Europrivacy™® Academy
GDPR Audit and Certification Courses

Europrivacy Academy

Implementation Course

www.academy.europrivacy.com

Europrivacy Academy

Implementation Course

v.3 del 2025

Informazioni su Europrivacy

Europrivacy è uno schema di certificazione sviluppato per valutare e certificare la conformità del trattamento dei dati al Regolamento Generale sulla Protezione dei Dati (GDPR) e alle normative nazionali complementari. Ha ricevuto l'approvazione del Comitato Europeo per la Protezione dei Dati (EDPB) come Sigillo Europeo per la Protezione dei Dati applicabile in tutte le giurisdizioni dell'UE.

Europrivacy consente una valutazione della conformità affidabile e sistematica, conforme ai principi ISO. È facilmente estensibile a normative complementari e tecnologie emergenti. Fornisce una metodologia efficiente per eseguire audit interni, identificare le Non Conformità residue e preparare il trattamento dei dati per la certificazione. Può essere utilizzato da DPO, auditor interni, consulenti e organismi di certificazione.

Europrivacy è gestito e supervisionato dal Comitato Internazionale di Esperti Europrivacy per mantenerlo aggiornato seguendo l'evoluzione della giurisprudenza sulla protezione dei dati personali, comprese le pubblicazioni dell'EDPB. Europrivacy è gestito amministrativamente dal Centro Europeo per la Certificazione e la Privacy (ECCP) di Lussemburgo ed è applicato da Organismi di Certificazione qualificati, nonché da studi legali e società di consulenza per supportare i loro clienti nel rispetto delle normative sulla protezione dei dati.

Informazioni sull'Europrivacy Academy

L'Europrivacy Academy offre corsi di formazione a coloro che sono interessati a ottenere una qualifica ufficiale di esperti Europrivacy. L'Europrivacy Academy si concentra sulla metodologia e sulle regole dello Schema di Certificazione Europrivacy. Si presuppone che gli studenti abbiano già familiarità con le normative sulla protezione dei dati. I corsi dell'Europrivacy Academy offrono un'esperienza di apprendimento personalizzata a un'ampia gamma di professionisti interessati.

Informazioni sul Manuale

L'Europrivacy Academy – il Manuale dell'Implementation Course di Europrivacy è un documento complementare fornito ai partecipanti all'Implementation Course Europrivacy su Europrivacy Academy. Questo Manuale intende fornire un supporto complementare e una sintesi del processo di certificazione, del ruolo degli implementers e dei criteri Europrivacy. Poiché il superamento dell'esame è necessario per ottenere una certificazione di competenza, il Manuale fornisce una simulazione di esame che può far conoscere agli studenti il tipo di esame e il tipo di domande a cui devono prepararsi.

Introduzione

Lo Schema di Certificazione Europrivacy specifica una metodologia chiara ed efficiente per valutare e certificare formalmente la conformità delle attività di trattamento dei dati al Regolamento Generale sulla Protezione dei Dati (GDPR) e ad altri obblighi complementari nazionali e/o specifici del settore. Si applica a un'ampia gamma di attività di trattamento dei dati, dai processi e servizi ai sistemi di gestione della protezione dei dati.

Dopo aver superato l'Introductory Course, conoscete già il quadro generale delle certificazioni GDPR e lo Schema di Certificazione Europrivacy. L'Implementation Course e il presente Manuale approfondiranno ulteriormente la comprensione del funzionamento del processo di certificazione, compreso il ruolo degli Implementers.

Il primo capitolo spiega il ruolo degli implementers nel processo di certificazione Europrivacy e illustra il processo di mantenimento e rinnovo delle certificazioni. Illustra inoltre la procedura di ricorso e di reclamo. **Il secondo capitolo** si concentra sulle regole relative alla gestione delle informazioni, compreso l'uso dei certificati e dei marchi di conformità. **Il terzo capitolo** fornisce una panoramica dettagliata sugli elenchi di criteri, verifiche e controlli di Europrivacy, compresa la loro applicazione e la specificazione del Target of Evaluation. Il Manuale si conclude con una sezione dedicata alla preparazione dei candidati all'esame finale, attraverso una simulazione di esame di 25 domande.

Tutti i riferimenti a qualsiasi documento devono essere intesi come riferimenti alla sua ultima versione. Quando viene rilasciata una nuova versione di un documento, questa sostituisce tutte le versioni precedenti dello stesso documento alla data di pubblicazione o alla fine del periodo di transizione. I processi di certificazione e di audit devono utilizzare l'ultima versione disponibile dello Schema di Certificazione Europrivacy e dei relativi documenti alla data di inizio del processo. Quando vengono rilasciate nuove versioni dei documenti durante un processo di certificazione e audit, la procedura di certificazione deve tenerne conto e, per quanto possibile, conformarsi alla nuova versione. Tuttavia, un processo in corso può essere completato secondo la versione ufficiale del momento in cui è iniziato.

In caso di dubbi relativi all'applicazione e/o all'interpretazione dei requisiti dello Schema di Certificazione, il documento a cui fare riferimento è la versione più recente dello Schema di Certificazione.

I documenti normativi e informativi specifici dello Schema di Certificazione rimangono sotto il controllo dello Scheme Owner assistito dal suo Comitato Internazionale di Esperti.

Gli esperti Europrivacy sono tenuti a procurarsi l'ultima versione dei documenti utilizzati attraverso il sito web della Community Europrivacy. I documenti forniti attraverso l'Europrivacy Academy sono strettamente finalizzati alla formazione e non costituiscono materiale ufficiale per lo svolgimento delle attività di certificazione.

Indice

Processo di certificazione Europrivacy

Ruolo degli Implementers

Nell'ecosistema Europrivacy, gli implementers qualificati lavorano per società di consulenza e supportano le organizzazioni nel garantire la costante conformità alle normative sulla protezione dei dati applicabili. Le società di consulenza non solo preparano i Richiedenti a certificare le loro attività di trattamento dei dati, ma li supportano continuamente durante il processo di certificazione e la fase di mantenimento.

L'obiettivo principale delle società di consulenza è quello di ridurre i rischi legali e finanziari per i Richiedenti. Gli implementers utilizzano i criteri Europrivacy per identificare potenziali lacune e non conformità residue che il Richiedente deve affrontare.

Gli implementers possono essere anche i DPO, interessati a convalidare e potenzialmente certificare la conformità del loro trattamento dei dati.

Come discusso in precedenza, il ruolo degli Implementers è duplice:

- Da un lato, gli implementers riducono i rischi legali e finanziari applicando una valutazione sistematica della conformità.
- D'altra parte, gli implementers supportano la preparazione e la documentazione delle attività di trattamento dei dati da certificare.

Figura 1 Il percorso dell'Implementer

Processo di preparazione Europrivacy

	FASE	LEAD	OBIETTIVI	RISORSE
1	Offerta di benvenuto	Partner	Preparare un'Offerta di Benvenuto Europrivacy per il Richiedente	Presentazione dell'Europrivacy Welcome Pack
2	Firma dell'offerta	Richiedente	Convalidare e firmare l'offerta	NA
3	Attivare il Welcome Pack	Partner	Attivare il Welcome Pack per il DPO del Richiedente	Attivazione del Welcome Pack con il supporto dell'ECCP
4	Selezionare le attività di trattamento dei dati	Partner	Selezionare con il Richiedente due attività di trattamento prioritarie da preparare	NA

5	Determinazione del Target of Evaluation	Partner	Determinazione del Target of Evaluation	A – Application & ToE Checklist
6	Preparare la documentazione	Partner	Preparare la documentazione richiesta, compresi inventari e NOCAR	Linee guida per il Richiedente; D – Documentation Checklist; Modelli
7	Verifica della conformità	Partner	Valutare la conformità del Target of Evaluation ai criteri, alle verifiche e ai controlli di Europrivacy	Criteri G, C, T, verifiche e controlli; Linee guida sull'uso dei criteri
8	Comunicare le lacune identificate	Partner	Elencare e comunicare al Richiedente le Non Conformità identificate	Elenco delle Non Conformità; Modello di Report di Valutazione Europrivacy
9	Correggere le Non Conformità	Richiedente	Affrontare e risolvere le Non Conformità identificate	Elenco delle Non Conformità
10	Convalidare la conformità	Partner	Controllare e convalidare che le Non Conformità siano state adeguatamente corrette	Criteri G, C, T, verifiche e controlli
11	Preparare la richiesta	Partner	Compilare e preparare la domanda da presentare all'Organismo di Certificazione	Modello di Richiesta di Europrivacy; A - Application & ToE Checklist
12	Richiedere la certificazione	Richiedente	Selezionare e richiedere a un Organismo di Certificazione la certificazione dei due trattamenti di dati selezionati	Modulo di richiesta online di Europrivacy
13	Supporto alla certificazione	Partner	Supportare il Richiedente durante il processo di certificazione	NA
14	Piano di certificazione	Partner	Elaborare un piano di certificazione per le restanti attività di trattamento dei dati del Richiedente	Modello di Piano di Certificazione
15	Offerta complementare	Partner	Fare un'offerta complementare per il trattamento dei dati rimanenti	NA
16	Riunione conclusiva e passi successivi	Partner	Presentare i risultati, raccogliere i feedback e presentare l'offerta complementare	NA
17	Firma della nuova offerta	Richiedente	Convalidare e firmare la nuova offerta	NA

Mantenimento, rinnovo e ricorsi

Mantenimento delle certificazioni

Ai sensi degli articoli 42 e 43 del GDPR, le misure di monitoraggio regolari sono obbligatorie per mantenere la certificazione durante il periodo di monitoraggio. Il periodo di monitoraggio di ciascuna certificazione deve essere documentato. In linea di principio, la certificazione Europrivacy dovrebbe essere concessa per **periodi rinnovabili di tre anni**, a partire dalla data dell'ultima certificazione e fino alla data di scadenza della stessa.

