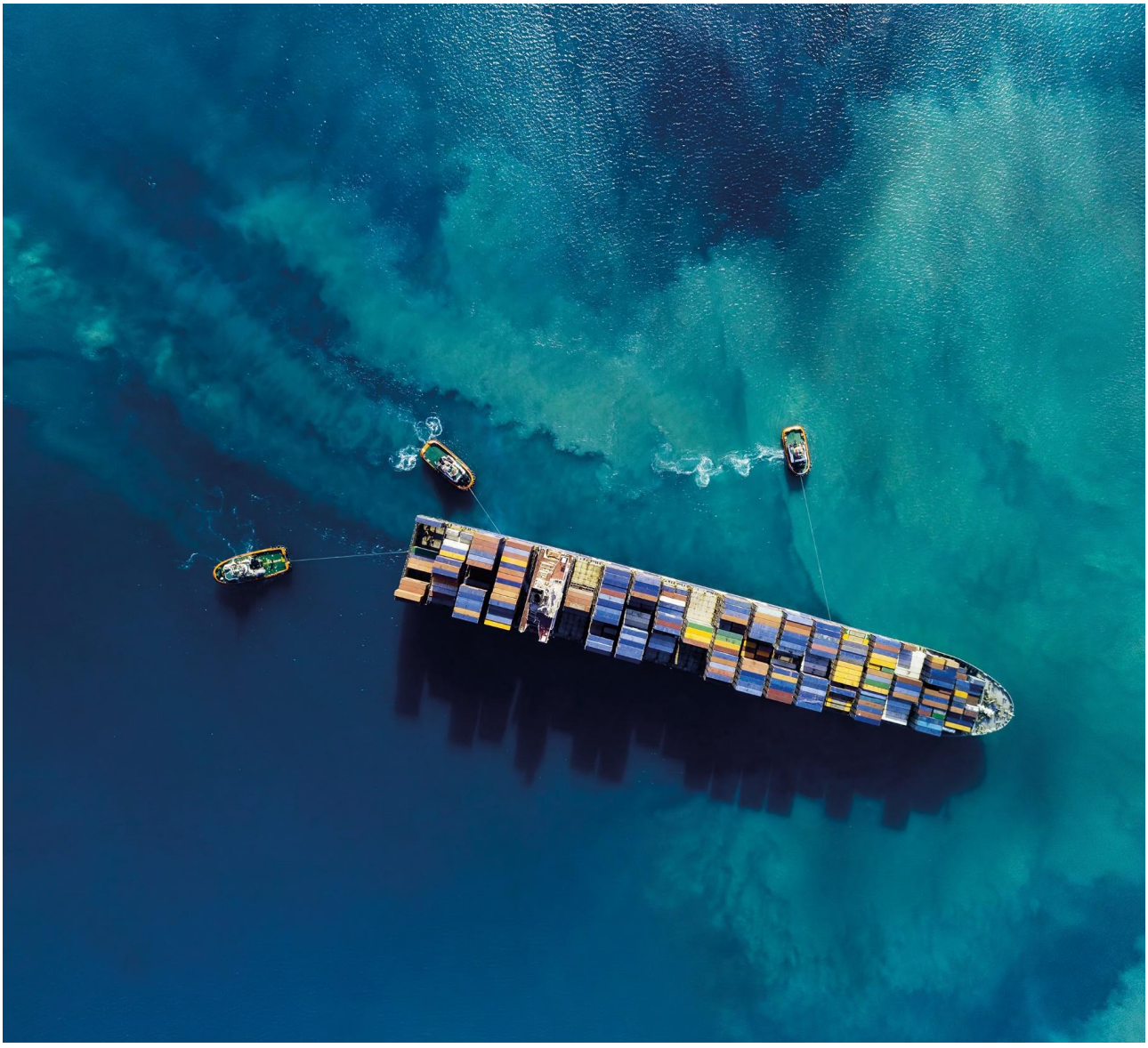
CER-REP-01-ITA_EUROPRIVACY

REGOLAMENTO PER LA CERTIFICAZIONE EUROPRIVACY

I&F

Rev.00 of 10/04/2026



INFORMAZIONI SUL DOCUMENTO

CONTROLLO DEL DOCUMENTO

Rev.	Editing	Verification	Approval	Date of issue
00	SL CER ICT	LTM/G. Focetola	SLM/ A. Filippi	10/04/2026

RIFERIMENTI NORMATIVI GENERALI:

- *ISO/IEC 17065: Conformity Assessment – Requirements for Bodies Certifying Products, Processes, and Services.*
- *ISO/IEC 17021: Requirements for Audit and Certification of Management Systems.*
- *ISO/IEC 27001: Information Security Management Systems – Requirements.*
- *ISO/IEC 27701: Privacy Information Management – Requirements and Guidelines for Data Protection.*
- *GDPR (EU Regulation 2016/679): General Data Protection Regulation.*

