e) la verifica della correzione e delle azioni correttive;
f) la documentazione delle decisioni di certificazione;
g) la documentazione pertinente per dimostrare la credibilità della certificazione, compresa l'evidenza della competenza degli Auditor e degli Esperti Tecnici;
h) se e dove applicabile:
   - i rapporti di audit di sorveglianza iniziale e di (ri)certificazione;
   - la giustificazione della metodologia utilizzata per il campionamento dei siti;
   - le registrazioni dei reclami e dei ricorsi e qualsiasi correzione o azione correttiva successiva;
   - i documenti di certificazione precedenti, compreso il Target of Evaluation;
   - le delibere e le decisioni del comitato.

9.7.4. Accesso al registro da parte dell'Autorità di Controllo

Ai sensi dell'articolo 43 del GDPR, l'Autorità di Controllo competente ha accesso alle informazioni private trasmesse allo Scheme Owner e/o archiviate nel Registro.

10. Mantenimento e rinnovo della certificazione

Le misure di monitoraggio regolari sono obbligatorie per il mantenimento della certificazione. Il periodo di monitoraggio di ciascuna certificazione deve essere documentato.

10.1. Mantenimento della certificazione - Principi Generali

In linea di principio, la certificazione Europrivacy viene concessa per periodi rinnovabili di tre anni. In questo periodo di tempo, il **Richiedente si impegna a**:

- **garantire la conformità dei propri Target of Evaluation certificati ai requisiti e ai Criteri dello Schema di Certificazione applicabili; e**
- **informare l'Organismo di Certificazione di qualsiasi cambiamento o preoccupazione in merito alla sua conformità**.

L'Organismo di Certificazione manterrà la certificazione sulla base della dimostrazione che il Richiedente continua a rispettare i requisiti dello Schema di Certificazione. **Le attività di monitoraggio e sorveglianza devono essere pienamente supportate dal Richiedente**.

L'identificazione di qualsiasi Non Conformità Maggiore comporterà la sospensione e il potenziale ritiro della certificazione. Se un Richiedente non si conforma ai requisiti dello Schema di Certificazione (come le attività di Sorveglianza, il pagamento delle quote, ecc.), il certificato viene sospeso o ritirato dall'Organismo di Certificazione. Tale decisione può essere eseguita anche dallo Scheme Owner e/o da un'Autorità di Controllo, ove applicabile.

10.1.1. Ciclo del Processo di Certificazione

Il ciclo di certificazione iniziale inizia alla data della decisione di certificazione e termina alla data di scadenza della certificazione. Le certificazioni e le ricertificazioni completate con successo devono essere seguite da:

a) un primo Audit di Sorveglianza entro 12 mesi dalla data di certificazione;
b) un secondo Audit di Sorveglianza entro 24 mesi dalla data di certificazione;
c) se applicabile, un Audit di Ricertificazione entro 36 mesi dalla data di certificazione.

Una ricertificazione completata con successo prima della fine del periodo di certificazione apre un nuovo ciclo di 36 mesi per la certificazione. Se la decisione di ricertificazione viene adottata negli ultimi tre mesi prima della data di scadenza del certificato precedente, la data di inizio del nuovo certificato può essere stabilita nella data successiva alla data di scadenza del certificato precedente.

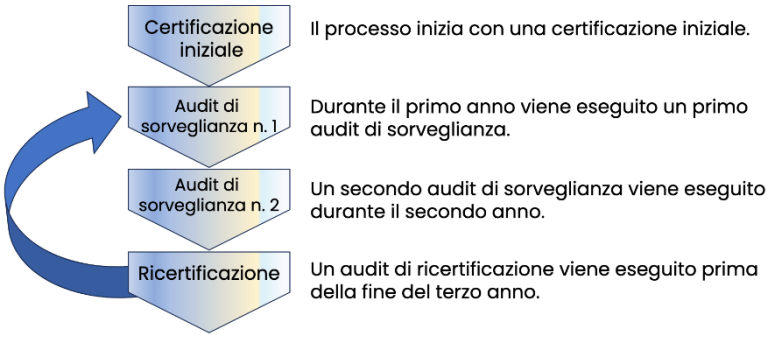

Figura 7 Ciclo di Certificazione

10.1.2. Audit di Monitoraggio e Sorveglianza

Le attività di monitoraggio vengono eseguite per determinare se il Target of Evaluation del Richiedente continua a soddisfare i requisiti dello Schema di Certificazione tra gli audit di ricertificazione.

L'Organismo di Certificazione deve pianificare e sviluppare le proprie attività di monitoraggio e sorveglianza su base annuale, in modo da monitorare regolarmente i principali requisiti di protezione dei dati applicabili al Target of Evaluation.

Gli audit di sorveglianza possono essere in loco e/o da remoto, sulla base di strumenti e metodologie adeguati.

10.1.3. Priorità delle Attività di Sorveglianza

Le Attività di Sorveglianza non richiedono la rivalutazione di tutti i criteri, ma si concentrano più specificamente su:

a) **una revisione degli audit interni, dei report di valutazione** (ad esempio, valutazione del rischio, valutazione d'impatto sulla protezione dei dati, ecc.), e una revisione del top management da parte del Richiedente dopo l'ultima valutazione;
b) **una revisione dello stato di avanzamento dei lavori e delle azioni intraprese dal Richiedente** su:
   - le Non Conformità identificate durante l'audit precedente;
   - i requisiti normativi e regolamentari cambiati rispetto all'ultima valutazione;
   - la gestione dei reclami;
   - le attività previste per lo sviluppo delle capacità e il miglioramento continuo;
c) **una valutazione** in merito a:
   - la continuità della liceità del trattamento dei dati;
   - l'efficacia delle misure adottate per rispettare i diritti degli interessati;
   - l'efficacia delle Misure Tecniche e Organizzative;
   - l'uso efficace di archivi e registri;
   - la continuità del controllo operativo;
   - l'uso e la comunicazione adeguati di marchi e altri riferimenti alla certificazione;
d) **la revisione di eventuali modifiche al trattamento dei dati oggetto del Target of Evaluation.**

L'Organismo di Certificazione deve selezionare un insieme di verifiche e controlli da verificare durante l'Audit di Sorveglianza. Inoltre, dovrà applicare lo specifico elenco di verifiche e controlli complementari per l'Audit di sorveglianza (*"S – Complementary Surveillance Checks and Controls "*).

10.1.4. Modifiche che riguardano la Certificazione

Le modifiche alla normativa applicabile in materia di protezione dei dati, quali revisioni legislative, decisioni di tribunali nazionali o sovranazionali, decisioni dell'EDPB o decisioni della Commissione europea, devono essere monitorate e prese in considerazione dall'Organismo di Certificazione. Se tali modifiche hanno un impatto sulle certificazioni rilasciate, l'Organismo di Certificazione deve:

1. Valutare il livello di impatto sulla validità della certificazione;
2. Elaborare un Piano d'Azione che specifichi:
   - i cambiamenti normativi identificati;
   - i certificati identificati;
   - le misure di adattamento proposte, quali: rivalutazione mirata, periodo di transizione, sospensione, revoca, ecc;
3. Se del caso, contattare l'Autorità di Controllo competente e richiedere la convalida del Piano d'Azione proposto;
4. Attuare il Piano d'Azione dopo che è stato approvato dall'Autorità di Controllo.

10.2. Ricertificazione

I certificati Europrivacy hanno una durata di tre anni e richiedono una valutazione di ricertificazione per essere rinnovati.

10.2.1. Informazioni per la Concessione della Ricertificazione

La decisione di rinnovare una certificazione si baserà sui risultati della valutazione di ricertificazione, comprese le misure adottate dal Richiedente per mantenere la conformità del Target of Evaluation e, se del caso, i reclami ricevuti in merito a tale conformità.

10.2.2. Attività di Ricertificazione (Rinnovo della Certificazione)

Lo scopo di una ricertificazione è quello di confermare la continua conformità del Target of Evaluation ai requisiti della certificazione Europrivacy. **La ricertificazione deve esaminare e prendere in considerazione le conclusioni dei precedenti report di audit** del ciclo di certificazione più recente.

11. Estensione dell'Ambito di Certificazione

Lo Schema di Certificazione può essere esteso per affrontare ambiti complementari in due modi:

a) Estensioni dei criteri di certificazione;
b) Adattamenti del campo di applicazione e dello Schema di Certificazione Europrivacy.

11.1. Estensioni dei criteri di certificazione Europrivacy

Il Richiedente può richiedere di estendere l'iniziale ambito normativo della certificazione GDPR, per valutare la conformità a normative nazionali complementari non UE sulla protezione dei dati o ad altre normative europee. Lo Scheme Owner identifica e specifica ogni Estensione in un documento separato con i corrispondenti criteri complementari che devono essere valutati dall'Organismo di Certificazione. Tutte le Estensioni dei criteri sono disponibili sul sito web di Europrivacy Resources and Community: https://community.europrivacy.com

11.1.1. Adattamento dei tempi e degli sforzi di audit

Il tempo e lo sforzo della valutazione saranno adeguati di conseguenza, in proporzione al numero di criteri aggiuntivi richiesti dall'Estensione, rispetto al numero regolare di criteri da valutare senza Estensione. Ad esempio, se una normale certificazione Europrivacy del Target of Evaluation richiede la valutazione di 50 criteri e il Richiedente vuole estendere la certificazione a un regolamento nazionale che richiede l'aggiunta di 5 criteri al processo di valutazione, il costo della certificazione deve essere aumentato del 10%.

11.1.2. Impatto sui marchi di conformità

Un'estensione dei criteri consente di fornire una doppia certificazione:

a) una certificazione di conformità ai criteri regolari;
b) una seconda certificazione di conformità secondo i criteri aggiuntivi.

Ciascuna di esse viene comunicata con un diverso marchio di conformità che viene specificato dal Scheme Owner.

11.2. Adattamenti dello Schema di Certificazione Europrivacy

Nelle giurisdizioni extra-UE, la certificazione in materia di protezione dei dati può essere adattata a diverse attività, come i sistemi di gestione della protezione dei dati personali. Europrivacy consente di affrontare questi casi adattati attraverso gli Adattamenti dello Schema di Certificazione, che specificano regole e requisiti complementari che devono essere applicati dall'Organismo di Certificazione. Gli adattamenti dello Schema di Certificazione sono elencati nell'Elenco degli Adattamenti dello Schema di Certificazione Europrivacy e sono disponibili sul sito web di Europrivacy Community: https://community.europrivacy.com

Dal punto di vista dell'accreditamento, un adattamento dello Schema di Certificazione è considerato come uno Schema di Certificazione distinto e viene comunicato con un marchio di conformità diverso che deve essere specificato dallo Scheme Owner.

12. Requisiti strutturali e organizzativi

12.1. Struttura organizzativa e Top Management

In linea con le norme e i principi della ISO/IEC 17065, l'Organismo di Certificazione deve documentare la propria struttura organizzativa, tra cui:

a) i ruoli e le responsabilità del personale coinvolto nelle attività di certificazione.
b) l'identificazione della top management authority per:
   - sviluppare e supervisionare:
     - sistema di gestione dell'Organismo di Certificazione;
     - requisiti di certificazione;
   - politiche, processi e procedure relative alla certificazione;
   - attività di certificazione;
   - valutare, monitorare e garantire l'adeguatezza:
     - requisiti di competenza del personale;
     - prestazioni e capacità di rispondere a reclami e ricorsi;
     - allocazione delle risorse per le attività di certificazione;
   - prendere decisioni in merito a:
     - valutazione e revisione delle certificazioni;
     - decisione formale sulla certificazione;
   - delega di autorità a comitati o individui;
     - accordi contrattuali.

12.1.1. Funzione di responsabile della protezione dei dati

L'Organismo di Certificazione deve avere una persona o un ufficio designato per garantire la conformità interna alle norme sulla protezione dei dati, compresi i compiti relativi alla funzione del responsabile della protezione dei dati.

12.1.2. Controllo operativo

In conformità ai requisiti ISO, l'Organismo di Certificazione che lavora con filiali e/o terze parti deve stabilire un processo appropriato per monitorare e controllare le attività di certificazione svolte per suo conto.

12.2. Alcuni ruoli e responsabilità chiave

12.2.1. Responsabilità esclusiva del Richiedente

È il Richiedente certificato (e non l'Organismo di Certificazione) ad avere la responsabilità di soddisfare e rispettare i requisiti di certificazione. La conformità legale rimane di sola ed esclusiva responsabilità del Richiedente, che dovrà garantire che il proprio Target of Evaluation certificato sia pienamente conforme ai requisiti dello Schema di Certificazione e, più in generale, alle normative applicabili in materia di protezione dei dati.

12.2.2. Ruolo e responsabilità dell'Organismo di Certificazione

L'Organismo di Certificazione ha la responsabilità di raccogliere e valutare sufficienti evidenze di audit su cui basare una decisione di certificazione in conformità allo Schema di Certificazione. In base alle conclusioni dell'audit, l'Organismo di Certificazione deciderà di concedere la certificazione se le prove di conformità sono sufficienti, o di non concederla se le prove di conformità sono insufficienti.

Nei limiti previsti dalla legge, l'Organismo di Certificazione non è responsabile di perdite o danni di qualsiasi tipo e natura derivanti dall'uso del prodotto, processo, servizio o sistema di gestione certificato.

12.2.3. Ruolo dello Scheme Owner

Lo Scheme Owner è responsabile della manutenzione e dell'aggiornamento dello Schema di Certificazione, nonché della consegna, della sospensione e della revoca della licenza Europrivacy agli Organismi di Certificazione. Lo Scheme Owner è anche responsabile della gestione del Registro dei Certificati Europrivacy e delle informazioni pubbliche sullo Schema di Certificazione. Non è responsabile delle decisioni di certificazione (che sono di competenza dell'Organismo di Certificazione competente), né della continua

conformità del Target of Evaluation alle normative sulla protezione dei dati (che è di esclusiva responsabilità del Richiedente).

I diritti e le competenze dello Scheme Owner devono essere riconosciuti e garantiti negli obblighi contrattuali che vincolano l'Organismo di Certificazione e i suoi Richiedenti.