In questo periodo di tempo, il Richiedente deve assicurare la conformità del proprio Target of Evaluation ai requisiti e ai Criteri dello Schema di Certificazione e informare l'Organismo di Certificazione di qualsiasi cambiamento o preoccupazione in merito alla sua conformità. L'Organismo di Certificazione mantiene 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.

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 di successo devono essere seguite da:

- un primo Audit di Sorveglianza entro 12 mesi dalla data di certificazione;
- un secondo Audit di Sorveglianza entro 24 mesi dalla data di certificazione;
- 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.

Le attività di monitoraggio vengono eseguite per determinare se il Target of Evaluation del Richiedente continua a essere conforme ai requisiti dello Schema di Certificazione. La frequenza dell'audit può aumentare in base alla capacità del Richiedente certificato di soddisfare i requisiti.

Le modifiche alla normativa applicabile in materia di protezione dei dati, quali revisioni legislative, decisioni di tribunali nazionali o sovranazionali, decisioni dell'EDPB o della Commissione Europea, vengono monitorate e affrontate dall'Organismo di Certificazione. Se queste modifiche hanno un impatto sulle certificazioni rilasciate, l'Organismo di Certificazione:

- Valuta il livello di impatto sulla validità della certificazione;
- Elabora un Piano d'Azione;
- Contatta l'Autorità di Controllo e richiede la convalida del Piano d'Azione proposto;
- Attua il Piano d'Azione dopo che è stato approvato dall'Autorità di Controllo.

Ricertificazione

I certificati Europrivacy hanno un periodo di validità di tre anni e richiedono una valutazione di ricertificazione per essere rinnovati. L'Organismo di Certificazione decide di rinnovare la certificazione in base ai risultati dell'audit di ricertificazione, nonché ai risultati della revisione del sistema durante il periodo di certificazione e ai reclami ricevuti dagli utenti della certificazione. Lo scopo dell'audit di ricertificazione è confermare la continua conformità del Target of Evaluation ai requisiti Europrivacy.

Ricorsi e reclami

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 processo di dati certificato non sia conforme allo Schema di Certificazione o alle normative applicabili in materia di protezione dei dati può presentare il proprio reclamo al Richiedente certificato, all'Organismo di Certificazione o all'Autorità di Controllo competente.

In base alle prove comunicate, la parte ricevente deve informare 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 viene 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.

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:

- conferma la ricezione di un reclamo o di un appello formale;
- raccoglie e verifica tutte le informazioni pertinenti;
- dà comunicazione formale dell'esito della procedura al reclamante o al ricorrente;
- intraprende qualsiasi azione successiva necessaria per risolvere il reclamo o l'appello;
- informa lo Scheme Owner di qualsiasi problema importante che possa costituire un rischio per lo Schema di Certificazione o per la sua reputazione.

Se i reclami sono ritenuti validi, l'Organismo di Certificazione deve affrontarli in modo appropriato e deve compiere uno sforzo ragionevole per risolverli. Il Richiedente e l'Organismo di Certificazione devono fornire pieno supporto per indagare e fornire chiarimenti per elaborare e risolvere il reclamo. Un reclamo fondato può portare alla sospensione o al ritiro del certificato.

Per garantire un processo imparziale, le decisioni relative a un reclamo o a un appello sono adottate da persone che:

- non sono stati direttamente coinvolti nel relativo processo di certificazione;
- non ha fornito servizi alla Parte ricorrente o al Richiedente Certificato.

Gestione delle informazioni e della riservatezza

Gestione delle informazioni e della riservatezza

L'Organismo di Certificazione deve disporre di una metodologia di documentazione standardizzata. La documentazione prodotta durante la valutazione dovrebbe concentrarsi su tre aspetti principali:

- La consistenza e la coerenza dei metodi di valutazione eseguiti;
- L'adeguatezza dei metodi per dimostrare la conformità del Target of Evaluation ai criteri di certificazione e quindi al regolamento sulla protezione dei dati;
- L'imparzialità del processo decisionale.

Gli Organismi di Certificazione devono utilizzare una metodologia e un processo chiari e coerenti per classificare e identificare la documentazione, al fine di garantire che il processo di certificazione sia affidabile e ben specificato, oltre che chiaro e di facile utilizzo. La classificazione e l'identificazione della documentazione ufficiale dello Schema di Certificazione seguono le linee guida specificate nel documento *Gestione e Classificazione dei Documenti Europrivacy*. Ogni documento rivisto viene rilasciato con un numero di versione incrementato.

Per quanto riguarda la documentazione fornita dallo Scheme Owner, i processi di Certificazione e audit devono utilizzare l'ultima versione disponibile dello Schema di Certificazione e dei relativi documenti alla data di inizio del processo. Quando vengono rilasciate nuove versioni dei documenti durante un processo di certificazione e audit, questo deve tenerne conto e, per quanto possibile, conformarsi ai requisiti della nuova versione.

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

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. Di default, tutte le informazioni fornite dal Richiedente o relative al Richiedente e alla sua certificazione sono trattate come informazioni riservate, tranne nel caso in cui l'informazione:

- è disponibile pubblicamente;
- è qualificata come non confidenziale dal Richiedente;
- è divulgata con il consenso del Richiedente; e/o
- deve essere divulgata per motivi legali o contrattuali.

La riservatezza non si applica alle informazioni che devono essere pubblicate sul Registro delle Certificazioni e non impedisce l'accesso legittimo alle informazioni da parte di soggetti autorizzati, come le Autorità di Controllo. L'Organismo di Certificazione può essere obbligato per legge a rilasciare informazioni riservate e deve soddisfare tali richieste. L'Autorità di Controllo e lo Scheme Owner possono richiedere l'accesso a informazioni riservate per

svolgere i loro compiti, come la sorveglianza e il trattamento dei reclami delle certificazioni. Solo le persone autorizzate, con l'obbligo formale e contrattuale di preservare la riservatezza delle informazioni, devono avere accesso ai dati e ai file archiviati.

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

Di default, l'Organismo di Certificazione rende **pubbliche le informazioni generali** sul:

- Processo di valutazione della certificazione;
- Processo decisionale relativo alla certificazione e al suo ambito;
- Tipi di sistemi di gestione e Schemi di Certificazione in cui opera;
- L'uso del nome, del logo e del marchio di conformità dell'Organismo di Certificazione;
- Processi in atto per la gestione delle richieste di informazioni, dei reclami e dei ricorsi;
- La policy e il meccanismo dell'imparzialità;
- Dati di contatto dell'Organismo di Certificazione, come l'indirizzo postale;
- L'informativa dell'Organismo di Certificazione e la procedura per contattare il suo DPO.

Su richiesta, l'Organismo di Certificazione deve fornire informazioni complementari su:

- Le aree geografiche in cui opera l'Organismo di Certificazione;
- Lo stato di una determinata certificazione;
- Il nome, il documento normativo correlato, il campo di applicazione e l'ubicazione geografica del Richiedente certificato;
- Informazioni sullo Schema di Certificazione;
- Una descrizione dei mezzi con cui l'Organismo di Certificazione ottiene il sostegno finanziario e informazioni generali sulle tariffe applicate ai Richiedenti;
- Una descrizione dei diritti e dei doveri dei Richiedenti;
- Informazioni sulle procedure di gestione dei reclami e dei ricorsi.

Lo Scheme Owner si occupa della gestione e supervisione del sito ufficiale di Europrivacy, che include l'archivio dei documenti di riferimento ufficiali e il registro online delle certificazioni Europrivacy rilasciate. Gli Organismi di Certificazione possono replicare le informazioni pubbliche sul proprio sito web, purché siano coerenti con le informazioni fornite dallo Scheme Owner. Gli Organismi di Certificazione mantengono aggiornate le informazioni pubblicate nel Registro ufficiale dei Certificati di Europrivacy e devono evitare qualsiasi ritardo nell'aggiornamento delle informazioni. Gli Organismi di Certificazione autorizzati devono fornire un link dal loro sito web al Registro dei Certificati di Europrivacy dei certified Objects e al Sito Web delle Informazioni Pubbliche.

Uso di marchi di conformità, licenze e certificati

Una volta concluso il processo di certificazione e pubblicata la certificazione rilasciata nel Registro dei Certificati di Europrivacy, i Richiedenti certificati possono iniziare a utilizzare il logo e il marchio di conformità di Europrivacy. **Il logo e il marchio di conformità Europrivacy**

sono 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.

Il marchio di conformità:

- fornisce informazioni chiare sullo schema di certificazione e sul campo di applicazione;
- impedisce qualsiasi comunicazione fuorviante in merito all'ambito della certificazione;
- consente di risalire all'Organismo di Certificazione e al suo Registro.

Non devono esserci ambiguità, nel marchio o nel testo di accompagnamento, per quanto riguarda l'Organismo di Certificazione che ha concesso la certificazione o l'entità della stessa.

L'Organismo di Certificazione e lo Scheme Owner hanno il diritto di esercitare un 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. Verificano, nella documentazione o in altri mezzi pubblicitari, se ci sono riferimenti errati allo Schema di Certificazione o un uso fuorviante di licenze, certificati, marchi o altri meccanismi.