RIFERIMENTI NORMATIVI SPECIFICI:

- *Europrivacy Certification Scheme v77: Comprehensive framework for assessing conformity with GDPR and related data protection regulations.*
- *EU GDPR Regulation (EU) 2016/679: General Data Protection Regulation, governing data protection and privacy in the European Union.*
- *ISO/IEC 29100: Privacy Framework – Providing a framework for privacy policies and controls.*
- *ePrivacy Directive (Directive 2002/58/EC): Directive on Privacy and Electronic Communications.*
- *Data Protection Impact Assessment Guidelines (WP248 Rev.01): Guidelines for conducting DPIAs under GDPR.*
- *National Data Protection Authority Requirements: Specific requirements or guidelines issued by relevant supervisory authorities.*
- *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)_Rev.3_04/06/2019*
- *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation_Rev.3_04/06/2019*
- *Guidelines 07/2022 on certification as a tool for transfers_Version 2.0 Adopted on 14 February 2023*
- *Italian Data Protection Autority resolution 148 dated 29/07/2020 "Requisiti aggiuntivi di accreditamento degli organismi di certificazione - 29 luglio 2020"*

Per i riferimenti normativi senza data, si applica l'ultima edizione del documento cui si fa riferimento, compresi gli aggiornamenti.

INFORMAZIONI SULLE REVISIONI PRECEDENTI

Rev.	Date	Comments

DOCUMENTI DI SUPPORTO E ASSOCIATI

Europrivacy Certification Scheme v77	Type
Europrivacy Certification Scheme v77	Framework Document
Europrivacy Guidelines for Applicants	Guidelines
Europrivacy Criteria, Checks, and Controls v21	Checklist/Criteria

GDPR Regulation (EU) 2016/679	Regulation
ISO/IEC 27701: Privacy Information Management	Standard
Data Protection Impact Assessment (DPIA) Guidelines	Methodology
Europrivacy Guidelines for Certification Bodies v5.2	Operational Guidelines
Handbook for the Europrivacy Implementation Course	Training Material

Table of Contents

1. SVILUPPO E APPROVAZIONE DI UN NUOVO SCHEMA DI CERTIFICAZIONE SECONDO IL FRAMEWORK EUROPRIVACY

1.1 SCOPO E AMBITO DI APPLICAZIONE

Questo documento specifica le condizioni particolari per l'implementazione e la certificazione dello schema Europrivacy, progettato per valutare e certificare la conformità delle attività di trattamento dei dati al Regolamento generale sulla protezione dei dati (GDPR) e alle normative nazionali e settoriali correlate.

1.2 L'ambito di applicazione include:

- Organizzazioni che trattano dati personali all'interno dell'Unione Europea e in giurisdizioni che richiedono la conformità al GDPR.
- Attività di trattamento dei dati ad alto rischio, incluse categorie speciali di dati personali e informazioni sensibili.
- Applicazioni tecnologiche avanzate come IoT, intelligenza artificiale, blockchain e servizi cloud.
- Adattamenti specifici per settore per industrie come sanità, servizi finanziari e amministrazione pubblica.

Lo schema Europrivacy mira a promuovere un approccio sistematico e verificabile alla protezione dei dati personali, garantendo fiducia e trasparenza per tutti gli stakeholder coinvolti.

2. INFORMAZIONI GENERALI

2.1 IMPEGNI DI BUREAU VERITAS

Nessuna aggiunta.

2.2 IMPEGNI DELL'ORGANIZZAZIONE

Per le finalità della certificazione Europrivacy, l'organizzazione si impegna a:

- **Garantire** che tutte le attività di trattamento dei dati, i sistemi, i prodotti o i servizi nell'ambito della certificazione siano conformi al GDPR e agli standard correlati.
- **Fornire** documentazione completa e accurata delle attività di trattamento dei dati, incluse prove dei controlli tecnici, organizzativi e operativi.
- **Affrontare** eventuali non conformità identificate attraverso azioni correttive e preventive entro i tempi specificati.
- **Garantire** che tutti i dipartimenti, il personale e gli stakeholder rilevanti siano informati e aderiscono ai requisiti di certificazione.
- **Consentire** agli organismi di certificazione l'accesso senza restrizioni ai siti, alla documentazione e al personale necessari per condurre valutazioni e audit.
- **Mantenere** la conformità continua ai requisiti di certificazione, inclusa l'implementazione di aggiornamenti in risposta a cambiamenti normativi o tecnologici.
- **Proteggere** l'integrità e la riservatezza dei dati trattati secondo lo schema di certificazione.

Questi impegni garantiscono l'efficacia e la credibilità del processo di certificazione, promuovendo fiducia e responsabilità nelle pratiche di protezione dei dati.

