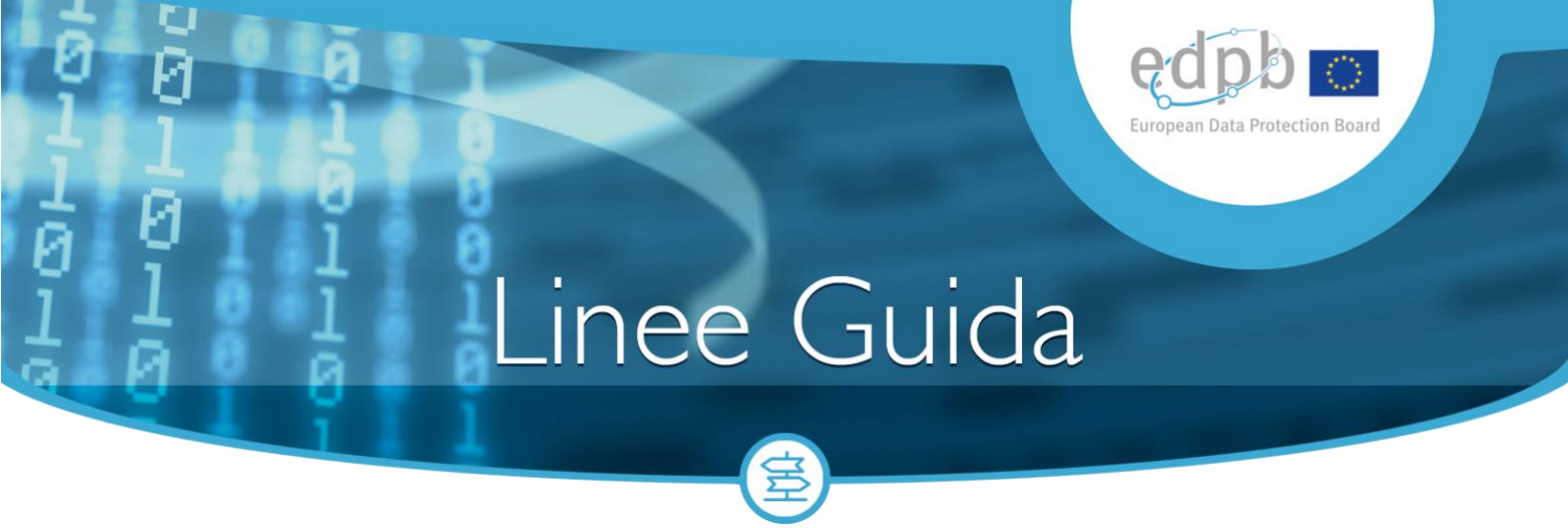

Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679

Versione 3.0

4 giugno 2019

Adottato

Cronologia delle versioni

Versione 3.0	4 giugno 2019	Aggiunta dell'allegato 2 (versione 2.0 dell'allegato 2 adottata il 4 giugno 2019 dopo consultazione pubblica)
Versione 2.1	9 aprile 2019	Adozione di una rettifica alle linee guida (paragrafo 45)
Versione 2.0	23 gennaio 2019	Adozione delle linee guida dopo consultazione pubblica - Nella stessa data l'allegato 2 (versione 1.0) è stato adottato per la consultazione pubblica
Versione 1.0	25 maggio 2018	Adozione delle linee guida per la consultazione pubblica

Sommario

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del regolamento interno del 25 maggio 2018,

tenuto conto dei risultati della consultazione pubblica sulle linee guida svoltasi tra il 30 maggio 2018 e il 12 luglio 2018 e della consultazione pubblica sull'allegato 2 svoltasi tra il 15 febbraio 2019 e il 29 marzo 2019, in conformità dell'articolo 70, paragrafo 4, del regolamento generale sulla protezione dei dati,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1 INTRODUZIONE

1. Il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679, nel prosieguo "il regolamento") istituisce un quadro di conformità aggiornato per la protezione dei dati in Europa, basato sul principio di responsabilizzazione e sulla tutela dei diritti fondamentali. Tale nuovo quadro è incentrato su una serie di misure atte ad agevolare la conformità alle disposizioni del regolamento generale sulla protezione dei dati, tra cui prescrizioni obbligatorie in circostanze specifiche (compresa la nomina di responsabili della protezione dei dati e lo svolgimento di valutazioni d'impatto sulla protezione dei dati) e misure volontarie come i codici di condotta e i meccanismi di certificazione.
2. Prima ancora che fosse adottato il regolamento generale sulla protezione dei dati il Gruppo di lavoro Articolo 29 aveva rilevato come la certificazione potesse rivestire un ruolo importante nel quadro di responsabilizzazione in materia di protezione dei dati[1]. Affinché la certificazione fornisca prove affidabili della conformità in termini di protezione dei dati è opportuno fissare norme chiare che introducano prescrizioni sull'erogazione della certificazione[2]. L'articolo 42 del regolamento generale sulla protezione dei dati fornisce la base giuridica per lo sviluppo di tali norme.
3. L'articolo 42, paragrafo 1, del regolamento generale sulla protezione dei dati stabilisce che:

   "[g]li Stati membri, le autorità di controllo, il Comitato [europeo per la protezione dei dati] e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di

[1] Gruppo di lavoro Articolo 29, parere 3/2010 sul principio di responsabilizzazione, WP173, 13 luglio 2010, punti da 69 a 71.
[2] Gruppo di lavoro Articolo 29, parere 3/2010 sul principio di responsabilizzazione, WP173, punto 69.

certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese".