L'ECCP è responsabile dell'uso corretto e dell'integrità del marchio, del logo, del sigillo e dei loghi secondari di Europrivacy su tutte le pubblicazioni, gli articoli promozionali e le attrezzature, siano essi prodotti dai partner di Europrivacy o da un'agenzia esterna.

Principi chiave

Europrivacy raccoglie alcuni principi chiave per quanto riguarda l'uso del marchio:

- Qualsiasi utilizzo del marchio Europrivacy e/o ECCP richiede il previo consenso scritto ed esplicito o la licenza da parte di ECCP.
- L'uso del termine Europrivacy e/o del logo Europrivacy deve sempre rispettare le linee guida indicate.
- L'ECCP non permette l'uso del nome o della grafica di Europrivacy in alcun annuncio, pubblicità, pubblicazione o relazione che possa:
    - implicare l'approvazione di qualsiasi prodotto o servizio non collegato a Europrivacy; oppure
    - ingannare terzi in merito alle certificazioni rilasciate.
- La documentazione di Europrivacy e il materiale di comunicazione fornito dall'ECCP sono protetti da copyright e non possono essere riprodotti, copiati, diffusi, modificati o venduti senza l'espressa autorizzazione scritta dell'ECCP.
- I terzi che utilizzano il marchio Europrivacy devono attenersi alle istruzioni ricevute dall'ECCP.

Marchio e logo Europrivacy

Figura 1 Marchio e logo Europrivacy

Il termine Europrivacy e il logo Europrivacy sono marchi internazionali gestiti dall'ECCP. I marchi testuali e visivi sono registrati in diverse giurisdizioni, tra cui gli Stati Uniti.

Il marchio verbale di Europrivacy è "Europrivacy".

Il logo di Europrivacy è composto dalle lettere "E" e "P" di colore blu, con sei stelle gialle, come mostrato nell'immagine. Il monogramma è spesso associato ai simboli del marchio e del marchio registrato, nonché a testi complementari.

Il marchio e la sigla di Europrivacy non devono essere alterati, trasformati, spezzati o utilizzati in modo da essere percepiti come un brand nuovo o diverso. Il **marchio verbale** e il **monogramma** devono essere chiaramente esposti e visibili in un'area di spazio libero che li circonda.

Certificati

Le attività di trattamento dei dati certificate possono ricevere un certificato Europrivacy, sotto il controllo e l'approvazione dell'Organismo di Certificazione. I certificati devono includere:

- Il logo dell'Organismo di Certificazione e di Europrivacy;
- Nome del Richiedente certificato;
- Se il Richiedente agisce in qualità di Titolare del trattamento, di Responsabile del trattamento o di Contitolare del trattamento;
- Ove applicabile, il nome dei Contitolari del trattamento;
- Descrizione chiara del Target of Evaluation e della sua portata geografica;
- Ove applicabile, eventuali Estensioni applicate;
- Date di emissione e di scadenza del certificato;
- Identificatore univoco del certificato consegnato;
- La dicitura "Maggiori informazioni su" seguita dal nome del dominio del sito web dello Schema di Certificazione e del Registro online dei certificati;.
- Nome e 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.

Marchio di conformità

Le attività di trattamento dei dati certificate possono essere contrassegnate con il marchio di conformità Europrivacy, sotto il controllo e l'approvazione dell'Organismo di Certificazione. Il Marchio di Conformità comprende:

- Logo Europrivacy;
- Identificatore unico di certificazione;
- Nome di dominio del sito web dello Schema di Certificazione.

Inoltre, il Marchio di Conformità può includere estensioni dell'ambito di certificazione, come mostrato nell'esempio.

Figura 2 Marchio di conformità Europrivacy

Dichiarazione di conformità

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 3 Dichiarazione di conformità Europrivacy

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

La Dichiarazione comprende:

- il riferimento a Europrivacy e, ove autorizzato, il logo Europrivacy;
- il nome del Richiedente certificato;
- se del caso, il nome del/i contitolare/i del trattamento;
- una chiara indicazione del Target of Evaluation e della sua portata geografica;
- se del caso, una chiara indicazione delle norme o dei requisiti complementari che sono stati aggiunti;
- le date di emissione e di validità del certificato;
- l'identificatore univoco del certificato consegnato;
- la dicitura "Maggiori informazioni su" seguita dal nome del dominio del sito web dello Schema di Certificazione e del Registro online dei certificati;
- e il nome e l'indirizzo dell'Organismo di Certificazione che rilascia il certificato.

Se la certificazione viene 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.

Altre considerazioni

Se un certificato, una dichiarazione o un marchio di conformità relativo a una certificazione Europrivacy viene visualizzato su un supporto elettronico, come una pagina web o un documento pdf, deve includere un collegamento ipertestuale diretto alla homepage principale dello Schema di Certificazione o alla pagina specifica del Target of Evaluation certificato nel Registro online. I marchi di conformità, i certificati e le dichiarazioni di certificazione non devono essere utilizzati in modo tale da causare confusione o comunicazioni fuorvianti sul Target of Evaluation della certificazione di riferimento.

L'Organismo di Certificazione deve esercitare un adeguato controllo sulla proprietà dell'uso e del riferimento ai certificati da lui rilasciati e deve intervenire in caso di riferimenti errati allo stato di certificazione o di uso fuorviante di documenti di certificazione, marchi o 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.

Elenco dettagliato di criteri, verifiche e controlli

Criteri, verifiche e controlli Europrivacy

Criteri di valutazione

I criteri di valutazione sono applicati in conformità all'ultima versione dei requisiti dello Schema di Certificazione Europrivacy. L'Organismo di Certificazione applica i criteri di valutazione:

- Tenendo conto dei diritti degli interessati e dei rischi potenziali per i loro dati personali;
- In modo coerente e omogeneo;
- In modo verificabile e controllabile;
- Tenendo conto delle dimensioni dell'organizzazione, della natura del trattamento dei dati e dei rischi identificati per i dati e gli interessati.

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

- Identificazione dei dati personali trattati;
- Rispetto dei requisiti per le informazioni sulle attività di trattamento dei dati fornite agli interessati;
- Liceità del trattamento e conformità ai requisiti del "Consenso Informato Preventivo";
- Rispetto dei requisiti relativi ai minori di età;
- Conformità al principio di minimizzazione dei dati by design and by default;
- Conformità al principio di trasparenza come specificato dal GDPR;
- L'analisi del flusso di dati personali, comprese le questioni relative al Responsabile del trattamento e al trasferimento transfrontaliero dei dati;
- Ciclo di vita dei dati personali e minimizzazione dei periodi di conservazione dei dati personali;
- Attuazione effettiva dei diritti dell'interessato;
- Presenza e conformità dei dati indiretti;
- Attuazione di misure idonee a salvaguardare i diritti, le libertà e gli interessi legittimi dell'interessato nel contesto del processo decisionale individuale automatizzato;
- Sicurezza ed efficace protezione e integrità dei dati raccolti;
- Implementazione di misure tecniche e organizzative adeguate per la protezione dei dati da parte del Titolare del trattamento;
- In caso di ricorso a Responsabili del trattamento, l'accordo sulle procedure consente al Titolare del trattamento di assicurarsi che i Responsabili forniscano garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate;
- Se inclusi nel campo di applicazione della certificazione, i requisiti normativi e i criteri complementari nazionali e/o specifici del settore.

I criteri di valutazione sono tradotti in elenchi dettagliati di criteri, verifiche e controlli gestiti dallo Scheme Owner e resi disponibili alle Autorità di Controllo e alle terze parti autorizzate.

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

I criteri, le verifiche e i controlli di Europrivacy sono resi disponibili attraverso il Welcome Pack e il sito web della community Europrivacy in varie forme. I criteri Europrivacy possono essere utilizzati anche attraverso software di valutazione della conformità e soluzioni di partner qualificati.

Criteri fondamentali

Oltre agli obblighi fondamentali del GDPR, i Targets of Evaluation possono essere soggetti a normative nazionali o specifiche del settore.

L'elenco dei criteri più importanti è:

1. I **GDPR Core Criteria** di Europrivacy che raccolgono i requisiti del GDPR applicabili a tutti i trattamenti di dati.

È completato da tre serie di requisiti complementari:

2. **Verifiche e Controlli Contestuali Complementari** per valutare la conformità ai requisiti specifici del dominio e della tecnologia.
3. **Verifiche e Controlli delle Misure Tecniche e Organizzative** per valutare le misure di sicurezza messe in atto per proteggere i dati trattati.
4. **Obblighi Nazionali di Protezione dei Dati** con la loro protezione complementare.

Requisiti nazionali e normativi complementari

Le certificazioni GDPR ai sensi dell'Art. 43 GDPR richiedono che il trattamento dei dati certificato sia conforme agli obblighi nazionali dell'UE del paese in cui ha sede il titolare del trattamento o il responsabile del trattamento. Tali obblighi comprendono anche tutte le normative nazionali specifiche del settore relative alla protezione dei dati personali applicabili al Target of Evaluation. Ogni Paese ha leggi e regolamenti nazionali distinti che hanno un impatto ed estendono i requisiti per la protezione dei dati. Il Richiedente deve assicurarsi che il proprio Target of Evaluation sia conforme alle normative nazionali applicabili, monitorandone al contempo la revisione.