3. RIFERIMENTI

I seguenti riferimenti sono parte integrante dello schema di certificazione Europrivacy:

- **Regolamento UE GDPR (UE) 2016/679**: Regolamento generale sulla protezione dei dati, che disciplina la protezione dei dati e la privacy nell'UE.
- **ISO/IEC 17065**: Valutazione della conformità – Requisiti per gli organismi che certificano prodotti, processi e servizi.
- **ISO/IEC 27701**: Gestione della privacy delle informazioni – Requisiti e linee guida per la protezione dei dati.
- **Direttiva ePrivacy (Direttiva 2002/58/CE)**: Direttiva sulla privacy e le comunicazioni elettroniche.
- **Linee guida sulla valutazione dell'impatto sulla protezione dei dati (DPIA)**: Linee guida per condurre DPIA secondo il GDPR.
- **Requisiti dell'Autorità nazionale di protezione dei dati**: Linee guida specifiche emesse dagli Stati membri dell'UE.

Per i riferimenti senza data, si applica l'ultima edizione del documento cui si fa riferimento, compresi gli aggiornamenti.

4. TERMINI E DEFINIZIONI

I seguenti termini e definizioni si applicano allo schema di certificazione Europrivacy:

- **Organizzazione**: Una persona giuridica responsabile del trattamento dei dati personali e soggetta a certificazione secondo il framework Europrivacy.
- **Dati personali**: Qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) come definito dall'articolo 4(1) del GDPR.
- **Titolare del trattamento**: L'ente che determina le finalità e i mezzi del trattamento dei dati personali.
- **Responsabile del trattamento**: L'ente che tratta i dati personali per conto del titolare del trattamento.
- **Target of Evaluation (ToE)**: I processi, i sistemi o i servizi specifici sottoposti a valutazione per la conformità al GDPR e ai criteri Europrivacy.
- **Non conformità**: Una situazione o un risultato che indica che le pratiche di un'organizzazione non soddisfano pienamente i requisiti del GDPR o dei criteri Europrivacy.
    - **Non conformità maggiore**: Un problema critico che pone un rischio significativo per la protezione dei dati personali o la conformità normativa.
    - **Non conformità minore**: Un problema che non pone un rischio immediato ma richiede un'azione correttiva.
- **Organismo di certificazione (OC)**: Un'entità accreditata autorizzata a valutare e certificare la conformità secondo lo schema Europrivacy.
- **Valutazione dell'impatto sulla protezione dei dati (DPIA)**: Un processo per valutare i rischi per la protezione dei dati personali e implementare controlli mitiganti, come definito nell'articolo 35 del GDPR.
- **Audit di certificazione**: L'esame sistematico delle pratiche di un'organizzazione per determinare la conformità ai criteri Europrivacy.
- **Audit di sorveglianza**: Audit periodici condotti per garantire il mantenimento della conformità ai requisiti di certificazione.
- **Responsabile della protezione dei dati (DPO)**: Il soggetto incaricato di supervisionare le strategie di protezione dei dati e garantire la conformità al GDPR e alle normative correlate.

Per ulteriori definizioni, fare riferimento all'articolo 4 del GDPR e alla documentazione normativa correlata.

5. PROCESSO DI CERTIFICAZIONE

5.1 Richiesta di certificazione

L'organizzazione che richiede la certificazione deve:

- **Identificare chiaramente** l'ambito della certificazione, incluse le specifiche attività di trattamento dei dati, i sistemi e i servizi da valutare.
- **Fornire documentazione dettagliata** dei processi e dei controlli relativi alla protezione dei dati, inclusi:
    - Valutazioni dell'impatto sulla protezione dei dati (DPIA).
    - Misure tecniche e organizzative (ad es. crittografia, controllo dell'accesso).
    - Registri delle attività di trattamento (Articolo 30, GDPR).
- **Garantire** che la richiesta di certificazione sia accurata, non fuorviante e non escluda attività, processi o servizi che potrebbero influire sulla conformità.

Le certificazioni multi-sito richiedono un elenco completo dei siti, con dettagli su loro ubicazioni e funzioni. I siti temporanei o i progetti (ad es. trattamento dati remoto o operazioni specifiche per eventi) devono essere esplicitamente inclusi e sottoposti a audit appropriati.

5.2 Offerta di certificazione

L'organismo di certificazione valuta l'applicazione e fornisce un'offerta dettagliata, inclusa:

- L'ambito della certificazione e i criteri Europrivacy applicabili.
- Una suddivisione del processo di certificazione, delle tempistiche e dei costi associati.
- Requisiti per gli audit iniziali e di sorveglianza.

L'organizzazione deve accettare formalmente l'offerta prima di avviare il processo di certificazione.

5.3 Audit di certificazione

L'audit di certificazione prevede due fasi principali:

FASE 1 (Audit iniziale)

Obiettivo: Valutare la disponibilità dell'organizzazione per la certificazione, concentrandosi su:

- Completezza della documentazione (politiche, DPIA, registri delle attività di trattamento).
- Identificazione iniziale dei gap di conformità.