12.2.4. Ruolo dell'Autorità di Controllo

Ai sensi dell'art. 43 del GDPR, le Autorità di Controllo sono incaricate di supervisionare e controllare la conformità del processo di certificazione al GDPR.

12.3. Questioni legali e contrattuali

Come richiesto dalla ISO/IEC 17065, l'Organismo di Certificazione deve essere una persona giuridica legalmente responsabile delle proprie attività di certificazione.

12.3.1. Accordo di certificazione con il Richiedente

L'Organismo di Certificazione adotterà un accordo (o una serie di accordi) legalmente vincolante con ciascun Richiedente per la fornitura di attività di certificazione in conformità ai requisiti pertinenti dello Schema di Certificazione. Gli accordi di certificazione devono chiarire le responsabilità dell'Organismo di Certificazione e dei suoi Richiedenti e devono essere applicati a tutti i siti del Richiedente che sono rilevanti per il campo di applicazione della certificazione.

12.3.2. Requisiti chiave dell'accordo di certificazione

In conformità ai requisiti ISO, l'accordo di certificazione deve includere almeno i seguenti obblighi per il Richiedente:

a) Il Richiedente **si impegna a rispettare i requisiti dello Schema di Certificazione e i relativi termini e condizioni. Dovrà garantire che i Target of Evaluation certificati siano conformi ai Criteri e alle normative applicabili in materia di protezione dei dati**. Dovrà:
   - **impegnarsi a rispettare le scadenze e le procedure applicabili,** anche per quanto riguarda gli audit di sorveglianza e i pagamenti delle fatture relative a audit e certificazione (indipendentemente dalla decisione sulla certificazione);
   - **riconoscere la propria piena ed esclusiva responsabilità** per il rispetto dei requisiti dello Schema di Certificazione e delle normative applicabili in materia di protezione dei dati;
   - **riconoscere che la certificazione non riduce la propria responsabilità** in relazione alle normative vigenti in materia di protezione dei dati.

b) Il Richiedente deve **adottare tutte le misure necessarie per sostenere il lavoro dell'Organismo di Certificazione**, tra cui:
   - consentire la piena trasparenza e l'accesso a tutte le attività di trattamento, ai siti, ai locali, ai processi, alle procedure, alle informazioni, ai dati e al personale necessari per condurre la certificazione prevista;
   - sostenere la conduzione delle attività di valutazione e monitoraggio, anche fornendo guide e adottando disposizioni per l'accesso e l'esame della documentazione, dei registri, delle attrezzature, dei luoghi, delle aree, del personale e dell'accesso ai subappaltatori del Richiedente, come Responsabile del Trattamento;
   - registrare e indagare su eventuali reclami relativi alla sua certificazione;
   - sostenere la partecipazione di Observer, se del caso.

c) Il Richiedente deve **fornire informazioni chiare, complete e trasparenti** all'Organismo di Certificazione (e, se richiesto, all'Autorità di Controllo competente) senza omettere alcuna informazione rilevante per il processo di certificazione.

d) Il Richiedente dovrà **adottare tutte le misure necessarie per mantenere la conformità** del/dei Target of Evaluation certificati allo Schema di Certificazione e ai suoi Criteri, anche:
   - implementando le modifiche appropriate quando vengono comunicate dall'Organismo di Certificazione;
   - garantendo che la produzione, l'erogazione di servizi e/o l'attività certificata in corso continuino a soddisfare i relativi requisiti del prodotto e dello Schema di Certificazione.

e) Il Richiedente deve **evitare qualsiasi comunicazione fuorviante** e qualsiasi uso fuorviante del marchio di conformità. In particolare, il Richiedente:
   - dovrà fare affermazioni solo in merito alla certificazione che siano coerenti con:
     - l'ambito della certificazione conseguita e in corso di validità;
     - le istruzioni e le linee guida scritte fornite dall'Organismo di Certificazione;
   - non potrà utilizzare o comunicare la propria certificazione in alcun modo che:
     - possa essere percepito come fuorviante da terzi;
     - possa danneggiare o screditare l'Organismo di Certificazione o lo Schema di Certificazione;
   - dovrà rispettare i requisiti dell'Organismo di Certificazione e dello Schema di Certificazione per la comunicazione della propria certificazione, comprese le informazioni relative al Target of Evaluation[18];
   - dovrà rispettare le regole specificate dallo Scheme Owner per l'utilizzo di logo, certificati e marchi di conformità.

f) Il Richiedente *"**dovrà informare l'Organismo di Certificazione, senza ingiustificato ritardo, di qualsiasi cambiamento che possa influire sulla sua conformità allo Schema di Certificazione**"*[19], anche in caso di incidenti come le violazioni di dati.

g) **In caso di sospensione, ritiro o cessazione di una certificazione, il Richiedente dovrà:**
   - **smettere di utilizzare e comunicare la relativa certificazione**;
   - **adempiere senza ingiustificato ritardo ai corrispondenti obblighi** specificati nello Schema di Certificazione e alle istruzioni ricevute dall'Organismo di Certificazione.

h) Il Richiedente deve **registrare tutti i reclami** ricevuti e **documentare le azioni di follow-up.**

i) Il Richiedente **deve accettare qualsiasi audit, campionamento o altra indagine supplementare o aggiuntiva** che l'Organismo di Certificazione possa ritenere necessaria per il processo di certificazione o per il mantenimento continuo della certificazione;

j) Il Richiedente **deve riconoscere e accettare che i risultati possono avere un impatto sul processo di certificazione**, tra cui:
   - rinvio o annullamento del processo di certificazione;
   - nel caso di non conformità significative o di modifiche che impattano sul trattamento nell'ambito del Target of Evaluation, l'Organismo di Certificazione può dover ripetere parte o tutto il processo di certificazione;
   - l'Organismo di Certificazione potrebbe anche dover rivedere i propri accordi e la stima dei costi.

k) Il Richiedente **farà riferimento alla certificazione Europrivacy e utilizzerà il marchio di conformità e l'etichettatura Europrivacy solo dopo aver ricevuto il certificato Europrivacy** e in conformità alle regole d'uso specificate dallo Scheme Owner;

l) Se il Richiedente fornisce copie dei documenti di certificazione a terzi, i documenti devono essere riprodotti integralmente o come specificato nello Schema di Certificazione.

m) Il Richiedente accetta che le informazioni fornite per il processo di certificazione siano accessibili allo Scheme Owner, sotto il sigillo della riservatezza, allo scopo di controllare, rivedere o aggiornare il processo di certificazione; gli stessi diritti sono applicabili all'Autorità di accreditamento dell'Organismo di Certificazione.

n) **L'Accordo chiarisce:**
   - **le regole di validità, rinnovo e ritiro della certificazione**;
   - **la struttura e la procedura per i reclami e i ricorsi;**
   - **le misure da adottare per soddisfare le esigenze dei clienti in caso di sospensione o revoca dell'accreditamento dell'Organismo di Certificazione.**

[18] Vedi anche ISO/IEC 17030, Guida ISO/IEC 23 e Guida ISO 27.

[19] Si veda la clausola 4.1.2.2, punto k della ISO/IEC 17065:2012. Esempi di tali modifiche sono: cambiamenti nel sistema di produzione o di gestione; cambiamenti *"nello status giuridico, commerciale, organizzativo o nella proprietà; nell'organizzazione e nella gestione (ad esempio, personale manageriale, decisionale o tecnico chiave); modifiche al prodotto o al metodo di produzione; indirizzo di contatto e siti di produzione; modifiche importanti al sistema di gestione della qualità".*

12.3.3. Responsabilità per le decisioni sulla certificazione

In linea con i principi ISO, **l'Organismo di Certificazione è responsabile e mantiene l'autorità per le sue decisioni relative alla certificazione**, tra cui la concessione, il rifiuto, il mantenimento della certificazione, l'espansione o la riduzione del campo di applicazione della certificazione, il rinnovo, la sospensione o il ripristino a seguito di sospensione, o il ritiro della certificazione.

Lo Scheme Owner non ha l'obbligo di monitorare attivamente le singole certificazioni e/o i Target of Evaluation certificati per verificare la presenza di Non Conformità. Tuttavia, se allo Scheme Owner viene fornita l'evidenza che un Target of Evaluation certificato presenta gravi Non Conformità e l'Organismo di Certificazione non ha proceduto rapidamente alla revisione e all'intervento sul caso, lo Scheme Owner si riserva il diritto di indagare e di sospendere e/o ritirare unilateralmente qualsiasi certificato concesso.

13. Gestione dell'imparzialità e dei rischi

13.1. Dovere di imparzialità

L'Organismo di Certificazione deve dimostrare la propria indipendenza e di disporre di procedure atte a prevenire conflitti di interesse con la certificazione da rilasciare.

Il processo di certificazione deve essere intrapreso in modo imparziale. **L'Organismo di Certificazione non deve avere alcun rapporto precedente o attuale con il Richiedente che possa compromettere la sua imparzialità.**

L'Organismo di Certificazione e il suo Top Management *sono "responsabili dell'imparzialità dei loro processi di certificazione e non devono permettere che pressioni commerciali, finanziarie o di altro tipo compromettano la loro imparzialità*".[20]

All'Organismo di Certificazione può essere richiesto di fornire prova della propria indipendenza all'Autorità di Controllo competente.

13.2. Meccanismo di salvaguardia dell'imparzialità

13.2.1. Ruolo e funzione del meccanismo di salvaguardia dell'imparzialità

Come richiesto dalla ISO, "l'Organismo di Certificazione ***deve disporre di un Meccanismo per salvaguardare la propria imparzialità.***[21] **Lo scopo del meccanismo è** quello di rafforzare l'imparzialità dell'Organismo di Certificazione:

a) rivedendone e migliorandone la policy sull'imparzialità;
b) gestendo e fornendo indicazioni su qualsiasi conflitto di interesse potenziale o identificato che possa influire sull'imparzialità delle certificazioni.

Al Meccanismo possono essere assegnati ulteriori compiti e mansioni, purché compatibili con la funzione di garantire l'imparzialità.

13.2.2. Forma del Meccanismo di salvaguardia dell'imparzialità

Il meccanismo deve:

a) essere formalmente documentato;
b) garantire una composizione diversificata ed equilibrata dei membri;
c) avere accesso a tutte le informazioni necessarie per poter svolgere tutte le sue funzioni.

13.2.3. Composizione del Meccanismo

L'Organismo di Certificazione deve identificare e invitare le parti significativamente interessate. Tali parti interessate possono includere:

- esperti in protezione dei dati personali;
- ricercatori in materia di protezione dei dati;
- Richiedenti dell'Organismo di Certificazione;
- rappresentanti di enti normativi governativi come le Autorità di Controllo;
- clienti e/o utenti finali dei Richiedenti o dei Target of Evaluation certificati;
- esperti di valutazione della conformità;
- rappresentanti di organizzazioni non governative, come le organizzazioni dei consumatori;
- Auditors;
- Esperti Tecnici.

Si consiglia di avere nel meccanismo un insieme eterogeneo di rappresentanti che rappresentino diversi settori, in modo che non prevalga un singolo interesse. Il personale interno o esterno dell'Organismo di Certificazione è considerato un unico interesse.

[20] Clausola 4.2.2 della ISO/IEC 17065:2012
[21] Clausola 5.2.1 della ISO/IEC 17065:2012

13.2.4. Impatto degli input del Meccanismo sulla decisione dell'Organismo di Certificazione

Per impostazione predefinita, l'Organismo di Certificazione deve prendere in considerazione e seguire gli input e le indicazioni fornite dal Meccanismo.

Tuttavia, gli input che sono in conflitto con le procedure operative dell'Organismo di Certificazione o con altri requisiti obbligatori non devono essere seguiti. Allo stesso modo, gli input che avrebbero un impatto sproporzionato sull'efficienza o sull'efficacia del processo di certificazione non devono essere seguiti o adattati per mitigare gli effetti negativi. Il Management dovrà documentare le motivazioni alla base della decisione di non seguire l'input fornito e dovrà conservare il documento per la revisione da parte dello Scheme Ownere/o dell'Autorità di Controllo competente.

13.3. Processo di identificazione e risoluzione dei conflitti di interesse

L'Organismo di Certificazione deve avere un processo per identificare, analizzare, valutare, trattare, monitorare e documentare i rischi relativi ai conflitti di interesse derivanti dalle sue attività di certificazione, compresi i conflitti derivanti dalle sue relazioni o dalle relazioni del suo personale.

13.3.1. Esempi di minacce all'imparzialità

Le minacce all'imparzialità possono assumere diverse forme, come ad esempio:

- Interessi personali, compreso qualsiasi interesse economico o in natura legato al risultato della certificazione;
- Auto-riesame del proprio lavoro, ad esempio quando un Organismo di Certificazione o un membro di un Team di Audit è stato coinvolto in attività di consulenza per il soggetto controllato;
- Familiarità e compiacenza che possono influire sull'affidabilità della valutazione;
- Minacce e intimidazioni;
- Relazioni, quali rapport commerciali, di proprietà o di committenza.

13.3.2. Limitazioni specifiche

Al fine di preservare la loro imparzialità, l'Organismo di Certificazione e gli Auditor non dovranno:

- fornire servizi di consulenza o di audit interno ai propri Richiedenti certificati22;
- certificare un Richiedente per il quale hanno fornito consulenza negli ultimi 24 mesi;
- certificare un Richiedente per il quale hanno effettuato un audit interno negli ultimi 24 mesi;
- essere coinvolti nello sviluppo, nella progettazione, nella produzione, nella distribuzione, nell'installazione, nell'implementazione, nel funzionamento o nello sfruttamento del trattamento dei dati da certificare;
- certificare altri Organismi di Certificazione.

Le limitazioni di cui sopra non impediscono all'Organismo di Certificazione:

- di condividere le informazioni con il Richiedente e chiarire i suoi risultati e i requisiti attesi (può spiegare in termini generici cosa ci si aspetta e cosa manca per soddisfare i requisiti, ma non può spiegare come risolvere le non conformità identificate);
- l'utilizzo, l'installazione e/o la manutenzione di un prodotto certificato a scopo di valutazione.