Il Richiedente che presenta la domanda dallo Spazio Economico Europeo (SEE) deve richiedere l'intervento di un esperto con adeguata competenza legale per valutare la conformità del proprio Target of Evaluation con gli obblighi nazionali aggiuntivi che superano quelli del GDPR nel Paese di applicazione. I risultati della valutazione devono essere riportati in una relazione scritta: il "*National Obligation 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 con l'obbligo nazionale pertinente nel Paese di applicazione, soggetta allo stesso livello di requisiti del NOCAR.

Requisiti delle Misure Tecniche e Organizzative Complementari

La certificazione Europrivacy richiede l'adozione di Misure Tecniche e Organizzative adeguate per la protezione dei dati trattati e conservati.

Per valutare l'adeguatezza della sicurezza del trattamento dei dati sono stati specificati le verifiche e controlli delle Misure Tecniche e Organizzative Complementari. Tali verifiche e controlli integrano i criteri fondamentali e sono obbligatori per tutti i Targets of Evaluation, tranne nel caso in cui il Target of Evaluation:

- è coperto da una certificazione ISO/IEC 27001 valida; e
- non esegue alcun Trattamento di Dati ad Alto Rischio.

Requisiti complementari contestuali e specifici del settore

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

Processo di certificazione

La valutazione di conformità di Europrivacy è organizzata in una sequenza ben strutturata di criteri, verifiche e controlli.

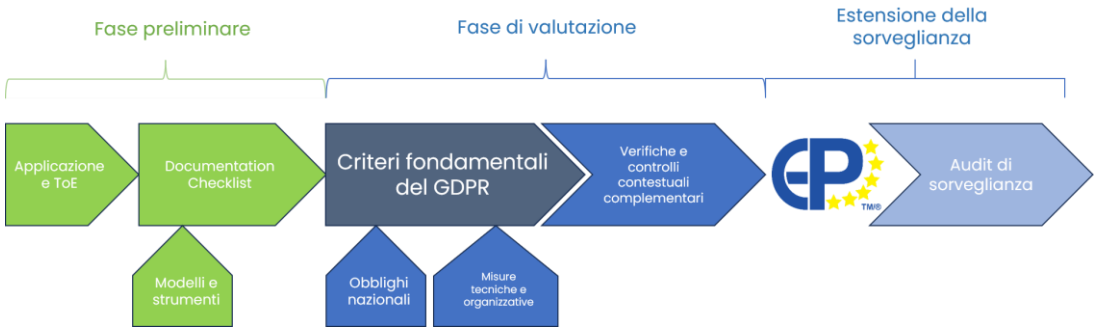


Figura 4 Processo di certificazione Europrivacy e verifiche e controlli applicabili

La fase preliminare mira a garantire che il Target of Evaluation sia pronto per essere valutato.

Le **verifiche e controlli** della **Richiesta** e del **Target of Evaluation** sono utilizzati dall'Organismo di Certificazione per valutare l'adeguatezza della determinazione del Target of Evaluation alle linee guida stabilite dall'EDPB. Tali verifiche e controlli possono essere preparati dal Richiedente, ma devono essere convalidati dall'Organismo di Certificazione prima di iniziare il processo di valutazione.

La **Documentation checklist** mira a facilitare la raccolta della documentazione e a garantire che il team di Audit abbia accesso alla documentazione richiesta. Deve essere completata dal Richiedente e convalidata dal Lead Auditor prima di iniziare la valutazione.

L'adeguatezza del Target of Evaluation e della documentazione disponibile deve essere convalidata dal Lead Auditor prima di avviare il processo di valutazione stesso.

Le seguenti verifiche e controlli sono utilizzati per valutare la conformità del Target of Evaluation con Europrivacy. Il Richiedente può preparare prove per soddisfare i vari criteri, ma la convalida formale è di esclusiva responsabilità dell'Organismo di Certificazione.

I **GDPR Core Criteria** costituiscono la spina dorsale di tutti i processi di certificazione di Europrivacy e vengono applicati dagli auditor dell'Organismo di Certificazione a ogni singolo Target of Evaluation, indipendentemente dal suo ambito di applicazione e dalla sua ubicazione. I GDPR Core Criteria consentono una valutazione sistematica della conformità agli obblighi contenuti nel GDPR. Assicurano che tutte le certificazioni Europrivacy garantiscano un elevato livello di conformità al GDPR. Questo elenco è obbligatorio per tutte le certificazioni.

Le **Verifiche e Controlli Contestuali Complementari** sono definiti per valutare i requisiti di protezione dei dati specifici del settore e della tecnologia. Essi tengono conto delle pubblicazioni e delle linee guida dell'EDPB e delle Autorità di Controllo, nonché dell'esperienza della comunità di ricerca. Questo elenco è obbligatorio per ogni certificazione. Le Verifiche e Controlli Contestuali Complementari sono raggruppati in vari sottoinsiemi di verifiche e controlli applicabili a tecnologie e settori applicativi specifici. L'Organismo di Certificazione deve scorrere l'elenco e deve valutare e verificare tutti i sottoinsiemi applicabili al Target of Evaluation.

La certificazione Europrivacy richiede l'adozione di misure tecniche e organizzative adeguate per la protezione dei dati trattati. Le **Verifiche e Controlli delle Misure Tecniche e Organizzative** mirano a valutare la conformità delle misure adottate dal Richiedente per garantire la sicurezza e la protezione dei dati trattati.

Europrivacy ha definito alcune verifiche e controlli complementari da applicare quando si eseguono audit di **Sorveglianza o di Ricertificazione** per valutare gli obblighi specifici dei trattamenti di dati già certificati, come l'obbligo di fornire informazioni sui trattamenti di dati certificati nelle lingue degli Stati membri.

Il modello di **Elenco di Non Conformità** deve essere utilizzato dall'Organismo di Certificazione per segnalare ed elencare le non conformità identificate che il Richiedente deve affrontare per essere certificato. In alternativa, l'Organismo di Certificazione può utilizzare i propri modelli per segnalare le non conformità.

L'informative checklist for certificate publication è messa a disposizione dell'Organismo di Certificazione per garantire che tutti i requisiti amministrativi siano soddisfatti prima di rilasciare un certificato Europrivacy.

ID	Elenco di verifiche e controlli	Stato	Lead	Alternativa	CF	CB
A	**Application e Target of Evaluation**	**Obbligatorio**	**CB**	**No**	**X**	**X**
I	Inventari da compilare o fornire da parte del Richiedente	Informativo	Richiedente	Registro del trattamento dei dati	X	X
D	**Convalida della documentazione**	**Informativo**	**App. e CB**	**No**	**X**	**X**
E	Evaluation of Datasets	Informativo	App. e CB	CB Management System	X	X
G	**Criteri fondamentali del GDPR**	**Obbligatorio**	**CB**	**No**	X	X
C	**Verifiche e controlli complementari e contestuali**	**Obbligatorio**	**CB**	**No**	**X**	**X**
T	**Misure tecniche e organizzative (TOM)**	**Obbligatorio**	**CB**	**ISO 27001/27701**	**X**	**X**
N	Requisiti nazionali	Informativo	CB	Valutazione legale	X	X
S	**Audit di sorveglianza**	**Obbligatorio**	**CB**	**No**	**X**	**X**
NC	**Elenco delle Non Conformità**	**Obbligatorio**	**Solo CB**	**CB Management System**		**X**
Z	Certificate Publication Checklist	Informativo	Solo CB	CB Management System		X

Figura 5 Applicabilità di verifiche e controlli

Applicabilità specifica

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:

- Titolari del trattamento
- Responsabili del trattamento
- Sia a Titolari che a Responsabili del trattamento

Al fine di affrontare il tema della proporzionalità e di differenziare i trattamenti di dati semplici da quelli più ampi e sensibili, un'altra colonna differenzia i criteri, le verifiche e i controlli nelle seguenti categorie:

- Obbligatorio di default per tutti i processi di certificazione
- Non è richiesto per la certificazione di semplici trattamenti di dati, ma è obbligatorio per la certificazione di qualsiasi Attività di Trattamento di Dati ad Alto Rischio, definita come elaborazione di dati 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.
- La categoria Esenzioni serve a determinare se è possibile giustificare un'esenzione da un requisito di un criterio.

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

- **S**pecifici per ogni trattamento dei dati
- **G**enerici e comuni per diversi trattamenti di dati

Un'altra colonna specifica se il criterio è applicabile agli Importatori di Dati con sede al di fuori dello Spazio Economico Europeo che non sono direttamente soggetti al GDPR, dove:

- **R** indica che il criterio è richiesto per gli Importatori di Dati con sede al di fuori del SEE;
- **NR** indica che il criterio non è richiesto per gli Importatori di Dati con sede al di fuori del SEE.

Formato dei criteri

I criteri sono formulati come clausole "devono" che sono articolate con chiare relazioni logiche utilizzando le parole "E", "O" e "SE...ALLORA".

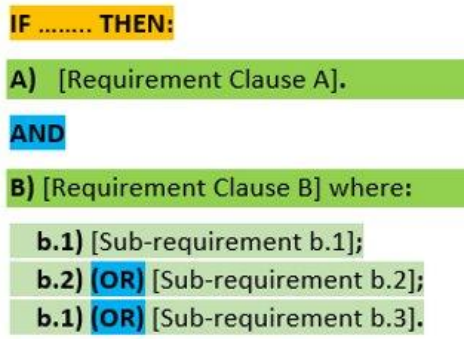


Figura 7 Formato dei criteri

Le clausole Condizionali consentono di limitare l'applicabilità di un criterio a determinate condizioni. Iniziano con la parola "SE" e terminano con "ALLORA". Se le condizioni sono applicabili al trattamento dei dati, allora i relativi criteri successivi devono essere valutati. Se la condizione non è applicabile, allora i criteri successivi possono essere saltati.