- Valutazione della comprensione organizzativa del GDPR e dei criteri Europrivacy.
- Condotto in sito o da remoto, a seconda dell'ambito e della ubicazione delle attività.

FASE 2 (Audit principale)

Obiettivo: Verificare l'implementazione e l'efficacia dei controlli, inclusi:

- Conformità ai requisiti del GDPR.
- Efficacia delle misure tecniche e organizzative.
- Coerenza delle pratiche di protezione dei dati nelle organizzazioni multi-sito.
- **Almeno il 50% della durata dell'audit** si concentra sull'implementazione operativa dei controlli e delle misure.

5.4 Conduzione dell'audit

Il processo di audit include:

- Revisione della documentazione, colloqui e ispezioni in sito.
- Campionamento delle attività di trattamento dei dati per convalidare l'applicazione coerente dei controlli.
- Comunicazione trasparente dei risultati, incluse le non conformità e le aree di miglioramento.

Per le certificazioni multi-sito, gli audit sono condotti sia presso la sede centrale che presso i siti campionati, seguendo metodologie di campionamento statistiche o basate sul rischio.

Le certificazioni multi-aziendali saranno gestite in conformità alle regole multi-sito e i certificati saranno gestiti secondo i metodi stabiliti da Europrivacy (un certificato per filiale).

5.5 Approvazione della certificazione

L'organismo di certificazione esamina i risultati dell'audit, incluse le azioni correttive per le non conformità identificate, prima di rilasciare la certificazione. L'approvazione è concessa solo quando:

- Tutte le non conformità maggiori sono risolte.
- Le non conformità minori sono affrontate con un piano d'azione chiaro.
- L'organizzazione dimostra la conformità continua ai criteri Europrivacy.
- **Il certificato sarà rilasciato da Bureau Veritas ma sarà valido solo quando caricato nel portale da Europrivacy.**

5.6 Manutenzione della certificazione

Per mantenere la certificazione, l'organizzazione deve:

- Sottoporsi a audit di sorveglianza periodici per verificare la conformità continua.
- Aggiornare e documentare le attività di trattamento nuove o modificate.
- Affrontare le non conformità identificate durante la sorveglianza entro il termine specificato.
- Notificare all'organismo di certificazione qualsiasi cambiamento significativo nelle operazioni o nelle attività di trattamento dei dati.

5.7 Sospensione o ritiro della certificazione

L'organismo di certificazione può sospendere o ritirare la certificazione se:

- Sono identificate non conformità significative e non risolte entro il termine specificato.
- L'organizzazione non aderisce ai criteri Europrivacy o ai termini della certificazione.
- I cambiamenti significativi nelle attività di trattamento dei dati non sono segnalati o affrontati.
- **Bureau Veritas comunicherà a Europrivacy la sospensione o la revoca del certificato al fine di evidenziare la sospensione e la revoca effettiva dello stesso nel portale.**

5.8 APPROVAZIONE DELLA CERTIFICAZIONE

L'approvazione della certificazione è concessa dall'organismo di certificazione dopo una revisione approfondita dei risultati dell'audit e della risoluzione di eventuali non conformità identificate. Il processo di approvazione comporta:

Revisione del rapporto di audit

- Valutazione dei risultati degli audit di Fase 1 e Fase 2.
- Verifica delle azioni correttive implementate per eventuali non conformità identificate.

Comitato decisionale

Il comitato decisionale dell'organismo di certificazione esamina la documentazione dell'audit, incluso:

- Prove di conformità ai criteri Europrivacy e ai requisiti GDPR.
- Efficacia delle misure tecniche e organizzative implementate dall'organizzazione.

- Coerenza delle pratiche in tutti i siti inclusi, se è richiesta una certificazione multi-sito.

Criteri di approvazione

- Tutte le non conformità maggiori devono essere risolte prima che la certificazione sia concessa.
- Le non conformità minori devono avere piani d'azione chiari con scadenze per la risoluzione.
- L'organizzazione deve dimostrare la conformità continua ai requisiti di certificazione.

Rilascio della certificazione

- Previa approvazione, all'organizzazione viene rilasciato un certificato Europrivacy ufficiale, valido per il periodo di certificazione specificato.
- La certificazione include l'ambito definito delle attività di trattamento certificate e i criteri Europrivacy applicabili.
- I dettagli della certificazione sono pubblicati nel registro ufficiale di Europrivacy per garantire trasparenza e verifica pubblica.
- **Il certificato sarà rilasciato da Bureau Veritas ma sarà valido solo quando caricato nel portale da Europrivacy.**
- **Bureau Veritas, prima di rilasciare il certificato, chiederà a Europrivacy se il cliente ha rispettato le procedure amministrative verso Europrivacy (pagamento delle tasse).**

La certificazione è valida per il ciclo determinato (tipicamente tre anni) soggetta ad audit di sorveglianza regolari e conformità continua ai requisiti Europrivacy.