13.3.3. Rischi specifici legati agli audit interni

L'esecuzione di audit interni da parte di un Organismo di Certificazione per i propri Richiedenti certificati costituisce una minaccia all'imparzialità. Pertanto, **l'Organismo di Certificazione non deve offrire o fornire audit interni ai propri Richiedenti certificati**. Ciò vale per qualsiasi parte della stessa persona giuridica e per qualsiasi entità sotto il controllo organizzativo dell'Organismo di Certificazione.

[22] Si veda la clausola 3.2 della ISO/CEI 17065:2012 e la definizione 3.3 della ISO/IEC 17021:2011.

13.3.4. Rischi specifici legati alla consulenza

"L'Organismo di Certificazione e qualsiasi parte della stessa persona giuridica e qualsiasi entità sotto il controllo organizzativo dell'Organismo di Certificazione non devono offrire o fornire servizi di consulenza sui sistemi di gestione o servizi di consulenza simili in relazione al campo di applicazione della certificazione."[23]

Allo stesso modo, l'Organismo di Certificazione **non può esternalizzare gli audit a un'organizzazione che fornisce servizi di consulenza** in relazione al campo di applicazione della certificazione, in quanto ciò rappresenta una minaccia inaccettabile all'imparzialità dell'Organismo di Certificazione. Ciò non si applica alle persone ingaggiate come Auditor.

Il personale che ha fornito consulenza o che ha svolto funzioni manageriali per un Richiedente non può essere utilizzato dall'Organismo di Certificazione per partecipare alle attività di certificazione per quel Richiedente per un minimo di due anni dalla fine della consulenza.

13.3.5. Rischi associati alle persone giuridiche collegate

L'Organismo di Certificazione deve garantire che la sua imparzialità nella certificazione non sia compromessa da persone giuridiche ad esso collegate. Nel caso in cui una persona giuridica collegata all'Organismo di Certificazione fornisca consulenza[24] o sviluppi prodotti o servizi da certificare, il personale direttamente coinvolto nel processo di valutazione e decisione della certificazione non deve essere coinvolto nelle attività dell'altra persona giuridica e viceversa.

13.3.6. Indipendenza da società di consulenza

L'Organismo di Certificazione non deve promuovere un'attività di marketing congiunto o essere presentato come collegato a un'organizzazione che fornisce consulenza. L'Organismo di Certificazione deve intervenire per correggere qualsiasi riferimento o dichiarazione inappropriata da parte di qualsiasi organizzazione di consulenza che affermi o implichi che la certificazione sarebbe più semplice, più facile, più veloce o meno costosa se si decidesse di ricorrere all'Organismo di Certificazione.

Questa clausola non impedisce la partecipazione dell'Organismo di Certificazione ad attività congiunte di comunicazione e marketing organizzate dall'ECCP per promuovere collettivamente i servizi relativi a Europrivacy e l'ecosistema di partner di Europrivacy (compreso l'accesso ai loro servizi). L'ECCP può anche invitare i propri Organismi di Certificazione e Società di Consulenza autorizzati a collaborare, sostenere e promuovere lo Schema di Certificazione Europrivacy e l'ecosistema di fornitori di servizi qualificati.

13.4. Obblighi specifici relativi all'imparzialità

13.4.1. Obbligo di adottare una policy formale sull'imparzialità

L'Organismo di Certificazione deve adottare una policy formale e scritta sull'imparzialità che includa i seguenti elementi:

- un chiaro impegno e una dichiarazione del top management che sottolinei l'importanza dell'imparzialità nell'esercizio delle attività di certificazione;
- linee guida chiare su come gestire i conflitti di interesse e garantire l'obiettività delle proprie attività di certificazione;
- un processo per identificare, analizzare, valutare, trattare, monitorare e documentare i rischi legati ai conflitti di interesse derivanti dalle proprie attività di certificazione, compresi i conflitti derivanti dalle proprie relazioni o dalle relazioni del proprio personale[25].

La policy sull'imparzialità degli Organismi di Certificazione certificati deve essere accessibile allo Scheme Owner.

[23] Clausola 5.2.5 della ISO/IEC 17021-1:2015

[24] Vedere la clausola 3.2 della ISO/IEC 17065:2012.

[25] Si veda la clausola 4.2.12 della ISO/IEC 17065:2012 e la 4.2.1 della ISO/IEC 17021-1:2015; l'identificazione dei rischi non implica la valutazione dei rischi come indicato nella ISO 31000:2009.

13.4.2. Obblighi del personale in materia di imparzialità

Il personale dell'Organismo di Certificazione coinvolto nelle attività di certificazione deve preservare e proteggere l'imparzialità delle attività di certificazione. Deve informare l'Organismo di Certificazione di qualsiasi rischio o pressione identificati che possano influenzare l'imparzialità delle certificazioni.

"L'Organismo di Certificazione richiede al proprio personale, interno ed esterno, di rivelare qualsiasi situazione a loro nota che possa rappresentare per loro o per l'Organismo di Certificazione un conflitto di interessi. L'Organismo di Certificazione registra e utilizza queste informazioni come input per identificare le minacce all'imparzialità sollevate dalle attività di tale personale o dalle organizzazioni che lo impiegano, e non utilizzerà tale personale, interno o esterno, a meno che non possa dimostrare l'assenza di conflitti di interesse."[26]

13.4.3. Obbligo di documentare la gestione dell'imparzialità

Se l'Organismo di Certificazione identifica minacce all'imparzialità, deve documentare e dimostrare come elimina o riduce al minimo tali minacce e deve documentare qualsiasi rischio residuo. Deve valutare e affrontare le minacce interne ed esterne all'imparzialità.

Il Report di Monitoraggio dell'Imparzialità deve essere reso accessibile allo Scheme Owner.

13.4.4. Obbligo di agire su questioni di imparzialità

L'Organismo di Certificazione deve intervenire per affrontare qualsiasi rischio per la sua imparzialità. Ogni volta che viene identificato un rischio per la sua imparzialità, l'Organismo di Certificazione deve intervenire per eliminare il rischio o almeno per ridurlo a un livello considerato limitato e accettabile.

L'Organismo di Certificazione deve intraprendere azioni correttive e, se necessario, legali per rispondere a qualsiasi minaccia alla sua imparzialità derivante da azioni di altre persone, enti o organizzazioni.

Quando una relazione rappresenta una minaccia inaccettabile per l'imparzialità (come nel caso di una filiale interamente controllata dall'Organismo di Certificazione che richiede la certificazione della propria casa madre), la certificazione non deve essere fornita.

13.5. Gestione del rischio

13.5.1. Analisi dei rischi da parte dell'Organismo di Certificazione

Ogni volta che viene identificato un rischio che potrebbe avere un impatto negativo sull'imparzialità o sull'affidabilità del processo di certificazione, il top management deve essere informato e deve essere eseguita una valutazione del rischio. Il processo di valutazione del rischio può avvalersi di consultazioni con le opportune parti interessate per fornire consulenza su questioni che incidono sull'imparzialità, tra cui l'apertura e la percezione pubblica. Le consultazioni con le parti interessate devono essere equilibrate e non devono prevalere singoli interessi.[27]

Il top management deve riesaminare qualsiasi rischio residuo per determinare se rientra nel livello di rischio accettabile.

13.5.2. Approccio basato sul rischio per il Richiedente

L'Organismo di Certificazione deve tenere conto dei rischi associati alla fornitura di una certificazione competente, coerente e imparziale. **L'allocazione delle risorse e dei tempi deve tenere conto dei rischi identificati**.

Nell'esecuzione del processo di certificazione, si deve dare priorità alle questioni di audit che hanno una maggiore rilevanza e che costituiscono rischi più importanti per gli interessati.

13.5.3. Identificazione del rischio, responsabilità e finanziamento

L'Organismo di Certificazione dovrà dimostrare all'Organismo di Valutazione o all'Autorità di Controllo che:

- ha identificato, analizzato e valutato i rischi legati alle sue attività di certificazione;

[26] Clausola 5.2.13 della ISO/IEC 17021-1:2015

[27] Se applicabile, l'analisi dei rischi può essere delegata al Meccanismo di Imparzialità.

- ha adottato misure adeguate per coprire le responsabilità legate alle sue attività di certificazione nelle regioni in cui opera;
- le sue risorse finanziarie non lo espongono a pressioni economiche.

13.5.4. Limitazione del campo di applicazione

L'Organismo di Certificazione deve specificare chiaramente il campo di applicazione di ciascuna certificazione.

La procedura e le attività di certificazione devono concentrarsi e rimanere all'interno del campo di applicazione concordato della certificazione.

14. Gestione del personale e delle risorse

14.1. Competenze del personale

Come richiesto dall'EDPB, l'Organismo di Certificazione dovrà dimostrare di possedere competenze adeguate e continuative in materia di protezione dei dati, tra cui:

- **requisiti del RGPD;**
- **applicazione della normativa in materia di protezione dei dati;**
- **misure tecniche e organizzative di protezione dei dati.**

14.1.1. Definizione del personale

Il "personale dell'Organismo di Certificazione" si riferisce a tutti coloro che lavorano sotto l'autorità dell'Organismo di Certificazione o per mezzo di un accordo contrattuale.[28]

14.1.2. Obbligo di avere processi di gestione del personale

L'Organismo di Certificazione deve disporre di processi per garantire che il personale coinvolto nel processo di certificazione abbia conoscenze e competenze adeguate. Dovrà essere in grado di dimostrare di ricorrere ad Auditor e responsabili dei team di audit in possesso di competenze e conoscenze generiche in materia di audit, nonché di competenze e conoscenze appropriate per l'audit in aree tecniche specifiche.

L'Organismo di Certificazione deve chiarire a ogni persona interessata i propri compiti, responsabilità e autorità.

14.1.3. Criteri di competenza

I Criteri di Competenza del personale che certifica ai sensi dell'articolo 42 del GDPR devono essere conformi:

- **ai requisiti generali delle Linee guida EDPB per la certificazione;**
- **ai requisiti nazionali complementari applicabili all'Organismo di Certificazione.**

L'Organismo di Certificazione deve disporre di un processo per stabilire e valutare i criteri di competenza del personale coinvolto nelle attività di certificazione. Nella costituzione di un Team di Audit, i criteri di competenza devono tenere conto dei requisiti specifici del Target of Evaluation.

Il Lead Auditor incaricato di certificare le grandi imprese, le imprese distribuite in diversi Paesi o le imprese che trattano categorie speciali di dati dovrà avere un livello di competenza più elevato.

I criteri minimi di competenza sono dettagliati e specificati nel documento "Management of Competencies of Personnel Involved in Europrivacy Certification Process", che è un documento vincolante e deve essere rispettato dall'Organismo di Certificazione. Esso documenta i criteri delle conoscenze e delle competenze necessarie per svolgere i compiti di certificazione Europrivacy.

14.1.4. Requisiti di capacità del personale e competenze complementari

L'Organismo di Certificazione deve avere accesso ad Auditor ed Esperti qualificati in grado di applicare il presente Schema di Certificazione e di fornire una valutazione affidabile della conformità al GDPR e ad altre normative complementari applicabili in materia di protezione dei dati. L'Organismo di Certificazione deve avere accesso alle competenze tecniche necessarie per la consulenza su questioni direttamente correlate alle attività di certificazione per tutti i settori applicativi e le aree geografiche in cui l'Organismo di Certificazione opera. Tali competenze possono essere fornite dall'esterno.

14.1.5. Capacità dei Decisori

Coloro che sono coinvolti nelle decisioni di un processo di certificazione devono dimostrare di:

- comprendere lo Schema di Certificazione;
- sono in grado di valutare l'esito di un processo di audit.

[28] vedere la clausola 6.1.3 della ISO/IEC 17065:2012.

Il concetto di processo decisionale nella certificazione deve essere inteso in senso ampio e comprende la decisione di concedere, rifiutare, mantenere, rinnovare, sospendere, ripristinare una certificazione, nonché la decisione di modificare il campo di applicazione della certificazione.

14.1.6. Informazioni e documentazione fornite a Auditors ed Esperti

"L'Organismo di Certificazione deve garantire che gli Auditor (e, se necessario, gli Esperti Tecnici) siano a conoscenza dei propri processi di audit, dei requisiti di certificazione e di altri requisiti rilevanti. L'Organismo di Certificazione deve consentire agli Auditor e agli Esperti Tecnici l'accesso a un insieme aggiornato di procedure documentate che forniscano istruzioni per l'audit e tutte le informazioni rilevanti sulle attività di certificazione."[29]

14.2. Obblighi contrattuali del personale

14.2.1. Contratti con il personale

L'Organismo di Certificazione deve richiedere al proprio personale coinvolto nel processo di certificazione di firmare un contratto con il quale si impegna:

a) rispettare le regole specificate nello Schema di Certificazione;
b) per preservare la riservatezza delle informazioni a cui si accede;
c) per prevenire qualsiasi conflitto di interessi e dichiarare qualsiasi situazione o relazione che possa causare tali conflitti.

14.2.2. Obbligo di riservatezza del personale

Tutto il personale che agisce per conto dell'Organismo di Certificazione **deve mantenere riservate tutte le informazioni** ottenute o create durante il processo di certificazione, salvo che sia richiesto dalla legge o dalle disposizioni dello Schema di Certificazione.

14.3. Gestione delle competenze

14.3.1. Procedura per la gestione delle competenze

L'Organismo di Certificazione deve stabilire, attuare e mantenere una procedura e dei processi per la gestione delle competenze del personale coinvolto nella gestione e nell'esecuzione degli audit e delle altre attività di certificazione.[30]

L'Organismo di Certificazione deve rispettare i criteri di competenza del personale specificati dal presente Schema di Certificazione, nonché gli eventuali requisiti richiesti dall'Autorità di Controllo competente. L'Organismo di Certificazione può adottare criteri aggiuntivi per la competenza del personale in relazione ai requisiti dello Schema di Certificazione per ogni funzione del processo di certificazione. Ove pertinente, devono essere utilizzati requisiti specifici relativi alla competenza di un'area tecnica specifica. L'Organismo di Certificazione deve garantire la raccolta delle competenze richieste in materia di protezione dei dati.