I criteri sono specificati in una o più clausole che specificano i requisiti formali, denominate **Clausola di Requisito**. Un criterio può contenere più Clausole di Requisiti. Ogni Clausola di Requisito inizia con una lettera maiuscola e una parentesi.

Quando i criteri includono più Clausole di Requisiti, tra ogni Clausola di Requisiti viene specificato un termine di **Relazione Booleana**.

Ogni clausola principale può contenere facoltativamente un insieme di **Sottorequisiti**. L'elenco dei Sottorequisiti è preceduto da una colonna (":"). Ogni Sottorequisito:

- inizia con la lettera della clausola di Requisito principale corrispondente, seguita da un punto e da un numero;
- include un termine di relazione Booleano tra parentesi, tranne che per il primo Sottorequisito dell'elenco;
- termina con una semicolonna se il Sottorequisito è seguito da un altro Sottorequisito, o con un punto se è l'ultimo Sottorequisito dell'elenco.

Specificare il Target of Evaluation

Il Target of Evaluation specifica e delimita l'ambito delle attività di trattamento dei dati personali da certificare. Deve essere chiaramente specificato e comprensibile da terzi, compresi gli interessati. Una certificazione GDPR non può essere rilasciata a livello di un'intera azienda o del suo sistema di gestione. È considerata troppo ampia e non abbastanza specifica per essere efficace e affidabile. Occorre invece considerare le singole attività di trattamento dei dati, come i database dei clienti, il servizio di assistenza ai clienti,

i servizi di gestione degli stipendi e della contabilità, il sito web aziendale o un'applicazione per smartphone.

La determinazione del Target of Evaluation presenta una certa flessibilità e libertà. Può includere una o più operazioni di trattamento con finalità distinte. Tuttavia, il Target of Evaluation deve avere un certo livello di omogeneità per quanto riguarda la fonte dei dati trattati e lo scopo generale dell'attività di trattamento da certificare. Se il Target of Evaluation coinvolge diverse giurisdizioni e/o entità legali, la sua determinazione deve essere coerente con il controllo effettivo e la responsabilità delle attività di trattamento dei dati da certificare. Ciò può comportare l'esecuzione e la consegna di una certificazione in più segmenti.

L'Organismo di Certificazione dovrà valutare ogni attività di trattamento dei dati inclusa nel Target of Evaluation. La documentazione di certificazione deve essere assolutamente trasparente e chiara.

Il Target of Evaluation deve essere formalmente specificato con una chiara descrizione dell'attività di trattamento dei dati personali da certificare. La determinazione deve includere informazioni dettagliate come la fonte da cui provengono i dati, le categorie di dati personali, le categorie di soggetti interessati, le finalità del trattamento dei dati, i Paesi in cui avviene il trattamento, il coinvolgimento di responsabili del trattamento, la descrizione narrativa del trattamento, ecc.

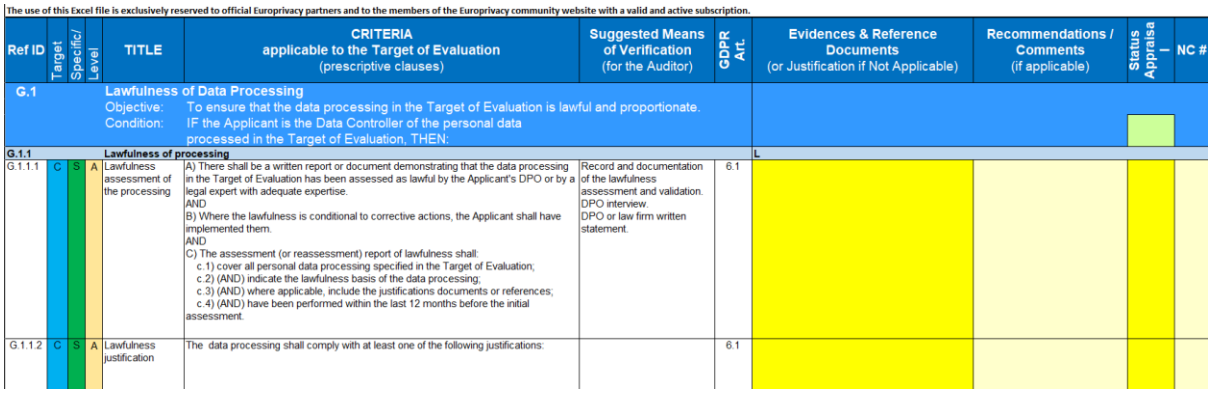
Il processo di definizione del Target of Evaluation si articola in 6 fasi principali.

1. **Selezionare l'attività di trattamento dei dati.** Iniziare con le attività di trattamento dei dati prioritarie, ad esempio in termini di rischio per il Richiedente.
2. **Specificare e mappare il Target of Evaluation.** Specificazione e mappatura dei flussi di dati personali nel Target of Evaluation, utilizzando il Modulo di Richiesta per la Certificazione Europrivacy.
3. **Verificare l'adeguatezza del Target of Evaluation** applicando il documento Verifiche e Controlli Preliminari sulla Richiesta e sul Target of Evaluation per validarne la completezza e l'adeguatezza.
4. **Documentare la conformità del Target of Evaluation** verificando e documentando come le attività di trattamento dei dati nel Target of Evaluation siano conformi ai criteri Europrivacy applicabili. Questa fase riduce già significativamente i rischi.
5. **Certificare il Target of Evaluation.** Il certificato di conformità consentirà al Richiedente di dimostrare, valorizzare e comunicare la propria conformità.
6. **Mantenere e godere della conformità.** Una volta certificati, è importante continuare a garantire che le attività di trattamento dei dati siano conformi, con l'aiuto delle risorse online che, tra le altre funzionalità, forniscono anche notifiche sui cambiamenti normativi. Gli audit di sorveglianza successivi dimostreranno se il Richiedente ha mantenuto e continua a mantenere la propria conformità nel tempo.

Struttura della tabella e modalità di compilazione

Struttura orizzontale della tabella

L'elenco è strutturato in diverse schede. La scheda "Criteri GDPR" raccoglie i criteri, le verifiche e i controlli fondamentali che vengono affrontati in ogni singolo audit.



The use of this Excel file is exclusively reserved to official Europrivacy partners and to the members of the Europrivacy community website with a valid and active subscription.

Ref ID	Target	Specific/	Level	TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	Suggested Means of Verification (for the Auditor)	GDPR Art.	Evidences & Reference Documents (or Justification if Not Applicable)	Recommendations / Comments (if applicable)	Status Appraisa l	NC #
G.1				Lawfulness of Data Processing Objective: To ensure that the data processing in the Target of Evaluation is lawful and proportionate. Condition: IF the Applicant is the Data Controller of the personal data processed in the Target of Evaluation, THEN:							
G.1.1				Lawfulness of processing				L			
G.1.1.1	C	S	A	Lawfulness assessment of the processing	A) There shall be a written report or document demonstrating that the data processing in the Target of Evaluation has been assessed as lawful by the Applicant's DPO or by a legal expert with adequate expertise. AND B) Where the lawfulness is conditional to corrective actions, the Applicant shall have implemented them. AND C) The assessment (or reassessment) report of lawfulness shall: c.1) cover all personal data processing specified in the Target of Evaluation; c.2) (AND) indicate the lawfulness basis of the data processing; c.3) (AND) where applicable, include the justifications documents or references; c.4) (AND) have been performed within the last 12 months before the initial assessment.	Record and documentation of the lawfulness assessment and validation. DPO interview. DPO or law firm written statement.	6.1				
G.1.1.2	C	S	A	Lawfulness justification	The data processing shall comply with at least one of the following justifications:		6.1				

Figura 6 Struttura orizzontale della tabella

La tabella Excel è composta dalle seguenti colonne:

1. La colonna **Ref ID** fornisce un identificativo unico e distinto per ogni singola verifica e controllo.
2. La colonna **Target** definisce a chi sono applicabili le verifiche e i controlli:
   - Solo ai **T**itolari del trattamento.
   - Solo ai **R**esponsabili del trattamento.
   - sia ai **T**itolari che ai **R**esponsabili del trattamento.
3. La colonna **"Specific/Generic" (Specifico/Generico)** chiarisce se le verifiche e i controlli sono specifici o generici.
4. La colonna **"Level" (Livello)** specifica il livello delle verifiche e dei controlli.
5. La colonna **"Title" (Titolo)** indica il titolo delle verifiche e dei controlli.
6. La colonna **"Criteria" (Criteri)** descrive il requisito formale che deve essere implementato dal Richiedente e valutato dall'auditor. I criteri sono clausole prescrittive che il Richiedente deve rispettare.
7. La colonna **"Suggested Means of Verification" (Mezzi di Verifica Suggeriti**) fornisce una guida all'auditor sulle fonti abituali in cui si trovano le informazioni. È indicativa e gli auditors possono scegliere qualsiasi altra fonte di informazione pertinente.
8. La colonna **"GDPR Article" (Articolo GDPR)** fornisce un'indicazione del principale articolo GDPR relativo alla verifica e al controllo.
9. La colonna **"Evidence & Reference Documents" (Evidenze e Documenti di Riferimento)** deve essere compilata dall'Auditor con una chiara indicazione delle evidenze che sono state considerate per determinare la conformità o la non conformità. Ad eccezione delle verifiche e dei controlli che si ritiene non siano applicabili alla certificazione, questo campo è obbligatorio.