6. MANUTENZIONE

La manutenzione della certificazione Europrivacy garantisce che le organizzazioni rimangono conformi ai requisiti di certificazione durante il periodo di validità. La manutenzione comporta le seguenti attività chiave:

6.1 Audit di sorveglianza

- **Frequenza**: Gli audit di sorveglianza sono condotti annualmente, o come specificato nell'accordo di certificazione.
- **Obiettivo**: Verificare che l'organizzazione continui a soddisfare i criteri Europrivacy, inclusi:
  - Conformità al GDPR e a qualsiasi normativa nazionale o settoriale applicabile.
  - Efficacia delle misure tecniche e organizzative in vigore.
  - Risoluzione delle non conformità identificate durante i precedenti audit.
- **Ambito**: Gli audit di sorveglianza possono concentrarsi su attività di trattamento dei dati selezionate o su aree specifiche dell'ambito di certificazione.

6.2 Notifica dei cambiamenti

L'organizzazione deve notificare l'organismo di certificazione di qualsiasi cambiamento significativo che possa influire sulla conformità, come:

- Cambiamenti nell'ambito delle attività di trattamento dei dati.
- Introduzione di nuove tecnologie, come implementazioni IoT o AI.
- Ristrutturazione organizzativa o cambiamenti nelle ubicazioni di trattamento dei dati.
- Aggiornamenti ai requisiti legali o normativi applicabili all'organizzazione.

6.3 Azioni correttive

- Le non conformità identificate durante gli audit di sorveglianza devono essere affrontate tempestivamente.
- L'organizzazione deve presentare prove delle azioni correttive all'organismo di certificazione entro il termine concordato.

6.4 Ricertificazione

- Al termine del ciclo di certificazione (tipicamente tre anni), l'organizzazione deve sottoporsi a un audit di ricertificazione completo.
- La ricertificazione comporta una revisione completa della conformità a tutti i criteri Europrivacy applicabili e la risoluzione di eventuali problemi in sospeso.

6.5 Sospensione o ritiro della certificazione

- La certificazione può essere sospesa o ritirata se l'organizzazione:
  - Non affronta le non conformità identificate entro il termine specificato.
  - Non rispetta i requisiti dell'accordo di certificazione.
  - Non mantiene l'integrità delle sue misure di protezione dei dati o dell'ambito.

Il processo di manutenzione garantisce che le organizzazioni rispettino continuamente gli standard elevati di protezione dei dati e rimangano allineate al framework Europrivacy durante il periodo di certificazione.

7. MODIFICHE ALL'AMBITO E AGLI STANDARD

I cambiamenti all'ambito di certificazione o agli standard applicabili devono essere gestiti sistematicamente per garantire la conformità continua ai requisiti Europrivacy. Ciò comporta quanto segue:

7.1 Modifiche all'ambito di certificazione

- **Requisito di notifica**:
  - Le organizzazioni devono prontamente informare l'organismo di certificazione di qualsiasi cambiamento nell'ambito delle loro attività di trattamento dei dati, inclusi:
    - Introduzione di nuove tecnologie di trattamento dei dati (ad es. IoT, AI).
    - Espansione dell'ambito per includere siti o attività di trattamento aggiuntivi.
    - Riduzione dell'ambito dovuta all'interruzione di attività o cambiamenti operativi.
- **Valutazione dei cambiamenti**:
  - L'organismo di certificazione valuterà l'impatto dei cambiamenti sulla certificazione esistente.
  - Possono essere richiesti audit aggiuntivi per convalidare la conformità delle attività nuove o modificate ai criteri Europrivacy.
- **Certificato aggiornato**:
  - Se i cambiamenti sono approvati, verrà emesso un certificato aggiornato che riflette l'ambito modificato.

7.2 Modifiche agli standard applicabili

- **Monitoraggio degli standard**:
  - L'organismo di certificazione monitora gli aggiornamenti degli standard rilevanti, inclusi GDPR, leggi nazionali sulla protezione dei dati e criteri Europrivacy.
- **Periodi di transizione**:
  - Alle organizzazioni viene concesso un periodo di transizione per conformarsi agli standard nuovi o aggiornati. La durata del periodo di transizione dipende dalla complessità e dalla significatività dei cambiamenti.
- **Comunicazione**:
  - L'organismo di certificazione comunica gli aggiornamenti agli standard e fornisce indicazioni sull'implementazione dei cambiamenti richiesti.
- **Audit per la conformità ai nuovi standard**:
  - Durante il periodo di transizione, possono essere condotti audit di sorveglianza o speciali per verificare la conformità ai requisiti aggiornati.

7.3 Miglioramento continuo

- Le organizzazioni sono incoraggiate a integrare i cambiamenti in modo proattivo per migliorare le loro pratiche di protezione dei dati e allinearsi agli ambienti normativi e tecnologici in evoluzione.