Nell'ambito della gestione delle competenze, l'Organismo di Certificazione deve:

a) identificare e soddisfare le esigenze di formazione per garantire che il personale coinvolto nelle attività di certificazione sia competente a svolgere i propri compiti;
b) documentare e dimostrare che il proprio personale possiede le competenze richieste per svolgere i propri compiti e responsabilità;
c) autorizzare formalmente i membri del proprio personale a svolgere funzioni legate alla certificazione;
d) monitorare e valutare le prestazioni del proprio personale.

14.3.2. Processo di selezione

L'Organismo di Certificazione deve disporre di processi per la selezione, la formazione e l'autorizzazione formale degli Auditor e degli Esperti Tecnici utilizzati nella certificazione. La valutazione iniziale della competenza degli Auditor include la loro capacità di applicare le conoscenze e le abilità richieste durante gli audit, anche osservandoli mentre conducono un audit.

[29] Clausola 7.2.6 della ISO/IEC17021-1:2015
[30] vedere la sezione 7 della ISO/IEC 17065:2012 e la clausola 9 della ISO/IEC 17021-1:2015.

Il comportamento personale degli Auditor può influenzare la capacità di svolgere funzioni specifiche. L'Organismo di Certificazione terrà conto del comportamento personale durante il processo di selezione e formazione. Dovrà sfruttare i punti di forza del comportamento personale e ridurre al minimo l'impatto dei punti deboli.

Per gli audit in loco, una descrizione del comportamento personale desiderato per il personale coinvolto nelle attività di certificazione è descritta nell'Allegato D della ISO/IEC 17021-1:2015.

14.3.3. Processi di valutazione

L'Organismo di Certificazione deve disporre di un processo documentato e di criteri di competenza per la valutazione iniziale delle competenze e il monitoraggio continuo delle competenze e delle prestazioni di tutto il personale coinvolto nelle attività di certificazione. L'Organismo di Certificazione deve dimostrare che i suoi metodi di valutazione sono efficaci per valutare e monitorare le competenze del personale e per garantire che il personale selezionato abbia un livello adeguato di competenze prima di assumersi la responsabilità dello svolgimento delle attività per le certificazioni Europrivacy.

14.3.4. Registri del personale

L'Organismo di Certificazione deve tenere un registro aggiornato di tutto il personale coinvolto nelle certificazioni Europrivacy, compresi gli auditor, gli esperti e il personale amministrativo.

In linea con i requisiti ISO/IEC, il registro del personale deve includere le seguenti informazioni[31]:

a) dati personali (nome, indirizzo, ecc.);
b) esperienza professionale (datori di lavoro, posizioni, ecc.);
c) istruzione e qualifiche;
d) esperienza e formazione complementare;
e) valutazioni delle loro competenze;
f) monitoraggio delle loro prestazioni;
g) funzioni e autorizzazioni detenute all'interno dell'Organismo di Certificazione;
h) la data dell'ultimo aggiornamento di ciascuna registrazione.

14.3.5. Prestazioni complessive del personale

L'Organismo di Certificazione deve monitorare e documentare la competenza e le prestazioni del proprio personale. Deve riesaminare regolarmente le proprie competenze e identificare le esigenze di formazione.

Nel controllare la competenza dei propri Auditor, l'Organismo di Certificazione deve:

- valutare periodicamente le prestazioni di ciascun Auditor in loco;
- combinare le valutazioni in loco, l'esame dei report di audit e il feedback dei Richiedenti (o delle parti interessate);
- ridurre al minimo l'impatto o il disturbo del processo di certificazione e dei Richiedenti.

14.4. Uso di risorse esterne per la valutazione

14.4.1. Obbligazione generale

Quando un Organismo di Certificazione svolge attività di valutazione con risorse esterne, deve rispettare i requisiti dello Schema di Certificazione, compreso il requisito di imparzialità.

14.4.2. Utilizzo di singoli Auditor esterni e di Esperti Tecnici esterni

L'Organismo di Certificazione richiederà a tutti gli Auditor esterni e agli Esperti Tecnici esterni di firmare un accordo scritto in cui si impegnano a:

a) rispettare le regole, i processi e le procedure dell'Organismo di Certificazione;
b) preservare la riservatezza e l'imparzialità;
c) notificare all'Organismo di Certificazione qualsiasi rapporto esistente o pregresso con qualsiasi organizzazione che potrebbe essere incaricata dell'audit.

[31] See Section 6 in ISO/IEC17065:2012

14.4.3. Chiarimenti sulla nozione di esternalizzazione

La ISO 9001:2008, al punto 4.1, definisce un processo esternalizzato come *"un processo di cui l'organizzazione ha bisogno per il suo sistema di gestione della qualità e che l'organizzazione sceglie di far eseguire da una parte esterna".* I termini "outsourcing" e "subappalto" possono spesso essere considerati come sinonimi. Tuttavia, il termine "outsourcing" non si riferisce all'utilizzo di personale esterno assunto individualmente per operare sotto l'autorità diretta dell'Organismo di Certificazione, anche se il loro lavoro viene addebitato all'Organismo di Certificazione da una terza parte.

14.4.4. Utilizzo dell'outsourcing

L'Organismo di Certificazione può esternalizzare le attività di valutazione solo a organismi che soddisfano i requisiti applicabili dello Schema di Certificazione, tra cui:

- un livello adeguato di competenza in materia di protezione dei dati;
- requisiti di imparzialità e riservatezza;
- i requisiti ISO/IEC 17065 applicabili quando si certifica il trattamento dei dati relativi a prodotti, processi e servizi.

Ciò può includere l'esternalizzazione ad altri Organismi di Certificazione.

14.4.5. Divieto di esternalizzare le decisioni

Tutte le decisioni relative a una certificazione (cfr. 6.3) devono rimanere sotto il controllo diretto ed effettivo dell'Organismo di Certificazione e non possono essere esternalizzate.

14.4.6. Processo e accordo richiesti per l'esternalizzazione

L'Organismo di Certificazione deve disporre di un processo per l'approvazione e il monitoraggio dei fornitori di servizi in outsourcing utilizzati per le attività di certificazione. Esso deve:

- garantire la presenza di competenze adeguate;
- garantire la registrazione delle competenze di tutto il personale coinvolto nelle attività di certificazione;
- tenere un registro documentato dei fornitori di servizi convalidati;[32]
- adottare un accordo giuridicamente vincolante con disposizioni adeguate in materia di riservatezza e conflitti di interesse, compreso l'obbligo di dichiarare eventuali relazioni e problemi di imparzialità con i Richiedenti da certificare.

L'Organismo di Certificazione può affidarsi al monitoraggio e alla valutazione di terze parti, quali autorità governative, organismi di accreditamento o organismi di valutazione tra pari.

14.4.7. Responsabilità dell'Organismo di Certificazione nell'esternalizzazione

L'Organismo di Certificazione mantiene la responsabilità delle attività esternalizzate. Deve garantire che l'organismo incaricato di svolgere le attività esternalizzate sia conforme allo Schema di Certificazione e ai requisiti ISO applicabili, anche in termini di competenza, imparzialità e riservatezza.

[32] La clausola 6.2.2.4 della ISO/IEC 17065:2012 richiede inoltre di *"attuare azioni correttive per qualsiasi violazione del contratto o di altri requisiti di cui venga a conoscenza"* e di *"informare il Richiedente in anticipo delle attività di esternalizzazione, al fine di fornire al Richiedente l'opportunità di opporsi".*

15. Gestione delle informazioni e riservatezza

Questa sezione si applica all'Organismo di Certificazione.

15.1. Gestione e classificazione dei documenti

*"**Certification mechanisms should provide for a standardised documentation methodology.** Thereafter evaluations will allow comparison of the certification documentation with the actual status onsite and against the certification criteria.* (…) *The documentation produced during the evaluation should, therefore, focus on three main aspects:*
*- **consistency and coherence of evaluation methods executed**;*
*- evaluation methods **directed to demonstrate compliance of the certification Object** with the certification criteria and thus with the Regulation; and*
*- that the results of the evaluation have been **validated by an independent and impartial certification body**."*
(EDPB Guidelines 1/2018)

***"I meccanismi di certificazione dovrebbero prevedere una metodologia di documentazione standardizzata.** Successivamente, la valutazione consentirà di confrontare la documentazione di certificazione con la situazione corrente in loco e con i criteri di certificazione. (...) La documentazione prodotta nel corso della valutazione dovrebbe quindi concentrarsi su tre aspetti fondamentali:*

-Coerenza dei metodi di valutazione impiegati;
-metodi di valutazione mirati a dimostrare la conformità dell'Oggetto della certificazione ai criteri di certificazione e quindi al Regolamento; e
-convalida dei risultati della valutazione da parte di un organismo di certificazione indipendente e imparziale". (Linee guida EDPB 1/2018)

15.1.1. Obiettivi della classificazione dei documenti

Gli Organismi di Certificazione devono utilizzare una classificazione e un'identificazione chiara e coerente di ogni documento. L'identificazione e la classificazione della documentazione relativa a Europrivacy devono essere strutturate in modo da garantire:

- un processo di certificazione ben specificato e affidabile;
- accesso chiaro e semplice alle informazioni e alla documentazione aggiornate.

15.2. Riservatezza delle informazioni e protezione dei dati

15.2.1. Obbligo di riservatezza e protezione dei dati

L'Organismo di Certificazione è responsabile dell'adeguata gestione e protezione delle informazioni raccolte e/o generate durante il processo di certificazione.

L'Organismo di Certificazione e tutte le parti coinvolte nei processi di certificazione dovranno inoltre proteggere i dati personali e rispettare pienamente le disposizioni del GDPR e le altre normative applicabili in materia di protezione dei dati.

Deve, inoltre, deve mettere in atto meccanismi contrattuali adeguati per garantire che tutti i suoi organi e agenti che agiscono per suo conto rispettino gli obblighi di cui sopra.

15.2.2. Obblighi del personale di preservare la riservatezza

Tutto il personale coinvolto nelle attività di certificazione o che ha accesso alle informazioni interne deve preservare e proteggere la riservatezza di tutte le informazioni riservate relative alla certificazione.

15.2.3. Ambito di applicazione della riservatezza

Per impostazione predefinita, tutte le informazioni fornite dal Richiedente o relative al Richiedente e alla sua certificazione saranno trattate come informazioni riservate, tranne nel caso in cui le informazioni:

- sono disponibili al pubblico; oppure
- sono qualificate come non confidenziali dal Richiedente; oppure
- sono divulgate con il consenso del Richiedente; oppure

- devono essere divulgate per motivi legali o contrattuali.

La riservatezza non si applica alle informazioni che devono essere pubblicate sul Registro e non impedisce l'accesso legittimo alle informazioni da parte di soggetti autorizzati, come le Autorità di Controllo.

15.2.4. Accesso legittimo di terzi alle informazioni riservate

L'Organismo di Certificazione può essere obbligato per legge a rilasciare informazioni riservate e dovrà ottemperare a tali richieste.

Le Autorità di Controllo e lo Scheme Owner possono richiedere l'accesso a informazioni riservate per svolgere i loro compiti, come la sorveglianza e l'elaborazione dei reclami delle certificazioni. Se giustificato, l'Organismo di Certificazione fornirà un accesso adeguato e proporzionato alle informazioni richieste, a condizione che la parte che accede sia vincolata da obblighi di riservatezza. L'accesso alle informazioni che fanno parte della regolare sorveglianza e del monitoraggio dell'attività di certificazione non richiede alcuna notifica specifica al Richiedente. Negli altri casi, il Richiedente deve essere informato, a meno che ciò non sia vietato dalla legge.

15.2.5. Infrastruttura conforme alla riservatezza e alla privacy

L'Organismo di Certificazione deve garantire un trattamento sicuro e riservato delle informazioni dei propri Richiedenti. Deve avere:

a) un'infrastruttura adeguata per archiviare, trattare e trasmettere in modo sicuro le informazioni e le registrazioni riservate sui Richiedenti;
b) una policy e procedure documentate sulla conservazione dei dati e sulla minimizzazione dei dati personali;
c) un'Informativa privacy accessibile pubblicamente dal suo sito web.

Solo le persone autorizzate, con l'obbligo contrattuale o legale di mantenere la riservatezza delle informazioni, avranno accesso ai dati e ai file archiviati.

L'Organismo di Certificazione deve garantire che i suoi strumenti online e i suoi siti web siano conformi al GDPR.

15.3. Scambio di informazioni tra l'Organismo di Certificazione e i suoi Richiedenti

15.3.1. Informazioni iniziali fornite al Richiedente

L'Organismo di Certificazione deve fornire informazioni chiare ai Richiedenti, tra cui:

a) una descrizione del processo di certificazione, tra cui:
   - Richiesta;
   - audit e valutazione, compresi gli audit di sorveglianza, ove applicabili;
   - processo decisionale per la concessione, il rifiuto, il mantenimento, il rinnovo, la sospensione, il ritiro o il ripristino di un certificato;
   - processo di espansione o riduzione del campo di applicazione della certificazione;
b) i riferimenti normativi e i requisiti per la certificazione;
c) informazioni sui costi e sulle tariffe per il Richiedente, anche per il mantenimento della certificazione e per la ricertificazione;
d) gli obblighi del Richiedente, compresi quelli di:
   - rispettare le regole e i requisiti dello Schema di Certificazione;
   - adottare tutte le misure necessarie per facilitare il lavoro dell'Organismo di Certificazione e fornire un accesso adeguato a tutte le aree, la documentazione, i file e il personale pertinenti in tutte le fasi del processo;
   - autorizzare l'eventuale partecipazione di Observer per la valutazione del lavoro dei Auditor;
e) informazioni sui diritti e gli obblighi dei Richiedenti certificati, anche in occasione della comunicazione della propria certificazione;
f) informazioni e contatti per reclami e ricorsi.