10. La colonna **"Recommendations/Comments" (Raccomandazioni/Commenti)** (se applicabile) consente al Team di Audit di identificare alcune questioni o elementi che il Richiedente deve affrontare.
11. La colonna **"Status" (Stato)** viene utilizzata dall'Auditor per qualificare lo stato della rilevazione sulla verifica e sul controllo.
12. La colonna **NC #** serve a indicare il numero identificativo di una non conformità identificata.

Le verifiche e i controlli sono raggruppati in diversi criteri in linea con la struttura del GDPR.

Struttura verticale della tabella

1. L'**intestazione** fornisce il titolo e la funzione di ogni colonna.
2. Le **Sezioni Superiori** indicano l'inizio di una sezione principale.
3. Le **Sottosezioni** indicano l'inizio di una sottosezione all'interno di una sezione principale.
4. Le **verifiche e i controlli** sono identificati dallo sfondo bianco delle celle nella colonna Requisiti Obbligatori.
5. I **Controlli Preliminari** sono identificati dallo sfondo verde chiaro delle loro celle nella colonna requisiti Obbligatori.

Figura 7 Struttura verticale della tabella

Processo complessivo

Quando si valutano le verifiche e i controlli di una sezione, si applica il seguente processo.

1. Eseguire le verifiche e i controlli richiesti nella categoria superiore
2. Eseguire sistematicamente le verifiche e i controlli
3. Completare i controlli preliminari

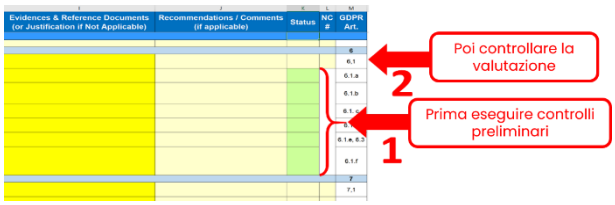


Figura 8 Processo complessivo

Per ogni verifica e controllo

4. Fornire prove chiare nella cella corrispondente
5. Completare con commenti e suggerimenti ("Raccomandazioni/commenti")
6. Determinare lo stato di verifica e controllo
7. Se viene identificata una Non Conformità, includerla nella colonna corrispondente ("NC#") con un chiaro identificatore (numero o lettera)
8. Nella parte inferiore della tabella è presente una dashboard che fornisce un riepilogo dello stato dei risultati delle verifiche e dei controlli

Codice di stato		Significato/Spiegazione	Tot	%
OK		Conformità: Il requisito è stato **verificato** e risulta essere conforme. Non sono state identificate non conformità.	2	22%
OK+		Buone pratiche che vanno oltre la semplice conformità	2	22%
Obs		**Osservazione**	1	11%
			5	56%
NC Min		È stata identificata una **non conformità minore** (non critica).	1	11%
NC Maj		È stata identificata una **non conformità maggiore** (critica).	1	11%
?		**Informazioni mancanti/non so**	0	0%
NA		Il controllo non è applicabile alla certificazione in questione	2	22%

Figura 9 Dashboard indicativa

Opzioni di stato

Il campo Stato nelle celle gialle offre un elenco di diverse opzioni, corrispondenti a diversi stati:

Figura 10 Celle di stato regolari

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

Tabella 1 Opzioni di stato

Alcune celle corrispondono a domande complementari utilizzate per valutare lo stato di una verifica e di un controllo. Il colore di sfondo delle celle corrispondenti allo Stato è verde anziché giallo. Il campo Stato nelle celle verdi offre un elenco semplificato di opzioni, corrispondenti a diversi stati.

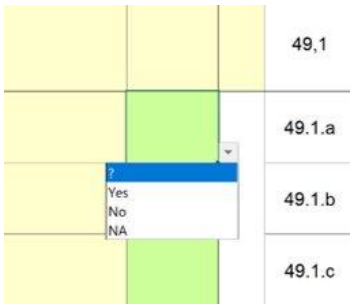


Figura 11 Cella di stato della sotto-domanda

Codice di stato	Significato/Spiegazione
?	Informazioni mancanti/Non so
SÌ	La risposta è Sì
NO	La risposta è No
NA	Il controllo **Non è applicabile** per la certificazione in questione

Tabella 2 Opzioni di stato della sotto-domanda

Preparazione all'esame

Per ottenere un certificato ufficiale e diventare un Implementer Europrivacy, i partecipanti devono superare un esame finale. Questa sezione del Manuale ha lo scopo di preparare e familiarizzare con il tipo di esame.

L'esame consiste in domande a scelta multipla (50 per l'Implementation Course) che devono essere completate entro il tempo stabilito (1 ora e 15 minuti). Ogni domanda prevede 4 possibili risposte. A volte una sola risposta è corretta, mentre altre volte ci sono più risposte corrette. Durante l'esame, vi verrà dato un suggerimento se dovete concentrarvi su una o più risposte corrette. Per ulteriori informazioni, è possibile consultare il Disclaimer dell'esame finale nella pagina del Corso.

L'esame simulato del Manuale è composto da 25 domande e si consiglia di completarlo entro 45 minuti. Come nell'esame, ogni domanda prevede 4 possibili risposte. Rispondendo correttamente a una domanda si ottiene un punto. Alcune domande hanno più risposte corrette e il punteggio è il seguente:

- 1 punto quando si risponde correttamente a una domanda;
- 0 punti per la mancata risposta corretta in una domanda a risposta multipla;
- 0 punti per una risposta errata, indipendentemente dal fatto che siano state segnate le risposte giuste.

Per superare l'esame simulato, è necessario totalizzare 19 punti su 25. Il foglio delle risposte è disponibile alla fine della sezione.

Esempio

	DOMANDA	A	B	C	D
15	Quale dei seguenti NON è un principio chiave delle certificazioni di Europrivacy?	Indipendenza	Presentazione corretta	Favoritismo	Riservatezza
16	Quali dei seguenti sono considerati Documenti Normativi Complementari di Europrivacy?	Linee guida Europrivacy per il Completamento del NOCAR	Regola sulla Comunicazione e sul Marketing di Europrivacy	Linee guida sull'Accountability e sul principio di Apertura	Linee guida Europrivacy sull'uso di Criteri, Verifiche e Controlli
17	Quale dei seguenti documenti fornisce le definizioni per lo Schema di Certificazione Europrivacy?	GDPR e Linee guida EDPB	Dizionario di Oxford	Altre fonti normative pertinenti, come ISO	Wikipedia

In questo scenario, lo studente ha scelto le seguenti risposte (indicate in arancione):

- Domanda 15: C
- Domanda 16: D
- Domanda 17: A, B e C

Il foglio risposte indica le seguenti risposte corrette:

Numero di domanda	Risposta corretta
15	C
16	B D
17	A C

Ciò significa quanto segue:

- La risposta alla Domanda 15 è corretta, lo studente riceve un punto.
- La risposta alla Domanda 16 è parziale, manca la Risposta B. Lo studente non riceve un punto.
- Nella Domanda 17, le risposte A e C sono corrette. Tuttavia, lo studente ha scelto anche la risposta B che non è corretta, il che significa che non riceverà un punto per l'intera domanda.

Spiegazione

Nelle risposte corrette è indicato a quale parte dei moduli si riferisce la domanda. In caso di incertezza, si prega di studiare prima con attenzione questi punti.

Esame Simulato

	DOMANDA	A	B	C	D
1	Quali delle seguenti affermazioni si applicano agli Implementers?	Lavorano per gli Organismi di Certificazione per certificare la conformità alla protezione dei dati	Lavorano per le Società di Consulenza per ridurre i rischi legali e finanziari dello Scheme Owner	Lavorano per gli Organismi di Certificazione per identificare potenziali lacune e Non Conformità residue	Lavorano per le Società di Consulenza per supportare i Richiedenti prima, durante e dopo il processo di certificazione
2	Quale delle seguenti categorie può essere applicata alle verifiche e ai controlli?	E Esenzioni	S Specifico	O Obiettivo	NC Non condizionato
3	Quali delle seguenti affermazioni sono vere?	Qualsiasi utilizzo del marchio Europrivacy e/o ECCP richiede la preventiva autorizzazione scritta ed esplicita o la licenza dell'Autorità di Controllo	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	L'Organismo di Certificazione deve esercitare un adeguato controllo della proprietà dell'uso e del riferimento ai certificati consegnati	Il trattamento dei dati certificato può ricevere un certificato Europrivacy, sotto il controllo e l'approvazione del Richiedente
4	Cosa succede durante la riunione di chiusura tra la Società di Consulenza e il Richiedente?	La Società di Consulenza presenta un'offerta complementare	La Società di Consulenza compila il modulo di richiesta da presentare allo Scheme Owner	La Società di Consulenza presenta i risultati e raccoglie i riscontri	La Società di Consulenza presenta al Richiedente gli auditor dell'Organismo di Certificazione
5	Quali sono i GDPR Core Criteria di Europrivacy?	Consentono una valutazione sistematica della conformità agli obblighi principali contenuti nel GDPR	Si tratta di una mandatory checklist che l'Organismo di Certificazione deve applicare a ogni singolo trattamento dei dati	Si tratta di una complementary checklist che deve essere applicata dall'Autorità di Controllo, se richiesta dallo Studio di Consulenza	Consentono di valutare i requisiti di protezione dei dati specifici per settore e tecnologia
6	Quali delle seguenti affermazioni sono vere?	Gli Organismi di Certificazione non possono replicare le informazioni pubbliche sul loro sito web	Di default, l'Organismo di Certificazione deve rendere pubbliche le informazioni generali sul processo di valutazione della certificazione	Di default, tutte le informazioni fornite dal Richiedente o relative al Richiedente e alla sua certificazione sono informazioni pubbliche	Le Società di Consulenza sono responsabili della gestione e del controllo del sito web ufficiale di Europrivacy