Gestendo efficacemente i cambiamenti all'ambito e agli standard, lo schema di certificazione Europrivacy garantisce che le organizzazioni certificate mantengano la conformità e rispettino gli standard elevati di protezione dei dati.

8. RECLAMI

Lo schema di certificazione Europrivacy include un processo strutturato per la gestione dei reclami al fine di garantire trasparenza, responsabilità e risoluzione dei problemi relativi alle attività di certificazione.

8.1 Presentazione del reclamo

I reclami possono essere presentati da:

- Organizzazioni certificate.
- Stakeholder, inclusi clienti, dipendenti o terze parti.
- Autorità di regolamentazione o altre parti interessate.

I reclami devono essere presentati per iscritto e includere:

- Una chiara descrizione del problema o della preoccupazione.
- Documentazione o prove di supporto, se disponibili.
- Informazioni di contatto del riclamante per il follow-up.

8.2 Procedura di gestione del reclamo

Riconoscimento:

- I reclami sono riconosciuti dall'organismo di certificazione entro un termine definito (ad es. 5 giorni lavorativi).

Indagine:

- Un team neutrale e qualificato indaga il reclamo per determinarne la validità e l'impatto.
- Se il reclamo riguarda un'organizzazione certificata, l'organizzazione sarà informata e avrà l'opportunità di rispondere.

Risoluzione:

- Le azioni correttive sono identificate e implementate se il reclamo è convalidato.
- La risoluzione è comunicata al riclamante in modo tempestivo.

8.3 Riservatezza

- L'identità del riclamante è protetta a meno che la divulgazione non sia necessaria per risolvere il problema o richiesta dalla legge.

8.4 Appelli

- Se il riclamante non è soddisfatto della risoluzione, può escalare il problema attraverso un processo di appello.
- Il processo di appello è supervisionato da un panel indipendente per garantire l'imparzialità.

8.5 Conservazione dei registri

- Tutti i reclami e le loro risoluzioni sono documentati e conservati dall'organismo di certificazione per la revisione e il miglioramento continuo.

Affrontando efficacemente i reclami, lo schema di certificazione Europrivacy promuove fiducia e confidenza tra le organizzazioni certificate e gli stakeholder.

9. AUDIT AGGIUNTIVI

Possono essere richiesti audit aggiuntivi in circostanze specifiche per garantire la conformità continua allo schema di certificazione Europrivacy. Questi audit sono condotti al di fuori della programmazione regolare di certificazione o sorveglianza.

9.1 Fattori scatenanti per audit aggiuntivi

Cambiamenti significativi:

- L'organizzazione subisce cambiamenti importanti nelle sue attività di trattamento dei dati, come:
  - Introduzione di nuove tecnologie (ad es. IoT, AI).
  - Espansione a nuovi mercati o giurisdizioni con requisiti normativi diversi.
  - Cambiamenti sostanziali all'ambito di certificazione.

Non conformità:

- Non conformità maggiori irrisolte identificate durante i regolari audit.
- Mancato rispetto delle azioni correttive entro il termine concordato.

Reclami:

- Reclami validi ricevuti da stakeholder o autorità di regolamentazione riguardanti potenziale non conformità ai criteri Europrivacy.

Richieste normative:

- Richieste da parte delle autorità nazionali di protezione dei dati per un'indagine o una rivalutazione della conformità dell'organizzazione.

9.2 Processo di audit

Pianificazione:

- Gli audit aggiuntivi sono pianificati in base al problema specifico o al fattore scatenante, con obiettivi chiari definiti prima dell'audit.

Ambito:

- L'ambito dell'audit aggiuntivo è limitato alle aree colpite dal problema identificato, ma può essere esteso se vengono rilevate non conformità sistemiche.

Esecuzione:

- Condotto utilizzando la stessa metodologia degli audit regolari, inclusa la revisione della documentazione, i colloqui e le ispezioni in sito secondo necessità.

Relazione:

- Una relazione dettagliata è emessa delineando i risultati, le azioni correttive e i tempi per la risoluzione.

9.3 Impatto sulla certificazione

- Lo stato di certificazione può rimanere invariato durante l'audit aggiuntivo a meno che non vengano riscontrate non conformità significative.

- Se le non conformità non vengono risolte, l'organismo di certificazione può sospendere o ritirare la certificazione.

9.4 Costi

- I costi degli audit aggiuntivi sono a carico dell'organizzazione certificata, come specificato nell'accordo di certificazione.

Conducendo audit aggiuntivi quando necessario, lo schema di certificazione Europrivacy garantisce l'integrità e l'affidabilità del processo di certificazione affrontando specifiche sfide di conformità.

10. SOSPENSIONE DEL CERTIFICATO

Lo schema di certificazione Europrivacy consente la sospensione della certificazione nei casi in cui l'organizzazione certificata non riesce a mantenere la conformità ai requisiti di certificazione. Quanto segue delinea le condizioni, il processo e la risoluzione per la sospensione del certificato.