15.3.2. Documentazione e informazioni su compiti e responsabilità

L'Organismo di Certificazione deve conservare la documentazione dei suoi compiti e delle sue responsabilità in merito alle attività di certificazione, compreso il processo di richiesta, allo scopo di:

- Informazioni sullo stato di una domanda;
- Valutazione da parte dell'Autorità di Controllo competente.

15.3.3. Comunicazione di modifiche da parte di un Organismo di Comunicazione

Lo Schema di Certificazione è stato sviluppato per rispondere alle normative europee in materia di protezione dei dati, che sono soggette a modifiche, anche attraverso l'evoluzione della giurisprudenza. Anche l'evoluzione tecnologica può avere un impatto sui requisiti tecnici e sui criteri di valutazione richiesti dallo Schema di Certificazione. Analogamente, si prevede che i requisiti dello Schema di Certificazione si evolveranno nel tempo.

Lo Scheme Owner, con il supporto del suo Comitato Internazionale di Esperti, determinerà ogni necessario adattamento dello Schema di Certificazione.

Quando lo Scheme Owner adotta una modifica dello Schema di Certificazione, gli Organismi di Certificazione devono verificare che i Target of Evaluation certificati dei loro Richiedenti siano conformi ai nuovi requisiti.

L'Organismo di Certificazione deve informare i Richiedenti certificati di qualsiasi modifica ai requisiti per la certificazione che possa avere un impatto sulla loro certificazione e deve fornire informazioni sui nuovi requisiti.

15.3.4. Comunicazione di modifiche da parte di un Richiedente certificato

L'Organismo di Certificazione deve stabilire adeguati accordi contrattuali per essere informato dal Richiedente certificato, senza ingiustificato ritardo, di qualsiasi cambiamento che possa influire sulla capacità del Target of Evaluation certificato di continuare a soddisfare i requisiti dello Schema di Certificazione. Ciò comprende qualsiasi cambiamento relativo:

a) all'estensione della finalità e dell'ambito del trattamento dei dati;
b) all'estensione delle categorie di dati personali trattati nel Target of Evaluation;
c) a nuovi Responsabili del trattamento coinvolti nel Target of Evaluation;
d) all'ubicazione del nuovo sito, compresa la posizione geografica dell'infrastruttura del server che elabora o memorizza i dati personali;
e) ad un nuovo trasferimento transfrontaliero di dati personali;
f) ad importanti cambiamenti legali, commerciali, organizzativi, compresa la modifica del controllo effettivo e/o della proprietà del Richiedente e/o del suo Target of Evaluation certificato;
g) a importanti decisioni organizzative e gestionali che possono avere un impatto sul Target of Evaluation certificato, come ad esempio il cambio del responsabile della protezione dei dati;
h) se applicabile, all'ambito delle operazioni nell'ambito del Target of Evaluation certificato;
i) a qualsiasi modifica importante al Target of Evaluation certificato, come il rilascio di una nuova versione;
j) all'indirizzo di contatto.

In caso di tali modifiche, l'Organismo di Certificazione dovrà intraprendere le azioni appropriate, che possono includere quanto segue:

a) valutazione;
b) revisione;
c) decisione sulla certificazione;
d) emissione di documentazione formale di certificazione rivista (compresa l'attività di monitoraggio o sorveglianza) per estendere o ridurre il campo di applicazione della certificazione.

Le registrazioni devono includere le azioni di follow-up e le motivazioni per l'esclusione di una qualsiasi delle attività di cui sopra.

15.4. Informazioni al pubblico

L'Organismo di Certificazione deve avere regole chiare che disciplinano la divulgazione di informazioni pubbliche sulle sue piattaforme di comunicazione.

15.4.1. Informazioni pubbliche rese disponibili senza richiesta

L'Organismo di Certificazione deve mantenere e rendere pubbliche (attraverso pubblicazioni, media elettronici o altri mezzi) senza richiesta, in tutte le aree geografiche in cui opera, informazioni generali su:

a) processo di valutazione della certificazione;
b) processo decisionale relativo alla certificazione e al suo campo di applicazione;[33]
c) tipi di attività di trattamento dei dati che può certificare;
d) l'uso del nome, del logo e del marchio di conformità allegati alle certificazioni consegnate;
e) i processi in atto per la gestione delle richieste di informazioni, dei reclami e dei ricorsi;
f) la policy e il meccanismo sull'imparzialità;
g) i dati di contatto dell'Organismo di Certificazione, come l'indirizzo postale;
h) la policy di protezione dei dati personali dell'Organismo di Certificazione e la procedura per contattare il suo Responsabile della Protezione dei Dati.

15.4.2. Informazioni pubbliche rese disponibili su richiesta

In conformità ai requisiti ISO, l'Organismo di Certificazione deve fornire **su richiesta** informazioni complementari su:

a) *"le aree geografiche in cui opera l'Organismo di Certificazione";*
b) lo stato di una determinata certificazione;
c) il nome, il documento normativo correlato, il campo di applicazione e la posizione geografica (città e paese) del Richiedente certificato;[34]
d) *informazioni (o riferimenti) allo Schema di Certificazione, comprese le procedure di valutazione, le regole e le procedure per la concessione, il mantenimento, l'estensione o la riduzione del campo di applicazione, la sospensione, il ritiro o il rifiuto della certificazione;*
e) *una descrizione dei mezzi con cui l'Organismo di Certificazione ottiene il sostegno finanziario e informazioni generali sulle tariffe applicate ai richiedenti e ai richiedenti;*
f) *una descrizione dei diritti e dei doveri dei Richiedenti, compresi i requisiti, le restrizioni o le limitazioni sull'uso del nome e del marchio di certificazione dell'Organismo di Certificazione e sulle modalità di riferimento alla certificazione concessa;*
g) informazioni sulle procedure di gestione dei reclami e dei ricorsi".[35]

L'Organismo di Certificazione può richiedere che le parti interessate richiedano queste informazioni per iscritto tramite posta e che includano un indirizzo e-mail da utilizzare per la risposta.

L'accesso a determinate informazioni può essere limitato da interessi legittimi su richiesta del Richiedente (ad esempio, per motivi di sicurezza) o per motivi di riservatezza o protezione dei dati.

L'Organismo di Certificazione può anche rendere pubbliche le informazioni senza richiesta sul proprio sito Internet.

15.4.3. Registro comune e sito web di informazione al pubblico

Lo Scheme Owner è responsabile della gestione e del controllo del sito web ufficiale di Europrivacy con i documenti ufficiali di riferimento, nonché del Registro dei Certificati Europrivacy. Gli Organismi di Certificazione possono replicare le informazioni pubbliche nel proprio sito web, purché siano coerenti con le informazioni fornite dallo Scheme Owner.

[33] Come, ad esempio, le decisioni relative alla concessione, al rifiuto, al mantenimento, al rinnovo, alla sospensione, al ripristino o al ritiro della certificazione o all'ampliamento o alla riduzione del campo di applicazione di una certificazione.
[34] Vedere la clausola 8.1.2, punto da a a c, della ISO/IEC 17021-1:2015.
[35] Clausola 4.6, punto da a a d, della ISO/IEC 17065:2012

Gli Organismi di Certificazione devono tenere aggiornato il Registro centrale con le informazioni relative ai propri Richiedenti e ai processi di certificazione, evitando qualsiasi ritardo nell'aggiornamento delle informazioni.

Gli Organismi di Certificazione autorizzati devono fornire un link dal loro sito web al Registro dei Certificati Europrivacy e al sito web di informazione pubblica.

15.4.4. Affidabilità delle informazioni

Le informazioni fornite dall'Organismo di Certificazione a qualsiasi Richiedente o al mercato, compresa la pubblicità, devono essere accurate e non fuorvianti. Qualsiasi uso del marchio legato a Europrivacy, compresi il marchio e il logo, deve rispettare le regole e le linee guida di Europrivacy per il marketing e la comunicazione.

15.5. Obbligo di tenere i registri del processo di certificazione

15.5.1. Obbligo di conservazione dei registri

L'Organismo di certificazione deve conservare le registrazioni per dimostrare che tutti i requisiti del processo di certificazione sono stati effettivamente soddisfatti. L'Organismo di Certificazione deve garantire che tali registrazioni siano trasportate, trasmesse e conservate in modo da assicurare la riservatezza.

15.5.2. Diritti di accesso

Lo Scheme Owner e, ove applicabile, le Autorità di Controllo e/o gli organismi autorizzati, possono richiedere l'accesso a informazioni e registrazioni riservate per svolgere i loro compiti, come la sorveglianza e la gestione dei reclami. L'Organismo di Certificazione deve collaborare e fornire l'accesso alle informazioni richieste.

15.5.3. Periodo di conservazione

Per impostazione predefinita, le registrazioni delle certificazioni rilasciate saranno conservate per la durata del relativo ciclo di certificazione più dieci anni. Il periodo di conservazione può essere esteso quando richiesto dalla legge o per soddisfare gli interessi legittimi dell'Organismo di Certificazione, come la mitigazione dei rischi legali o la necessità di accedere ai dati storici nel contesto delle ricertificazioni previste. Qualora il periodo di conservazione debba essere esteso, l'Organismo di Certificazione dovrà registrarne le motivazioni. Al termine del periodo di conservazione, le registrazioni devono essere cancellate.

15.6. Riferimenti alla certificazione e all'uso di marchi di conformità, licenze e certificati

15.6.1. Uso di certificati, etichette e marchi di conformità

Il logo Europrivacy e il marchio di conformità sono e restano di proprietà dello Scheme Owner. Possono essere utilizzati dal Richiedente solo dopo l'approvazione dell'Organismo di Certificazione e sotto la sua supervisione.

Gli Organismi di Certificazione e i Richiedenti **devono rispettare le regole dello Schema di Certificazione che disciplinano l'uso dei certificati e del marchio di conformità, nonché le regole e le linee guida per la comunicazione su Europrivacy.** Le regole principali sono specificate dallo Scheme Owner e possono essere integrate da regole aggiuntive specificate dall'Organismo di Certificazione.

I certificati di conformità devono:

- fornire informazioni chiare sullo schema di certificazione e sul Target of Evaluation;
- evitare qualsiasi comunicazione fuorviante in merito all'ambito della certificazione;
- consentire la rintracciabilità dell'Organismo di Certificazione e del suo Registro.

Non devono esserci ambiguità riguardo alla portata della certificazione per la quale è stata concessa. Ad esempio, utilizzare un trattamento di dati certificato per affermare che la società nel suo complesso è certificata è vietato e può portare alla sospensione o al ritiro del certificato.

Le regole e i dettagli relativi all'uso dei certificati e dei marchi di conformità Europrivacy sono specificati nel documento "Europrivacy Rules on the Use of Logo, Certificates, and Marks of Conformity", che è un documento vincolante che tutte le parti devono rispettare.

15.6.2. Diritto di controllare l'uso conforme

L'Organismo di Certificazione e lo Scheme Owner hanno il diritto di esercitare il controllo sulla proprietà, l'uso e l'esposizione di licenze, certificati, marchi di conformità e qualsiasi altro meccanismo che indichi che il trattamento dei dati è certificato dall'Organismo di Certificazione.

L'Organismo di Certificazione deve verificare se *nella documentazione o in altre forme di pubblicità si trovino "riferimenti non corretti allo Schema di Certificazione o un uso fuorviante di licenze, certificati, marchi o qualsiasi altro meccanismo che possa indicare che il prodotto, il processo o il servizio è certificato"*[36]. Se si verifica un caso del genere, l'Organismo di Certificazione deve intervenire in modo adeguato.

15.6.3. Marchio e Logo Europrivacy

Il logo di Europrivacy è composto dalle lettere "E" e "P" in colore blu, con sei stelle gialle, come presentato negli esempi sottostanti:

Figura 8 Logo e Marchio di conformità Europrivacy

Il termine Europrivacy e il logo sono marchi di proprietà dello Scheme Owner. Il loro utilizzo è soggetto ad autorizzazioni scritte e a regole severe.

15.6.4. Certificati

"Un certificato, sigillo o marchio in conformità del GDPR può essere rilasciato solo a seguito di una valutazione indipendente degli elementi di prova ad opera di un Organismo di Certificazione accreditato o di un'Autorità di Controllo competente, che attesti il soddisfacimento dei criteri di certificazione." (Fonte: Linee guida EDPB 1/2018)

Il trattamento dei dati certificato può ricevere un certificato Europrivacy sotto il controllo e l'approvazione dell'Organismo di Certificazione. I certificati devono includere almeno:

a) il **logo dell'Organismo di Certificazione e il logo Europrivacy**;
b) il **nome del Richiedente**;
c) se il Richiedente agisce in qualità di **Titolare del trattamento, di Responsabile del trattamento o di Contitolare del trattamento**;
d) se del caso, il **nome del/i contitolare/i del trattamento**;
e) una chiara **descrizione del Target of Evaluation** e della sua **portata geografica**;
f) ove applicabile, **qualsiasi estensione** applicata alla certificazione;
g) le **date di emissione e di scadenza del certificato**;
h) l'**identificatore univoco** del certificato consegnato;
i) la dicitura *"Informazioni dettagliate all'indirizzo"* seguita dal nome del dominio del sito web dello Schema di Certificazione e del Registro dei Certificati Europrivacy online: http:ww//europrivacy.com;
j) il **nome e l'indirizzo dell'Organismo di Certificazione** che rilascia il certificato.

I certificati devono essere chiari e facilmente comprensibili per gli interessati. Non devono superare preferibilmente una pagina.

[36] Clausola 4.1.3.2 della ISO/IEC 17065:2012

15.6.5. Marchio di conformità

Ove applicabile, il trattamento dei dati certificato può essere contrassegnato con il marchio di conformità Europrivacy, sotto il controllo e l'approvazione dell'Organismo di Certificazione.

Il marchio di conformità deve sempre includere:

a) il logo Europrivacy;
b) l'identificativo unico della certificazione;
c) il nome di dominio del sito web dello Schema di Certificazione (http://www.europrivacy.com), che dà **accesso al Registro online dei Certificati Europrivacy** con informazioni dettagliate sul certificato consegnato grazie al suo identificativo unico.