7	In quali formati sono disponibili i criteri Europrivacy?	Presentazione PowerPoint	Sway page	Fogli Excel	Lo Scheme Owner non rende disponibili i criteri a nessuno
8	Quali delle seguenti affermazioni sono vere?	L'Autorità di Controllo prende decisioni sul rinnovo della certificazione in base ai risultati dell'audit di ricertificazione	Durante i 3 anni successivi al ricevimento del certificato, il Richiedente deve rispettare i requisiti dello Schema di Certificazione e informare l'Organismo di Certificazione di qualsiasi cambiamento o preoccupazione in merito alla sua conformità	L'identificazione di qualsiasi Non Conformità Minore porta automaticamente alla sospensione e al potenziale ritiro della certificazione	La certificazione di riferimento si basa su un audit in loco, seguito da audit di sorveglianza ogni 5 anni
9	Quale delle seguenti affermazioni si applica alla "colonna Criteri" nella struttura della tabella dei criteri Europrivacy?	Fornisce un identificatore unico e distinto per ogni singola verifica e controllo	Permette al Team di Audit di identificare alcune questioni o elementi che il Richiedente deve affrontare	Fornisce indicazioni all'auditor sulle fonti abituali in cui si trovano le informazioni	Descrive il requisito formale che deve essere implementato dal Richiedente e valutato dall'auditor
10	Che cosa deve fare l'Organismo di certificazione quando riceve un reclamo o un appello?	Informare il Richiedente di qualsiasi problema importante che possa costituire un rischio per lo Schema di Certificazione o per la sua reputazione	Richiedere all'Autorità di Controllo di intraprendere qualsiasi azione successiva necessaria per risolvere il reclamo o il ricorso	Raccogliere e verificare tutte le informazioni rilevanti	Dare comunicazione formale dell'esito della procedura al reclamante o al ricorrente
11	Durante il Processo di Preparazione a Europrivacy, cosa deve fare l'Implementer dopo aver segnalato le lacune identificate?	Consigliare il cliente su come rimediare alle lacune identificate	Inoltrare il rapporto allo Scheme Owner	Chiedere un secondo parere sulle lacune all'Autorità di Controllo	Nessuna delle risposte è corretta
12	Quali delle seguenti checklist vengono utilizzate nella fase preliminare?	GDPR Core Criteria	Application and Target of Evaluation	Obblighi Nazionali di Protezione dei Dati	Documentation checklist
13	Chi è tenuto a mantenere la riservatezza delle	Il pubblico in generale	Lo Scheme Owner	L'Organismo di Certificazione	Non è un obbligo, ma una raccomandazione

	informazioni sulle certificazioni?				
14	Quali delle seguenti affermazioni sono vere?	Nel valutare le verifiche e i controlli di una Sezione, l'interessato esegue le verifiche e i controlli richiesti	La Technical and Organisational Measures checklist raccoglie i requisiti del GDPR applicabili a tutti i trattamenti dei dati	Le Verifiche e Controlli Contestuali Complementari sono specificati per valutare i requisiti di protezione dei dati specifici del dominio e della tecnologia	Il modello di Elenco delle Non-Conformità deve essere utilizzato dall'Autorità di Controllo per segnalare ed elencare le Non Conformità identificate
15	Chi è il target principale del Welcome Pack?	Interessati	Autorità di Controllo	Organismi di Certificazione	Richiedenti
16	Cosa succede se il regolamento sulla protezione dei dati applicabile cambia durante il periodo di mantenimento?	Le modifiche legislative non hanno impatto sulle certificazioni rilasciate	L'Organismo di Certificazione deve elaborare un Piano d'Azione e convalidarlo con l'Autorità di Controllo	Lo Scheme Owner deve sospendere tutte le certificazioni consegnate e invalidarle	Il Richiedente deve valutare il livello di impatto sulla validità della certificazione
17	Quali delle seguenti affermazioni si applicano al marchio di conformità?	È sotto il controllo e l'approvazione dell'Organismo di Certificazione	Disabilita la tracciabilità	È di proprietà del Richiedente	Il documento segna l'accettazione da parte di un'azienda delle decisioni del Parlamento Europeo
18	Cosa viene specificato nel meccanismo di reclamo e di appello?	Chi è il responsabile del processo per conto dell'EDPB	Chi può presentare reclami o obiezioni	Un processo per garantire che l'Autorità di Controllo intraprenda le azioni correttive appropriate	I costi aggiuntivi che lo Scheme Owner deve pagare all'Organismo di Certificazione
19	Quali delle seguenti affermazioni sono vere?	L'interessato conserva la documentazione dei propri compiti e delle proprie responsabilità in merito alle attività di certificazione	Il Richiedente stabilisce adeguati accordi contrattuali per essere informato dalla Società di Consulenza certificata	Di default, i registri delle certificazioni consegnate vengono conservate per la durata del relativo ciclo di certificazione più 20 anni	L'Autorità di Controllo e lo Scheme Owner possono richiedere l'accesso alle informazioni riservate
20	Quali dei seguenti elementi devono essere garantiti dall'Organismo di Certificazione?	Nella documentazione o in altre forme di pubblicità non si trovano riferimenti errati al marchio di conformità	Il Richiedente ha pubblicato una linea guida sull'uso dei marchi di conformità	Che l'Autorità di Controllo esercita la proprietà sui marchi di conformità	Che il marchio di conformità rappresenti le convinzioni degli interessati in merito ai processi valutati
21	Quali delle seguenti affermazioni sono vere?	I criteri Europrivacy e le verifiche e i controlli complementari sono applicabili e richiesti per tutti i processi di certificazione	Il NOCAR deve valutare la conformità del Target of Evaluation con le normative del paese in cui il Richiedente è domiciliato	L'elenco di riferimento dei criteri, delle verifiche e dei controlli è gestito da Società di Consulenza autorizzate da Europrivacy	La List of Non-Conformities checklist consente di verificare in anticipo se le politiche e le procedure messe in atto dal Richiedente sono sufficientemente complete per

					soddisfare i requisiti Europrivacy
22	Quali dei seguenti elementi sono inclusi nella dichiarazione di conformità?	Il nome e i contatti di tutte le persone certificate	Le condizioni per il rinnovo del certificato	Il nome dell'auditor certificato	Nessuna delle risposte è corretta
23	Quali delle seguenti informazioni sono disponibili sul sito web di Europrivacy?	Il Registro Online dei Certificati di Europrivacy	Copia dei contratti tra gli Organismi di Certificazione e i Richiedenti	Biblioteca online delle certificazioni non andate a buon fine	Dati di contatto dei Richiedenti certificati
24	Quale delle seguenti condizioni NON si applica alle attività di sorveglianza?	Le attività di sorveglianza devono essere pienamente supportate dagli interessati	Di default, un'attività di sorveglianza bimestrale dovrebbe essere la norma	L'Organismo di Certificazione deve mantenere la certificazione sulla base della dimostrazione che il Richiedente continua a rispettare i requisiti dello Schema di Certificazione	L'Organismo di Certificazione seleziona una serie di verifiche e controlli da verificare durante gli Audit di Sorveglianza
25	Quali delle seguenti affermazioni sono vere?	Durante il processo di certificazione, le società di consulenza possono supportare il Richiedente nell'affrontare e risolvere le potenziali Non Conformità	Per ottenere la licenza, le società di consulenza devono firmare un accordo scritto con l'Autorità di Controllo competente prima di fornire qualsiasi servizio legato all'Europrivacy	Le società di consulenza possono preparare un'offerta complementare per fornire un supporto continuo all'elaborazione dei dati certificati e per supportare la preparazione delle rimanenti elaborazioni dei dati da certificare	L'ECCP supporta il Richiedente nell'identificazione delle prime due attività di trattamento dei dati da certificare, per poi specificare formalmente l'obiettivo della valutazione