10.1 Condizioni per la sospensione

L'organismo di certificazione può sospendere il certificato nelle seguenti circostanze:

Non conformità:

- Non conformità maggiori sono identificate e non affrontate entro il termine specificato per l'azione correttiva.

Mancato notificare i cambiamenti:

- L'organizzazione non informa l'organismo di certificazione di cambiamenti significativi nelle sue attività di trattamento dei dati, nell'ambito o nella struttura organizzativa.

Violazione dell'accordo di certificazione:

- Non conformità ai termini delineati nell'accordo di certificazione, come il diniego di accesso per gli audit o il trattenimento di informazioni necessarie.

Violazioni legali o normative:

- L'organizzazione è riscontrata in violazione del GDPR o di altre normative pertinenti sulla protezione dei dati.

Reclami o indagini:

- Reclami sostanziati o indagini normative indicano significativa non conformità.

10.2 10.2. Notifica della sospensione

L'organismo di certificazione emette una notifica formale all'organizzazione, specificando:

- I motivi della sospensione.
- Le azioni correttive richieste.
- La scadenza per risolvere i problemi (tipicamente entro 90 giorni).

10.3 Impatto della sospensione

Durante la sospensione, l'organizzazione:

- È vietato utilizzare il marchio di certificazione Europrivacy o rivendicare lo stato di certificazione in qualsiasi comunicazione o documentazione.
- Rimane elencata come "sospesa" nel registro pubblico di certificazione di Europrivacy.

10.4 Revoca della sospensione

La sospensione è revocata una volta che l'organizzazione dimostra che:

- Tutte le non conformità sono state risolte in modo soddisfacente per l'organismo di certificazione.
- Le azioni correttive sono state efficacemente implementate.
- Può essere richiesto un audit di follow-up per verificare la conformità.

10.5 Escalation al ritiro

- Se l'organizzazione non riesce a risolvere i problemi entro il termine specificato, l'organismo di certificazione può procedere al ritiro del certificato, seguendo il processo delineato nella Sezione 11.

Il processo di sospensione garantisce che le organizzazioni certificate mantengano standard elevati di conformità e integrità, preservando la credibilità dello schema di certificazione Europrivacy.

11. RITIRO DELLA CERTIFICAZIONE

Lo schema di certificazione Europrivacy include disposizioni per il ritiro della certificazione quando un'organizzazione non riesce a soddisfare gli standard di conformità necessari o viola i termini dell'accordo di certificazione. Il processo di ritiro garantisce l'integrità e la credibilità dello schema di certificazione.

11.1 Condizioni per il ritiro

La certificazione può essere ritirata nelle seguenti circostanze:

Mancato risolvere le non conformità:

- Non conformità maggiori rimangono irrisolte oltre il termine specificato per l'azione correttiva, anche dopo la sospensione.

Mancata conformità continua:
- Ripetuto mancato rispetto dei criteri Europrivacy o dei requisiti GDPR.

Rifiuto degli audit:
- Diniego di accesso a siti, documentazione o personale necessari per condurre audit di sorveglianza o aggiuntivi.

Uso improprio del marchio di certificazione:
- Uso non autorizzato del marchio di certificazione Europrivacy o affermazioni fuorvianti riguardanti lo stato di certificazione.

Violazione legale o normativa:
- Gravi violazioni del GDPR o delle leggi nazionali sulla protezione dei dati che compromettono la certificazione.

11.2 Notifica del ritiro

L'organismo di certificazione notifica formalmente l'organizzazione per iscritto, specificando:
- I motivi del ritiro.
- La data effettiva del ritiro.
- L'organizzazione ha la possibilità di presentare ricorso secondo il processo di reclami e appelli (vedere Sezione 13).

11.3 Conseguenze del ritiro

- La certificazione dell'organizzazione è immediatamente invalidata.
- L'organizzazione è rimossa dal registro pubblico di certificazione.
- L'organizzazione è vietata dall'utilizzare il marchio di certificazione o rivendicare lo stato di certificazione in qualsiasi forma di comunicazione.

11.4 Richiesta di ricertificazione

Le organizzazioni che hanno avuto la loro certificazione ritirata possono fare nuova richiesta dopo:
- Aver affrontato i problemi che hanno portato al ritiro.
- Aver implementato azioni correttive e fornito prove di conformità.
- Aver subito un audit di ricertificazione completo.

Il processo di ritiro garantisce che solo le organizzazioni che soddisfano i più alti standard di protezione dei dati mantengono la certificazione, preservando così la credibilità dello schema di certificazione Europrivacy.