I Marchi di Conformità per le estensioni dei criteri sono specificati dallo Scheme Owner e indicano chiaramente la relativa estensione normativa.

Di seguito vengono presentati alcuni esempi di marchi di conformità:

Figura 9 Esempi di marchi di conformità

15.6.6. Dichiarazioni di conformità

I Richiedenti possono includere dichiarazioni di certificazione sul proprio sito web o su altre informazioni e documentazioni pertinenti, previa approvazione scritta dell'Organismo di Certificazione.

La dichiarazione deve sempre includere:

a) il riferimento a Europrivacy e, ove autorizzato, il logo Europrivacy;
b) il nome del Richiedente certificato;
c) se del caso, il nome del/i contitolare/i del trattamento;
d) una chiara indicazione del Target of Evaluation e della sua portata geografica;
e) se del caso, una chiara indicazione delle norme o dei requisiti complementari che sono stati aggiunti;
f) le date di emissione e di validità del certificato;
g) l'identificatore univoco del certificato consegnato;
h) la dicitura "Informazioni dettagliate all'indirizzo" seguita dal nome del dominio del sito web dello Schema di Certificazione e del Registro online dei Certificati Europrivacy: http://www.europrivacy.com;
i) il nome dell'Organismo di Certificazione che rilascia il certificato.

Nel caso in cui la certificazione sia rilasciata su base volontaria senza che il Richiedente ne richieda la validità ai sensi degli articoli 42 e 43 del GDPR, la dichiarazione di conformità deve indicarlo chiaramente.

Ecco un esempio di dichiarazione di certificazione:

Statement of Conformity

with the GDPR and Europrivacy

Applicant
COMPANYNAME.SA
123 Address street
1111 City, Country
declares under its sole responsibility that the following data processing is in conformity with the following requirements:

Certification

Target of Evaluation:	Personal data processing by the smart parking solution deployed on the municipal territory of the city ABC.
Normative Scope:	Europrivacy criteria, v. 05.03.2019
Certified on and until:	April 27 2019 – April 26 2022
Certificate ID:	83F4:A014
Detailed information at:	www.europrivacy.com
Certification Body:	CERTIFICATION.SA 567 Address street 2222 City, Country

Signature

Authorized representative:	Mr ABC
Date:	May 3 2019
Signature:	XXXXXX

Figura 10 Dichiarazione di certificazione

15.6.7. Dichiarazioni e Marchi di Conformità sui supporti elettronici

Se un certificato, una dichiarazione o un marchio di conformità relativi a una certificazione Europrivacy vengono visualizzati su un supporto elettronico, come una pagina web o un documento pdf, devono includere un collegamento ipertestuale diretto alla homepage principale dello Schema di Certificazione (http://www.europrivacy.com) o alla pagina specifica del Target of Evaluation certificato nel Registro online.

15.6.8. Restrizioni all'uso di Certificati e Marchi di Conformità

I marchi di conformità, i certificati e le dichiarazioni di certificazione non devono essere utilizzati in modo tale da generare confusione o comunicazioni fuorvianti sul Target of Evaluation della certificazione in questione.

15.6.9. Obblighi contrattuali del Richiedente

L'Organismo di Certificazione deve, attraverso accordi legalmente applicabili, richiedere che il Richiedente certificato:

a) sia conforme ai requisiti dello Schema di Certificazione e alle istruzioni fornite dall'Organismo di Certificazione nel comunicare la propria certificazione;
b) prevenga ed escluda qualsiasi comunicazione fuorviante sulla propria certificazione, compresa la sua effettiva portata e il suo stato attuale;[37]
c) riceva l'approvazione dell'Organismo di Certificazione prima di utilizzare un marchio di conformità in relazione alla certificazione rilasciata;
d) adegui senza ingiustificato ritardo la propria comunicazione a qualsiasi cambiamento nella certificazione, come la riduzione del campo di applicazione, la sospensione o il ritiro, modificando o interrompendo l'uso del materiale di comunicazione che fa riferimento alla certificazione;
e) non utilizzi la propria certificazione in alcun modo che possa danneggiare la reputazione e la fiducia dell'Organismo di Certificazione e dello Schema di Certificazione.

15.6.10. Dichiarazione aggiuntiva per i Richiedenti che agiscono come importatori di dati

Nel caso in cui il Richiedente agisca come importatore di dati con sede in un Paese terzo senza una decisione di adeguatezza, l'Organismo di certificazione e il Richiedente dovranno entrambi dichiarare per iscritto di non avere motivo di ritenere che la legislazione e le prassi applicabili al Target of Evaluation possano impedire al Richiedente di adempiere agli obblighi previsti dalla certificazione.

15.6.11. Controllo dell'organismo di Certificazione

L'Organismo di Certificazione "*deve esercitare un adeguato controllo della proprietà*" dell'uso e del riferimento ai certificati da esso rilasciati, e deve *"intraprendere azioni per affrontare i riferimenti errati allo stato di certificazione o l'uso fuorviante dei documenti di certificazione, dei marchi o dei report di audit". Tali azioni possono includere richieste di correzione e azioni correttive, sospensione, ritiro della certificazione, pubblicazione della trasgressione e, se necessario, azioni legali*".[38]

Lo Scheme Owner può richiedere agli Organismi di Certificazione di indagare sui casi di uso improprio o di potenziale Non Conformità. L'Organismo di Certificazione deve procedere senza ingiustificato ritardo.

In caso di evidenza concreta che un Target of Evaluation certificato presenti una Non Conformità Maggiore o che possa avere un impatto negativo sulla reputazione e sulla fiducia nello Schema di Certificazione, lo Scheme Owner può adottare misure provvisorie o derogatorie per sospendere e/o ritirare una certificazione senza il consenso dell'Organismo di Certificazione.

[37] Inoltre, l'ISO richiede espressamente che la comunicazione su una certificazione eviti qualsiasi ambiguità tra la certificazione di prodotto e di processo e la certificazione del sistema di gestione.
[38] Clausola 8.3.5 della ISO/IEC 17021-1:2015

16. Gestione della qualità dell'Organismo di Certificazione

Gli Organismi di Certificazione che beneficiano di un accreditamento nazionale valido e attivo ai sensi della norma ISO/IEC 17065 o 17021-1 sono considerati conformi ai requisiti della presente sezione.

16.1. Requisiti del sistema di gestione dell'Organismo di Certificazione

L'Organismo di Certificazione deve stabilire e mantenere un sistema di gestione adeguato, conforme ai requisiti del presente Schema di Certificazione, in accordo con una delle due opzioni proposte dalla norma ISO/IEC 17065, vale a dire:

a) Opzione A: L'Organismo di Certificazione deve stabilire un sistema di gestione con:
   - una chiara documentazione del sistema di gestione generale;
   - controllo efficace di documenti e registrazioni;
   - audit interno annuale;
   - revisione annuale della gestione;
   - azioni correttive e preventive;

b) Opzione B: L'Organismo di Certificazione deve stabilire un sistema di gestione conforme ai requisiti della ISO 9001. Deve essere in grado di dimostrare il costante soddisfacimento di tali requisiti.

"Le procedure in caso di sospensione o revoca dell'accreditamento dell'Organismo di Certificazione devono essere integrate nel sistema di gestione dell'Organismo di Certificazione, compresa la notifica ai clienti." (EDPS)

16.2. Requisiti Specifici per l'Opzione A

La documentazione del Sistema di Gestione Generale deve fare riferimento a tutta la documentazione pertinente (compresi i processi e le registrazioni) per soddisfare i requisiti dello Schema di Certificazione.
il top management dell'Organismo di Certificazione deve:

a) adottare e mantenere una serie di **policy e obiettivi** per soddisfare i requisiti dello Schema di Certificazione;
b) assicurare che le sue policy e i suoi obiettivi siano **riconosciuti da tutti coloro che sono coinvolti nelle attività di certificazione e siano efficacemente implementati** in tutta l'organizzazione;[39]
c) **fornire prova del proprio impegno** a migliorare e rispettare il sistema di gestione;
d) **nominare** un responsabile per:
   - *"garantire che i processi e le procedure necessarie per il sistema di gestione siano stabiliti, implementati e mantenuti";*
   - *riferire al top management sulle prestazioni del sistema di gestione e sulle eventuali necessità di miglioramento*".[40]

16.2.1. Controllo dei documenti

L'Organismo di Certificazione deve disporre di procedure per il controllo dei documenti relativi alle sue attività di certificazione e per la sua conformità allo Schema di Certificazione. Tali procedure devono comprendere tutti i documenti pertinenti, indipendentemente dalla loro forma e dal loro supporto.
Le procedure devono determinare e specificare i controlli necessari per:

a) approvare formalmente i documenti (prima dell'emissione e/o dell'entrata in vigore);
b) rivedere, aggiornare e riapprovare i documenti, compreso il fatto di:
   - indicare le modifiche apportate al documento e lo stato di revisione attuale;
   - rendere disponibili tutte le versioni pertinenti dei documenti applicabili;
   - prevenire l'uso involontario di documenti obsoleti e applicarvi un'adeguata identificazione;
c) garantire che:

[39] Secondo la ISO/IEC 17065, tutto il personale coinvolto nelle attività di certificazione deve avere accesso alle parti della documentazione del sistema di gestione e alle relative informazioni applicabili alle proprie responsabilità.
[40] Sezione 8.2.3 della ISO/IEC 17065:2012

- i documenti rimangano leggibili e facilmente identificabili;
- i documenti esterni siano identificati e la loro distribuzione sia controllata.

16.2.2. Controllo dei Registri

L'Organismo di Certificazione deve disporre di procedure per la gestione e il controllo dei propri registri di audit, tra cui l'identificazione, l'archiviazione, la protezione, il recupero, il tempo di conservazione e la disposizione.

16.2.3. Revisione della Gestione

Il top management dell'Organismo di Certificazione deve disporre di procedure per riesaminare l'adeguatezza e l'efficacia del proprio sistema di gestione almeno su base annuale.

Review degli input

Il contributo alla review della gestione deve includere informazioni relative a quanto segue:

a) risultati degli audit interni ed esterni;
b) informazioni su ricorsi e reclami pertinenti da parte degli utenti delle attività di certificazione;
c) feedback ricevuti da:
   - i Richiedenti
   - le parti interessate, compreso lo Scheme Owner e/o altre autorità qualificate;
   - il meccanismo di salvaguardia dell'imparzialità;
d) le review:
   - dell'imparzialità;
   - dei ricorsi e dei reclami;
   - delle qualifiche del personale e delle esigenze di formazione;
   - delle azioni preventive e correttive;
   - delle azioni di follow-up delle precedenti review della gestione;
   - il raggiungimento degli obiettivi;
   - i cambiamenti che potrebbero influenzare il sistema di gestione.

Review degli output

La review della gestione deve includere una serie di decisioni e azioni per:

a) migliorare l'efficacia del sistema di gestione e dei suoi processi;
b) migliorare la conformità e l'attuazione dello Schema di Certificazione;
c) valutare il fabbisogno di risorse.

16.2.4. Audit interni

L'Organismo di Certificazione deve stabilire procedure ed eseguire audit interni[41] su base annuale, con l'obiettivo di verificare e migliorare:

a) la sua conformità ai requisiti dello Schema di Certificazione;
b) il suo sistema di gestione.

L'Organismo di Certificazione deve pianificare un programma di audit che tenga conto dei risultati degli audit precedenti. Deve garantire che:

a) gli Auditor interni siano competenti in materia di certificazione, audit e requisiti del presente Schema di Certificazione;
b) gli Auditor interni non controllino il proprio lavoro;
c) il personale responsabile dell'area sottoposta ad audit sia informato dei risultati dell'audit;
d) le azioni pertinenti risultanti dall'audit siano affrontate in modo tempestivo e appropriato;
e) vengano identificate le opportunità di miglioramento.

Gli Auditor devono redigere un audit report sintetico che includa il loro apprezzamento generale e le divergenze identificate. Le divergenze identificate devono essere annotate in un modulo per il miglioramento.

[41] La ISO 19011 fornisce le linee guida per la conduzione degli audit interni.

16.2.5. Azioni correttive e preventive

L'Organismo di Certificazione deve disporre di **procedure per la gestione delle Non Conformità** e per intraprendere azioni appropriate per eliminare le cause delle Non Conformità effettive o potenziali.

Come richiesto dalla ì ISO/IEC 17021-1, deve disporre di processi per:

a) "identificare le Non-Conformità (ad esempio, da reclami e audit interni);
b) determinare le loro cause;
c) correggere le Non Conformità identificate;
d) valutare se sono necessarie azioni per garantire che le Non Conformità non si ripetano;
e) determinare e attuare tempestivamente le azioni necessarie;
f) registrare i risultati delle azioni intraprese;
g) riesaminare l'efficacia delle azioni correttive".[42]

16.2.6. Direction Review Meeting

Una volta all'anno, tutti i dipendenti coinvolti nel processo di certificazione si riuniranno per riesaminare l'attuazione dello Schema di Certificazione e la sua gestione della qualità. I membri del Consiglio di Amministrazione saranno invitati a partecipare al Direction Review Meeting.

Il Direction Review Meeting deve prendere in considerazione nel suo ordine del giorno:

a) Follow-up dei punti d'azione del precedente Direction Review Meeting;
b) Reclami, ricorsi, NoC conformità e deroghe;
c) Sistema di gestione della qualità;
d) Monitoraggio del personale e sviluppo delle capacità;
e) Infrastruttura e sicurezza ICT;
f) Informazione e comunicazione esterna.

La Direction Review produrrà un report sintetico, che includerà, se del caso, le informazioni necessarie:

a) Un piano d'azione con azioni preventive e di miglioramento;
b) Un piano di gestione della qualità;
c) Valutazione delle esigenze del personale (ad esempio, reclutamento e formazione);
d) Raccomandazioni per rafforzare la sicurezza dell'infrastruttura ICT.

[42] Sezione 8.7.4 della ISO/IEC 17065:2012

17. Ricorsi e Reclami

Gli Organismi di Certificazione che beneficiano di un accreditamento nazionale valido e attivo ai sensi della ISO/IEC 17065 o 17021-1 sono considerati conformi ai requisiti della presente sezione.