Risposte

Numero di domanda	Risposta corretta	Spiegazione
1	D	**Modulo 1 - Ruolo degli implementers (diapositiva 3)** Gli implementers qualificati lavorano per società di consulenza e supportano le organizzazioni nel garantire la costante conformità alle normative sulla protezione dei dati. Le società di consulenza non solo preparano i Richiedenti a certificare le loro attività di trattamento dei dati, ma li supportano costantemente durante il processo di certificazione e la fase di mantenimento.
2	A B	**Modulo 3 - Applicabilità di criteri, verifiche e controlli (diapositiva 9)** I criteri, le verifiche e i controlli rientrano in diverse categorie, tra cui Obbligatori, Esenti e Specifici.
3	B C	**Modulo 5 - Uso di marchi di conformità, licenze e certificati** La domanda fa riferimento a diversi punti del Modulo 5. La *Risposta A* non è corretta in quanto è l'ECCP, e non l'Autorità di Controllo, a fornire il consenso preventivo all'utilizzo del marchio Europrivacy. La *Risposta D* non è corretta in quanto i certificati non sono sotto il controllo e l'approvazione del Richiedente ma dell'Organismo di Certificazione.
4	A C	**Modulo 1 - Servizi post-certificazione (diapositiva 7)** Durante la riunione di chiusura, la società di consulenza presenterà i risultati del processo di preparazione, raccoglierà il feedback del Richiedente e, facoltativamente, presenterà un'offerta complementare. La *Risposta B* non è corretta, in quanto il modulo di domanda viene presentato all'Organismo di Certificazione e non allo Scheme Owner. La *Risposta D* non è corretta in quanto la presentazione degli auditor non fa parte della Riunione di Chiusura.
5	A B	**Modulo 4 - Fase di valutazione (diapositiva 5)** I GDPR Core Criteria costituiscono la spina dorsale di tutti i processi di certificazione di Europrivacy e devono essere applicati dagli auditor dell'Organismo di Certificazione a ogni singolo Target of Evaluation, indipendentemente dal suo ambito di applicazione e dalla sua ubicazione. I GDPR Core Criteria consentono di valutare sistematicamente la conformità agli obblighi principali contenuti nel GDPR.
6	C	**Modulo 2 - Gestione delle informazioni e della riservatezza** Questa domanda riassume le informazioni del modulo. Per quanto riguarda la *Risposta A*, gli Organismi di Certificazione possono replicare le informazioni pubbliche sul loro sito web, purché abbiano l'approvazione dell'ECCP. *Risposta C*, di default,

		tutte le informazioni sul Richiedente devono essere trattate in modo confidenziale. *Risposta D*, la manutenzione del sito web di Europrivacy è responsabilità dell'ECCP e non delle società di consulenza.
7	**C**	**Modulo 3 - Criteri di valutazione (diapositiva 3)** I criteri, le verifiche e i controlli di Europrivacy sono resi disponibili attraverso il Welcome Pack e il sito web della community Europrivacy in varie forme, tra cui file Excel, file pdf e modelli Word per facilitare la valutazione della conformità.
8	**B**	**Modulo 5 - Manutenzione, rinnovo e ricorsi** Questa domanda riassume le informazioni contenute nel modulo. *Risposta A*, è l'Organismo di Certificazione, non l'Autorità di Controllo per la protezione dei dati, a prendere la decisione di rinnovo. *Risposta C*, l'identificazione di una Non Conformità non comporta automaticamente la sospensione o il ritiro. *Risposta D*, la frequenza degli audit di sorveglianza è fissata a una volta all'anno e possono essere sia in loco che a distanza.
9	**D**	**Modulo 3 - Struttura della tabella (diapositiva 12)** Risposte errate: la *Risposta A* si riferisce alla colonna Ref ID, la *Risposta B* si riferisce alla colonna Raccomandazioni, mentre la *Risposta C* si riferisce alla colonna "Implementing Guidance" (Guida all'Attuazione).
10	**C D**	**Modulo 6 - Policy dei ricorsi e dei reclami (diapositive 8-11)** Risposte errate: *Risposta A* è lo Scheme Owner che deve essere informato. *Risposta B* l'Autorità di Controllo non è responsabile della risoluzione dei reclami o dei ricorsi.
11	**A**	**Modulo 1 - Processo di preparazione all'Europrivacy (diapositive 5)** Gli Implementers possono supportare i Richiedenti nel rimediare alle lacune identificate. Non devono inoltrare il documento allo Scheme Owner o chiedere un secondo parere.
12	**B D**	**Modulo 4 - Fase preliminare (diapositiva 4)** I GDPR Core Criteria (*Risposta A*) e gli Obblighi Nazionali di Protezione dei Dati (*Risposta C*) sono utilizzati come parte della fase di Valutazione.
13	**B C**	**Modulo 2 - Gestione delle informazioni e della riservatezza** La *Risposta A* non è corretta, in quanto il pubblico non è una parte interessata vincolata alle regole di riservatezza in relazione al processo di certificazione. Allo stesso modo, la *Risposta D* non è corretta in quanto la riservatezza è un obbligo e non una raccomandazione.
14	**C**	**Modulo 3 e Modulo 4** Questa domanda riassume le informazioni dei due moduli sui criteri. La *Risposta A* non è corretta, in quanto è l'auditor (e

		l'implementer) a eseguire le verifiche e i controlli, non l'interessato. La *Risposta B* non è corretta in quanto sono i GDPR Core criteria e non la TOM checklist a raccogliere i requisiti GDPR. La *Risposta D* non è corretta in quanto è l'auditor (e l'implementer) che può utilizzare l'Elenco delle Non Conformità per segnalare le Non Conformità.
15	**D**	**Modulo 1 - Ruolo degli implementers (diapositiva 3)** Le società di consulenza possono sfruttare l'offerta dell'Europrivacy Welcome Pack per fornire un supporto completo ai loro Richiedenti.
16	**D**	**Modulo 6 - Modifiche che riguardano la certificazione (diapositiva 6)** Le modifiche alla normativa applicabile in materia di protezione dei dati, quali revisioni legislative, decisioni di tribunali nazionali o sovranazionali, decisioni dell'EDPB o della Commissione Europea, sono monitorate e affrontate dall'Organismo di Certificazione. Se queste modifiche hanno un impatto sulle certificazioni rilasciate, l'Organismo di Certificazione: (1) Valuta il livello di impatto sulla validità della certificazione; (2) Elabora un Piano d'Azione; (3) Contatta l'Autorità di Controllo competente e richiede la convalida del Piano d'Azione proposto; (4) Attua il Piano d'Azione dopo che è stato approvato dall'Autorità di Controllo.
17	**A**	**Modulo 5 - Marchio di conformità (diapositiva 9)** Le attività di trattamento dei dati certificate possono essere contrassegnate con il marchio di conformità Europrivacy, sotto il controllo e l'approvazione dell'Organismo di Certificazione.
18	**B**	**Modulo 6 - Policy dei ricorsi e dei reclami (diapositiva 9)** La *Risposta A* non è corretta in quanto è per conto dell'Organismo di Certificazione, non dell'EDPB. La *Risposta C* non è corretta in quanto non è l'Autorità di Controllo, ma l'Organismo di Certificazione o lo Scheme Owner. La *Risposta D* non è corretta in quanto non ci sono costi aggiuntivi da pagare allo Scheme Owner.
19	**D**	**Modulo 2 - Gestione delle informazioni e della riservatezza** Questa domanda riassume le informazioni del modulo. La *Risposta A* non è corretta in quanto non è compito dell'interessato, ma dell'Organismo di Certificazione, conservare i registri delle attività di certificazione. La *Risposta B* non è corretta in quanto è l'Organismo di Certificazione a stabilire gli accordi contrattuali con i Richiedenti certificati. La *Risposta C* non è corretta in quanto i registri vengono conservati per 10 anni.
20	**A**	**Modulo 5 - Controllo dell'Organismo di Certificazione (diapositiva 13)**

		La *Risposta B* non è corretta in quanto è lo Scheme Owner a pubblicare le linee guida sull'uso dei marchi di conformità. Allo stesso modo, la *Risposta C* non è corretta in quanto è l'Organismo di Certificazione che esercita il controllo di proprietà sui marchi di conformità. La *Risposta D* non è corretta in quanto il marchio di conformità è un sigillo o un marchio che può essere utilizzato per indicare il completamento della procedura di certificazione.
21	**A B**	**Modulo 3 e Modulo 4** Questa domanda riassume le informazioni dei due moduli sui criteri. La *Risposta C* non è corretta, in quanto è lo Scheme Owner e non una Società di Consulenza a mantenere l'elenco di riferimento. La *Risposta D* non è corretta, in quanto la List of Non-Conformities checklist serve a segnalare ed elencare le non conformità identificate che il Richiedente deve affrontare per ottenere la certificazione.
22	**D**	**Modulo 5 - Dichiarazioni di conformità (diapositiva 10)** Nessuna delle risposte è corretta in quanto la dichiarazione di conformità include: il riferimento a Europrivacy e, ove autorizzato, il logo Europrivacy; il nome del Richiedente certificato; ove applicabile, il nome dei contitolari; una chiara indicazione del Target of Evaluation e del suo ambito geografico; ove applicabile, una chiara indicazione di norme o requisiti complementari che sono stati aggiunti; le date di emissione e di validità del certificato; l'identificativo univoco del certificato consegnato; la dicitura "Maggiori informazioni su" seguita dal nome del dominio del sito web dello Schema di Certificazione e del Registro Online dei Certificati; il nome e l'indirizzo dell'Organismo di Certificazione che ha rilasciato il certificato.
23	**A**	**Modulo 2 - Gestione delle informazioni e della riservatezza** Il Registro Online dei Certificati di Europrivacy è disponibile sul sito web di Europrivacy.
24	**A B**	**Modulo 6 - Audit di monitoraggio e sorveglianza (diapositiva 5)** La *Risposta A* non si applica agli audit di sorveglianza, poiché gli interessati non hanno bisogno di supportare tali attività. La *Risposta B* non si applica agli audit di sorveglianza, poiché le attività hanno cadenza annuale e non bimestrale.
25	**A C**	**Modulo 1 - Ruolo degli Implementers** Questa domanda riassume le informazioni del modulo. La *Risposta B* non è corretta, in quanto le Società di Consulenza devono firmare un accordo con l'ECCP e non con l'Autorità di Controllo per fornire servizi relativi all'Europrivacy. La *Risposta D* non è corretta in quanto è la Società di Consulenza, e non l'ECCP,

		a supportare il Richiedente nella scelta delle prime due attività di trattamento dei dati.