12. PUBBLICITÀ DELLE INFORMAZIONI E RISERVATEZZA {#13-pubblicità-delle-informazioni-e-riservatezza}

Lo schema di certificazione Europrivacy garantisce un equilibrio tra la trasparenza delle organizzazioni certificate e la riservatezza delle informazioni sensibili. I seguenti principi si applicano:

12.1 Informazioni pubbliche

Organizzazioni certificate:

L'organismo di certificazione pubblica un registro pubblicamente accessibile delle organizzazioni certificate, incluso:
- Il nome dell'organizzazione.
- L'ambito della certificazione (ad es. attività di trattamento specifiche coperte).
- Il periodo di validità della certificazione.

Decisioni di certificazione:
- Gli stati di certificazione, incluse sospensioni o ritiri, sono aggiornati nel registro pubblico per mantenere la trasparenza.

Uso dei marchi di certificazione:
- Le organizzazioni certificate possono utilizzare il marchio di certificazione Europrivacy per scopi promozionali, a condizione che rispettino le regole delineate nell'accordo di certificazione e nelle linee guida di branding.

12.2 Riservatezza

Protezione dei dati:

L'organismo di certificazione garantisce la riservatezza di tutte le informazioni non pubbliche ottenute durante il processo di certificazione, incluse:
- Documentazione interna e politiche dell'organizzazione certificata.
- Risultati e relazioni di audit.

Queste informazioni non sono divulgate a terzi a meno che:

- Richiesto dalla legge.
- Autorizzato dall'organizzazione certificata.

Controllo dell'accesso:

- Solo il personale autorizzato dell'organismo di certificazione ha accesso alle informazioni riservate.
- Gli accordi di riservatezza sono firmati da tutto il personale coinvolto nel processo di certificazione.

12.3 Eccezioni

Richieste normative:

- Le informazioni possono essere divulgate alle autorità di regolamentazione se richiesto per indagini o verifiche di conformità.

Obblighi legali:

- La divulgazione può verificarsi in risposta a ordini giudiziari o altri requisiti legali.

Dati aggregati:

- I dati non identificabili e aggregati possono essere utilizzati per scopi statistici o di reporting per migliorare il processo di certificazione.

12.4 Uso improprio delle informazioni

- Qualsiasi uso improprio di informazioni riservate da parte dell'organismo di certificazione o dell'organizzazione certificata è soggetto ad azioni correttive e, se necessario, a procedimenti legali.

Mantenendo la trasparenza mentre si proteggono le informazioni sensibili, lo schema di certificazione Europrivacy costruisce fiducia e garantisce la conformità agli standard etici e legali.

---

13. RECLAMI, APPELLI E CONTROVERSIE

Lo schema di certificazione Europrivacy fornisce un processo strutturato per la gestione dei reclami, degli appelli e delle controversie al fine di garantire equità, trasparenza e responsabilità nelle decisioni di certificazione.

13.1 **Reclami**

Ambito:

I reclami possono essere presentati riguardanti:

- Il processo di certificazione o le decisioni prese dall'organismo di certificazione.
- La non conformità di un'organizzazione certificata con i criteri Europrivacy.

I reclami devono includere:

- Una chiara descrizione del problema.
- Prove di supporto, se disponibili.
- Informazioni di contatto per il follow-up.

Gestione:

- I reclami sono riconosciuti entro un termine specificato (ad es. 5 giorni lavorativi).
- Un team neutrale indaga il reclamo e fornisce una risoluzione.
- Se il reclamo riguarda un'organizzazione certificata, l'organizzazione è informata e ha l'opportunità di rispondere.

Risultato:

- La risoluzione del reclamo è comunicata al riclamante per iscritto.
- Le azioni possono includere audit aggiuntivi o misure correttive per l'organizzazione certificata.

13.2 Appelli

Diritto di appello:

Le organizzazioni possono presentare ricorso contro le decisioni di certificazione, incluse:

- Il rifiuto di concedere la certificazione.
- La sospensione o il ritiro della certificazione.

Gli appelli devono essere presentati per iscritto entro 30 giorni dalla decisione e includere:

- La decisione oggetto di ricorso.
- Giustificazione del ricorso.
- Documentazione di supporto.

Processo di appello:

- Una commissione di appello indipendente esamina il caso per garantire l'imparzialità.
- La commissione esamina le prove, inclusi i risultati dell'audit, e prende una decisione finale.
- La decisione finale è comunicata al ricorrente entro un termine definito (ad es. 30 giorni lavorativi).

13.3 Controversie

Definizione:

- Le controversie sorgono quando c'è disaccordo tra l'organismo di certificazione e un'organizzazione o stakeholder riguardante le attività di certificazione.

Risoluzione:

- Le controversie sono inizialmente affrontate attraverso la negoziazione diretta.
- Se irrisolte, le controversie possono essere sottoposte a mediazione o arbitrato secondo l'accordo di certificazione.

Ricorso legale:

- Le parti mantengono il diritto di cercare una risoluzione legale se la mediazione o l'arbitrato fallisce.

13.4 Conservazione dei registri

- Tutti i reclami, gli appelli e le controversie sono documentati e conservati per la revisione e il miglioramento continuo del processo di certificazione.