17.1. Principi generali

I ricorsi contro una decisione possono essere presentati dal Richiedente all'Organismo di Certificazione o dall'Organismo di Certificazione allo Scheme Owner, a seconda di quale sia la decisione presa.

Una terza parte che ritenga che un Target of Evaluation certificato non sia conforme allo Schema di Certificazione o alle normative applicabili in materia di protezione dei dati coperti dal certificato può presentare il proprio reclamo al Richiedente certificato, all'Organismo di Certificazione o all'Autorità di Controllo competente. I reclami devono essere basati su constatazioni e prove concrete.

In base alle prove comunicate, la parte ricevente informerà l'Organismo di Certificazione e/o l'Autorità di Controllo . Se le informazioni rivelate dal reclamo possono avere un impatto sulla fiducia pubblica e sulla reputazione dello Schema di Certificazione, lo Scheme Owner deve essere informato senza alcun ritardo.

Nel caso in cui il reclamo non sia stato trattato correttamente dall'Organismo di Certificazione, la parte reclamante è invitata a informare lo Scheme Owner.

17.2. Policy dei Ricorsi e dei Reclami

L'Organismo di Certificazione deve disporre di un meccanismo chiaro per raccogliere, documentare e trattare i reclami o i ricorsi.

La presentazione, l'indagine e le decisioni sui reclami/ricorsi non devono comportare azioni discriminatorie da parte dell'Organismo di Certificazione nei confronti del reclamante/ricorrente.

Il meccanismo di reclamo e di ricorso deve specificare:

a) **chi può presentare reclami o obiezioni**, tra cui almeno qualsiasi amministrazione pubblica e gli interessati i cui dati personali sono trattati nell'ambito del Target of Evaluation certificato;
b) **il processo di ricezione, convalida, indagine ed elaborazione di ricorsi e reclami**, tra cui:
   - una procedura e un termine per confermare se il reclamo o il ricorso è relativo a una certificazione rilasciata dall'Organismo di Certificazione;
   - **la possibilità di consultare le Parti interessate;**
   - **ove applicabile, i limiti temporali;**
c) **chi è responsabile** del processo per conto dell'Organismo di Certificazione;
d) **un processo per registrare, documentare e monitorare sistematicamente i ricorsi e i reclami**, nonché le azioni intraprese per risolverli;
e) **un processo che garantisca l'adozione di azioni correttive adeguate**.

Lo Scheme Owner può stabilire processi e meccanismi complementari per la gestione dei reclami e dei ricorsi che devono essere sostenuti e rispettati dall'Organismo di Certificazione e dal Richiedente.

17.2.1. Obbligo di raccogliere e documentare i Reclami e i Ricorsi

L'Organismo di Certificazione e i suoi dipendenti sono responsabili della registrazione di tutti i reclami ricevuti, dei ricorsi e delle azioni successive.

Al ricevimento di un reclamo o di un ricorso relativo alle attività di certificazione, l'Organismo di Certificazione dovrà:

a) riconoscere il ricevimento di un reclamo o di un ricorso formale;
b) raccogliere e verificare tutte le informazioni pertinenti;
c) dare comunicazione formale dell'esito della procedura al reclamante o al ricorrente;
d) intraprendere qualsiasi azione successiva necessaria per risolvere il reclamo o il ricorso;
e) informare lo Scheme Owner di qualsiasi problema importante che possa costituire un rischio per lo Schema di Certificazione o per la sua reputazione.

17.2.2. Obbligo di procedere e dovere di diligenza

Se i reclami sono ritenuti validi, l'Organismo di Certificazione li affronta in modo appropriato e compie uno sforzo ragionevole per risolverli.

Il Richiedente e l'Organismo di Certificazione devono fornire pieno supporto per indagare e fornire chiarimenti al fine di elaborare e risolvere il reclamo. Un reclamo fondato può portare alla sospensione o al ritiro del certificato.

17.2.3. Obbligo di ricorrere a soggetti neutrali

Al fine di garantire un processo imparziale, le decisioni relative a un reclamo o a un ricorso saranno adottate da persone che:

- non sono state direttamente coinvolte nel relativo processo di certificazione;[43]
- non hanno fornito servizi alla Parte ricorrente o al Richiedente certificato.

[43] Vedere la sezione 7.13.5 della ISO/IEC 17065:2012.

18. Scheme Owner

18.1. Ruolo dello Scheme Owner

Lo Scheme Owner è responsabile di:

a) mantenere, aggiornare e migliorare lo Schema di Certificazione, le sue verifiche e i suoi controlli, i suoi termini e condizioni e l'altra documentazione correlata;
b) mantenere le informazioni pubbliche sullo Schema di Certificazione;
c) mantenere e rendere disponibile online il Registro ufficiale dei Certificati Europrivacy, il cui contenuto è fornito dagli Organismi di Certificazione;
d) fissare i termini e le condizioni per la concessione di licenze e l'utilizzo dello Schema di Certificazione, comprese le relative tariffe;
e) concedere in licenza il diritto di utilizzare lo Schema di Certificazione e i relativi diritti di proprietà intellettuale (come il brand e il marchio di conformità) e, se del caso, sospendere o ritirare tali diritti;
f) formazione e qualificazione di esperti per l'applicazione dello Schema di Certificazione.

Fatta eccezione per i casi in cui una parte o tutte le seguenti competenze sono riservate per legge a un'Autorità di Controllo, lo Scheme Owner può intervenire anche:

g) affrontando e indagando sui reclami relativi alle certificazioni Europrivacy;
h) controllando la conformità degli Organismi di Certificazione allo Schema di Certificazione;
i) facilitando la collaborazione e lo scambio di esperienze e informazioni tra gli Organismi di Certificazione autorizzati;
j) sospendendo e/o ritirando la certificazione;
   - concessa da Organismi di Certificazione non conformi allo Schema di Certificazione; oppure
   - ottenuta o utilizzata in modo ingannevole dai beneficiari; oppure
   - utilizzata in modo tale da screditare lo Schema di Certificazione;
k) ponendo in essere qualsiasi altra azione pertinente che lo Schema di Certificazione ritenga necessaria e/o utile per lo Schema di Certificazione.

Pur potendo intervenire a posteriori per sospendere, ritirare o invalidare una certificazione, lo Scheme Owner non ha alcuna responsabilità per il processo e la decisione sulla certificazione, che rimane di esclusiva competenza degli Organismi di Certificazione. Lo Scheme Owner non è responsabile di eventuali inadempienze o errori nei processi di certificazione (che sono di competenza degli Organismi di Certificazione), né di eventuali inadempienze dei Richiedenti. La conformità alle normative sulla protezione dei dati e allo Schema di Certificazione è di esclusiva responsabilità dei Richiedenti certificati. Tutti gli utilizzatori dello Schema di Certificazione Europrivacy accettano che lo Scheme Owner non è responsabile di eventuali inadempienze degli Organismi di Certificazione autorizzati o di eventuali inadempienze da parte dei Richiedenti certificati.

Lo Scheme Owner può addebitare agli Organismi di Certificazione i servizi forniti.

18.2. Comitato Internazionale di Esperti

Lo Scheme Owner istituirà un Comitato Internazionale di Esperti che riunisca esperti in materia di protezione dei dati, sicurezza informatica e certificazione. Questo organismo supporterà lo Scheme Owner nel:

a) rivedere, mantenere e aggiornare il sistema di certificazione Europrivacy;
b) rispondere alle domande trasmesse dallo Scheme Owner a questo organismo;
c) fungere da meccanismo di imparzialità quando richiesto dallo Scheme Owner.

18.3. Conformità ai requisiti specifici del GDPR per la certificazione

Lo Schema di Certificazione deve essere conforme ai requisiti del GDPR, comprese le disposizioni specifiche relative alla certificazione di cui agli articoli 42 e 43 del GDPR.

18.3.1. Collaborazione con le Autorità di Controllo

Lo Scheme Owner deve informare e mantenere una stretta collaborazione con le Autorità di Controllo competenti.

18.3.2. European Data Protection Board

Lo Scheme Owner consulterà e seguirà le decisioni e le indicazioni dell'European Data Protection Board.

18.3.3. Atti della Commissione europea

La Commissione europea può adottare atti che stabiliscono le norme tecniche per i meccanismi di certificazione e i sigilli e marchi di protezione dei dati, nonché i meccanismi di promozione e riconoscimento di tali meccanismi di certificazione, sigilli e marchi.

18.3.4. Responsibilita

La certificazione non riduce la responsabilità di un Titolare o di un Responsabile del Trattamento per quanto riguarda la conformità alle normative applicabili in materia di protezione dei dati e viene fornita senza pregiudicare i compiti e i poteri delle Autorità di Controllo competenti.

18.4. Miglioramento dei documenti dello Schema di Certificazione

18.4.1. Miglioramento dello Schema di Certificazione

Lo Scheme Owner condurrà una regolare revisione e miglioramento dello Schema di Certificazione con il supporto di un Comitato Internazionale di Esperti.

L'Organismo di Certificazione deve stabilire procedure per la revisione e l'aggiornamento dei propri metodi di valutazione "in funzione dei cambiamenti del quadro normativo, dei rischi rilevanti, dello stato dell'arte e dei costi di implementazione delle misure tecniche e organizzative". **(EDPB)**

18.4.2. Suggerimenti per i miglioramenti

Gli Organismi di Certificazione e il loro team di audit raccoglieranno e comunicheranno allo Scheme Owner eventuali suggerimenti di miglioramento. Tali suggerimenti possono riguardare lo Schema stesso e/o le verifiche e i controlli dettagliati. Lo Scheme Owner deve raccogliere e compilare i suggerimenti ricevuti e selezionare quelli più rilevanti da sottoporre alla discussione del Comitato Internazionale di Esperti Europrivacy e da considerare per la revisione dello Schema di Certificazione.

18.4.3. Revisione o aggiunta di documenti

Se necessario, lo Scheme Owner, con il supporto del suo Comitato Internazionale di Esperti, può rivedere e adattare i documenti relativi allo Schema di Certificazione e/o crearne di nuovi.

Lo Scheme Owner comunicherà gli aggiornamenti dei criteri di certificazione all'Autorità di Controllo competente, indicando se ciò implica modifiche sostanziali ai criteri di certificazione.

Le revisioni dello Schema di Certificazione Europrivacy sono:

a) inserite nel sito web di Europrivacy Community and Resources;
b) rese disponibili alle parti interessate autorizzate e competenti.

Quando i requisiti dello Schema di Certificazione vengono modificati e possono avere un impatto sui Richiedenti certificati, gli Organismi di Certificazione comunicheranno tali modifiche ai propri Richiedenti e verificheranno che le attività di trattamento dei dati certificati siano conformi a tali modifiche in occasione del successivo audit di sorveglianza.

18.4.4. Versioni

Ogni documento rivisto deve essere rilasciato con un numero di versione incrementato.

18.4.5. Cronologia delle versioni e traccia delle modifiche

Il redattore deve conservare e rendere disponibile una versione del documento con le modifiche apportate rispetto alla versione precedente. Un riassunto delle principali modifiche apportate dall'ultima versione può essere incluso nella prima parte del documento o in un documento separato.

18.4.6. Classificazione di riferimento

La classificazione e l'identificazione della documentazione ufficiale dello Schema di Certificazione seguono le linee guida specificate nel documento *"Management and Classification of Europrivacy Documents"*.

18.5. Rilascio di documenti ufficiali

18.5.1. Revisione interna tra pari

I documenti normativi, i documenti informativi e i rapporti devono essere sottoposti a una revisione paritaria formale e interna e a un controllo prima di essere formalmente approvati e rilasciati.

18.5.2. Archivio ufficiale dei documenti Europrivacy

Tutti i documenti necessari per l'applicazione dello Schema di Certificazione (comprese le nuove versioni ufficiali dei documenti esistenti) sono disponibili sul sito web di Europrivacy Community and Resources: http://community.europrivacy.com

18.5.3. Effetti della Pubblicazione

Non appena un documento viene aggiornato e pubblicato sul sito web di Europrivacy Community and Resources, esso viene considerato il documento di riferimento da utilizzare, sostituendo qualsiasi versione precedente.

I processi di certificazione e di audit devono utilizzare l'ultima versione disponibile dello Schema di Certificazione e dei relativi documenti alla data di inizio del processo. Quando nel corso di un processo di certificazione e di audit vengono rilasciate nuove versioni dei documenti, è necessario tenerne conto e, per quanto possibile, conformarsi a questa nuova versione, ma è accettabile completare un processo in corso secondo la versione ufficiale al momento dell'inizio del processo di audit.

19. Organismi di certificazione Licenze e accreditamento

19.1. Principi Generali

L'uso di Europrivacy per rilasciare certificazioni è riservato agli Organismi di Certificazione che soddisfano i seguenti requisiti:

a) **L'Organismo di Certificazione deve essere autorizzato dallo Scheme Owner** a utilizzare lo Schema di Certificazione Europrivacy e le relative risorse attraverso un contratto di licenza scritto che chiarisca gli obblighi dell'Organismo di Certificazione nell'utilizzo di Europrivacy. L'elenco degli Organismi di Certificazione autorizzati viene mantenuto sul sito web pubblico di Europrivacy.
b) **L'Organismo di Certificazione deve richiedere e ottenere un accreditamento o un accordo formale e adeguato** in conformità alle normative nazionali applicabili.
c) **L'Organismo di Certificazione deve rispettare le specifiche dello Schema di Certificazione e le normative nazionali applicabili** e, quando rilascia una certificazione ai sensi dell'art. 43 del GDPR, le relative Linee Guida EDPB.

L'Organismo di Certificazione applicherà lo Schema di Certificazione come previsto, senza alcun adattamento, limitazione o estensione che non sia espressamente previsto e autorizzato dallo Schema di Certificazione.

L'accreditamento degli Organismi di Certificazione per il rilascio di certificazioni sulla protezione dei dati è di default sotto l'autorità della propria Autorità di Controllo e/o della propria Autorità nazionale di accreditamento. Lo Scheme Owner ha il diritto di monitorare, verificare e controllare il rilascio delle licenze di Europrivacy.

Ove applicabile, le normative e i meccanismi nazionali possono integrare, correggere o sostituire le prescrizioni menzionate in questa sezione.

19.1.1. Rapporti con le Autorità di accreditamento e di Controllo

Ai sensi dell'art. 43 del GDPR, gli Organismi di Certificazione accreditati dell'Unione Europea sono sotto il controllo dell'Autorità di Controllo e/o dell'Autorità di accreditamento. Nel caso in cui tali autorità siano incaricate di monitorare e controllare l'operato dell'Organismo di Certificazione, lo Scheme Owner rispetterà, sosterrà e collaborerà con l'Autorità di Controllo.

19.2. Procedura di autorizzazione

La procedura di autorizzazione intende creare fiducia nelle certificazioni Europrivacy, garantendo che solo i fornitori di servizi qualificati e affidabili siano autorizzati a utilizzare Europrivacy per fornire servizi ad altre aziende. Il processo di autorizzazione riduce il rischio di un uso inappropriato di Europrivacy e/o di fornitura di certificazioni inaffidabili.

Lo Scheme Owner deve definire, mantenere e aggiornare la procedura, la policy e l'insieme dei requisiti per le aziende interessate a essere autorizzate a eseguire e rilasciare certificazioni Europrivacy.

Le aziende interessate possono richiedere una licenza Europrivacy presentando una domanda con un file di presentazione dettagliato che illustri la loro esperienza nei processi di certificazione e in materia di protezione dei dati personali. L'elenco dei requisiti per la domanda iniziale viene fornito su richiesta dallo Scheme Owner. La società che presenta la domanda deve impegnarsi a rispettare la procedura e a coprire i costi e le tasse relative alla licenza.

Per impostazione predefinita, la procedura di richiesta seguirà un processo in due fasi. Tuttavia, le Autorità nazionali europee che desiderano utilizzare lo Schema di Certificazione per rilasciare certificazioni possono richiedere una licenza gratuita allo Scheme Owner attraverso una procedura semplificata.

19.2.1. Prima fase del processo - Valutazione dell'idoneità e concessione della licenza

Nella prima fase, lo Scheme Owner effettua una valutazione iniziale delle domande ricevute secondo una procedura e dei requisiti adottati dallo Scheme Owner. Esso valuterà gli elementi che possono avere un impatto sulla reputazione, lo sviluppo, l'imparzialità, la qualità e l'affidabilità delle attività di certificazione previste, quali:

a) la capacità di fornire servizi di alta qualità a un gran numero di Richiedenti;

b) il percorso e l'esperienza della società richiedente nelle attività di certificazione;
c) la qualificazione del personale della società richiedente, comprese le competenze in materia di protezione dei dati, sicurezza informatica e nelle attività di certificazione;
d) l'ubicazione e l'ambiente normativo, nonché le prassi aziendali che possono influire sull'imparzialità, l'indipendenza e l'affidabilità del processo di certificazione;
e) la qualità e l'ambizione della strategia per la fornitura di servizi relativi a Europrivacy.

Per valutare il rischio sull'imparzialità, l'indipendenza e l'affidabilità dei processi di certificazione, lo Scheme Owner può utilizzare indicatori relativi al rispetto dello stato di diritto, al livello di corruzione e alla libertà di stampa e di informazione nel Paese in cui si trova la sede centrale della società richiedente. Si terrà conto delle decisioni di adeguatezza ai sensi del Capitolo V del GDPR.

Lo Scheme Owner può anche prendere in considerazione altri parametri, come la reputazione e la fiducia, la sostenibilità a lungo termine dello Schema di Certificazione, la struttura del mercato e la domanda.

Se la società richiedente sembra soddisfare i criteri, lo Scheme Owner provvederà:
a) ad organizzare un incontro con la società richiedente;
b) a decidere se la società richiedente è idonea a diventare partner ufficiale;
c) se la decisione è positiva, a fornire alla società richiedente il contratto di licenza formale da firmare.

19.2.2. Seconda fase - Preparazione e accreditamento

La seconda fase della procedura di autorizzazione richiede all'Organismo di Certificazione di:
a) firmare il contratto di licenza;
b) completare il processo di preparazione (formazione degli esperti, sviluppo di una pagina web, ecc.);
c) richiedere un accreditamento o un accordo formale da parte di un'Autorità di Controllo.

19.2.3. Obblighi degli Organismi di Certificazione autorizzati

Gli Organismi di Certificazione autorizzati devono:
a) rispettare le regole e i requisiti dello Schema di Certificazione e garantire che i Target of Evaluation certificati siano conformi ai Criteri Europrivacy applicabili;
b) lavorare in stretta collaborazione con lo Scheme Owner e, se del caso, con l'Autorità di Controllo e/o l'Autorità di accreditamento;
c) rendicontare e fornire informazioni trasparenti sulle loro attività di certificazione;
d) monitorare annualmente la continua conformità delle certificazioni attive ai requisiti dello Schema di Certificazione;
e) promuovere lo Schema di Certificazione e contribuire alla sua reputazione positiva;
f) presentare allo Scheme Owner suggerimenti per migliorare lo Schema di Certificazione, compresi i criteri, le verifiche e i controlli.

19.2.4. Monitoraggio degli Organismi di Certificazione autorizzati

Il monitoraggio degli Organismi di Certificazione autorizzati può assumere diverse forme, tra cui:
a) esaminare la documentazione di certificazione (compresi i registri e i risultati);
b) fornire Observer o Auditor interni per gli audit condotti dall'Organismo di Certificazione;
c) richiedere le qualifiche degli Auditor;
d) qualsiasi altra azione o procedura ritenuta necessaria dallo Scheme Owner.

Gli Organismi di Certificazione dovranno collaborare pienamente e fornire senza ingiustificato ritardo le informazioni e la documentazione richieste, a seconda dei casi, dalla loro Autorità di Controllo , dalla loro Autorità di Accreditamento o dallo Scheme Owner.

19.2.5. Durata della licenza

Lo Scheme Owner è incoraggiato a monitorare e rivedere i propri accordi di licenza su base annuale e può decidere di sospendere o terminare l'accordo di licenza se un Partner o un Organismo di Certificazione non soddisfa i requisiti.

19.2.6. Scadenza della licenza

La scadenza o la cessazione di una licenza concessa a un Organismo di Certificazione non ha alcun effetto retroattivo sulle certificazioni già concesse da quell'Organismo di Certificazione, tranne nel caso in cui l'Autorità di Controllo o lo Scheme Owner abbiano motivo di ritenere inaffidabili tali certificazioni. In questi casi, un certificato può essere sospeso fino alla revisione e alla convalida da parte di un altro Organismo di Certificazione autorizzato. L'Autorità di Controllo, l'Autorità di accreditamento e/o lo Scheme Owner possono suggerire al Richiedente un Organismo di Certificazione sostitutivo.

19.3. Procedura di accreditamento o di accordo

Affinché una certificazione sia valida ai sensi del GDPR o di altre normative nazionali sulla protezione dei dati, l'Organismo di Certificazione deve aver ricevuto un accreditamento formale o un accordo rilasciato da un'Autorità di Controllo.

Gli accreditamenti rilasciati ai sensi dell'Art. 43 del GDPR si basano sulla ISO/IEC 17065.

19.3.1. Requisiti per l'accreditamento

L'accreditamento richiede una valutazione formale della capacità dell'Organismo di Certificazione di rispettare e applicare lo Schema di Certificazione. Esso richiede di valutare, tra l'altro:

a) Le competenze e l'esperienza richieste all'Organismo di Certificazione richiedente, tra cui:
   - Competenza ed esperienza in ambito ISO;
   - Competenza ed esperienza in materia di protezione dei dati.

b) La conformità con i requisiti delle infrastrutture e delle procedure, tra cui:
   - Requisiti ISO ed Europrivacy applicabili;
   - Requisiti relativi alla protezione dei dati.

c) La capacità, le competenze e le qualifiche delle Risorse Umane, compresa la disponibilità di auditor qualificati con conoscenze e competenze adeguate in materia di:
   - Processi di certificazione ISO;
   - GDPR e le normative applicabili in materia di protezione dei dati;
   - Cybersecurity;
   - Criteri, regole e procedure dello Schema di Certificazione Europrivacy.

Le regole e le procedure dello Schema di Certificazione sono ritenute sufficientemente dettagliate ed esaurienti da non richiedere all'Organismo di Certificazione di dimostrare la conformità alle ISO/IEC 17020 e 17025.

Le regole e le procedure di certificazione sono omogenee e rimangono le stesse, indipendentemente dal settore industriale e dal livello di complessità del Trattamento dei Dati. Di conseguenza, il rilascio dell'accreditamento non richiede di essere specifico per il settore.

L'accreditamento può essere soggetto a requisiti nazionali complementari.

Lo Scheme Owner può specificare una guida complementare per la procedura di accreditamento.

19.4. Processo di sospensione e ritiro

L'obiettivo principale di qualsiasi certificazione è garantire che il pubblico possa sviluppare fiducia nei Target of Evaluation certificati. Quando questa fiducia viene messa a repentaglio, le licenze e i certificati possono essere sospesi o ritirati.

19.4.1. Sospensione e revoca di accreditamenti e licenze

L'Autorità di Controllo e/o l'Autorità di Accreditamento sono competenti a sospendere o revocare l'accreditamento di un Organismo di Certificazione. Allo stesso modo, in caso di gravi inadempienze o di ripetute inadempienze minori rispetto allo Schema di Certificazione, lo Scheme Owner può sospendere o revocare la licenza concessa a un Organismo di Certificazione non conforme.

19.4.2. Sospensione e ritiro delle certificazioni consegnate

Le suddette autorità possono inoltre sospendere o ritirare le certificazioni concesse da un Organismo di Certificazione in qualsiasi situazione che metta a rischio la certificazione stessa o che possa indurre in errore il pubblico. Esempi di situazioni che possono portare alla sospensione o al ritiro dei certificati sono:

a) l'Organismo di certificazione sembra non aver rispettato o ignorato gli obblighi e i requisiti specificati nello Schema di Certificazione;
b) un beneficiario della certificazione sembra non essere conforme allo Schema di certificazione;
c) un beneficiario della certificazione sembra aver occultato informazioni relative alla sua politica e prassi in materia di protezione dei dati;
d) l'esistenza o l'uso di un certificato che possa indurre in errore il pubblico circa la conformità del trattamento dei dati certificato alla normativa in materia di protezione dei dati.

19.4.3. Processo decisionale di sospensione e di ritiro

La sospensione di una licenza o di un certificato consegnato può essere attuata immediatamente se giustificata per proteggere il pubblico e/o la reputazione dello Schema di Certificazione. L'organo decisionale adotterà misure ragionevoli per informare rapidamente il beneficiario dei motivi della sospensione e per consentirgli di fornire chiarimenti e/o proporre una serie di misure correttive.

Per impostazione predefinita, la revoca di una licenza o di un certificato consegnato sarà attuata solo dopo che il beneficiario avrà avuto un tempo ragionevole per fornire chiarimenti e/o proporre una serie di misure correttive. I beneficiari potenzialmente soggetti a revoca avranno almeno un periodo di 30 giorni per presentare chiarimenti/misure correttive prima che l'organo qualificato prenda una decisione sulla revoca della certificazione. Il periodo di 30 giorni decorre dal momento in cui l'organo decisionale comunica al beneficiario interessato l'avvio del processo di revoca.

Nel prendere la decisione di sospendere o revocare la certificazione, l'organo decisionale deve tenere conto del principio di proporzionalità, nonché dell'importanza di mantenere la fiducia del pubblico nell'affidabilità e nella serietà dello Schema di Certificazione.

Tutti gli Organismi di Certificazione e i Richiedenti si impegnano a rispettare e ad accettare le decisioni dell'Autorità di Controllo, dell'Autorità di Accreditamento e/o dello Scheme Owner accettano di rinunciare a qualsiasi diritto di risarcimento relativo a decisioni riguardanti la concessione, la sospensione o il ritiro della certificazione o della licenza, nella misura consentita.

Allegato 1 - Tabella riassuntiva dei criteri applicabili

La seguente tabella riassume l'applicabilità dei Criteri Europrivacy in base alla sede e all'attività del Richiedente.

		Applicant in the EEA		Applicant outside the EEA		
		Subject to the GDPR according to Art. 3 GDPR			NOT Subject to the GDPR under Art. 3 GDPR	
		Not exporting data	**Data Exporter**	**Data Controller subject to the GDPR**	**Data Importer only**	**Data Importer with onward transfers**
		Art. 42 and 3(1) GDPR	Art. 42 and 3(1) GDPR	Art. 42 and 3(2) GDPR	Art. 46 and 42 GDPR	Art. 46 and 42 GDPR
Criteria	**G.1**	YES	YES	YES	YES, except for G.1.1.3, G.1.1.4	YES, except for G.1.1.3, G.1.1.4
	G.2	YES	YES	YES	YES, except for G.2.2.1	YES, except for G.2.2.1
	G.3	YES	YES	YES	YES, except for G.3.2.1, G.3.2.2, G.3.2.3	YES, except for G.3.2.1, G.3.2.2, G.3.2.3
	G.4	YES	YES	YES	YES, except for G.4.1.4	YES, except for G.4.1.4
	G.5	YES	YES	YES	YES	YES
	G.6	YES	YES	YES	YES	YES
	G.7	YES	YES	YES	YES, except for G.7.1.2, G.7.1.3 and G.7.1.4	YES, except for G.7.1.2, G.7.1.3 and G.7.1.4
	G.8	YES	YES	YES	NO	NO
	G.9	YES	YES	YES	YES, except for G.9.1.3	YES, except for G.9.1.3
	G.10.1	NO	YES	YES	NO	NO
	G.10.2	NO	NO	NO	YES	YES
	G.10.3	NO	NO	NO	NO	YES
	T Criteria	YES	YES	YES	YES	YES
	C Criteria	YES	YES	YES	NO	NO
	S Criteria	YES	YES	YES	YES	YES