4. I meccanismi di certificazione3 possono incrementare la trasparenza non solo per gli interessati, ma anche nel quadro delle relazioni tra imprese, per esempio tra titolare del trattamento e responsabile del trattamento. Il considerando 100 del regolamento generale sulla protezione dei dati rileva che l'istituzione di meccanismi di certificazione può migliorare la trasparenza e il rispetto del regolamento e consentire agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi4.

5. Il regolamento generale sulla protezione dei dati non introduce alcun diritto od obbligo di certificazione per i titolari del trattamento e i responsabili del trattamento; come stabilito all'articolo 42, paragrafo 3, la certificazione è una procedura volontaria a sostegno della dimostrazione della conformità al regolamento. Gli Stati membri e le autorità di controllo sono invitati a incoraggiare l'istituzione di meccanismi di certificazione e determineranno il coinvolgimento delle parti interessate nel processo e nel ciclo di vita della certificazione.

6. Le autorità di controllo sono inoltre tenute a considerare l'adesione a meccanismi di certificazione approvati come fattore aggravante o attenuante al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa (articolo 83, paragrafo 2, lettera j))5.

1.1 Ambito di applicazione delle linee guida

7. Le presenti linee guida hanno un ambito di applicazione limitato e non costituiscono un manuale procedurale per la certificazione in conformità del regolamento generale sulla protezione dei dati. L'obiettivo primario delle presenti linee guida è identificare requisiti e criteri generali che possano applicarsi a tutti i tipi di meccanismi per le certificazioni rilasciate in conformità degli articoli 42 e 43 del regolamento generale sulla protezione dei dati. A tal fine le linee guida:

    - esplorano le motivazioni alla base della certificazione come strumento di responsabilizzazione,
    - illustrano i concetti chiave delle disposizioni in materia di certificazione di cui agli articoli 42 e 43,
    - illustrano ciò che può essere certificato a norma degli articoli 42 e 43 e lo scopo della certificazione,

[3] Nell'ambito delle presenti linee guida il termine "meccanismi di certificazione" si riferisce collettivamente ai meccanismi di certificazione e ai sigilli e marchi di protezione dei dati, cfr. la sezione 1.3.2.
[4] Il considerando 100 rileva che dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione "che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi, al fine di migliorare la trasparenza e il rispetto del regolamento".
[5] Cfr. Gruppo di lavoro Articolo 29, Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) 2016/679 (WP253).

- favoriscono un esito della certificazione che sia significativo, inequivocabile, il più possibile riproducibile e comparabile a prescindere dal soggetto certificatore (comparabilità).

8. Il regolamento generale sulla protezione dei dati contempla una serie di modalità per l'attuazione degli articoli 42 e 43 da parte degli Stati membri e delle autorità di controllo. Le linee guida forniscono indicazioni sull'interpretazione e sull'attuazione delle disposizioni di cui agli articoli 42 e 43 e aiuteranno gli Stati membri, le autorità di controllo e gli organismi nazionali di accreditamento a istituire un approccio più coerente e armonizzato per l'applicazione dei meccanismi di certificazione in conformità del regolamento generale sulla protezione dei dati.

9. Le indicazioni contenute nelle linee guida saranno pertinenti per:

    - le autorità di controllo competenti e il Comitato europeo per la protezione dei dati, (il "Comitato") nella fase di approvazione dei criteri di certificazione in conformità dell'articolo 42, paragrafo 5, dell'articolo 58, paragrafo 3, lettera f), e dell'articolo 70, paragrafo 1, lettera o),

    - gli organismi di certificazione nella fase di definizione e revisione dei criteri di certificazione prima della presentazione all'autorità di controllo competente ai fini dell'approvazione a norma dell'articolo 42, paragrafo 5,

    - il Comitato nella fase di approvazione di un sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, e dell'articolo 70, paragrafo 1, lettera o),

    - le autorità di controllo nella fase di definizione dei propri criteri di certificazione,

    - la Commissione europea, a cui l'articolo 43, paragrafo 8, conferisce il potere di adottare atti delegati al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione,

    - il Comitato nella fase di presentazione alla Commissione di un parere in merito ai requisiti di certificazione in conformità dell'articolo 70, paragrafo 1, lettera q), e dell'articolo 43, paragrafo 8,

    - gli organismi nazionali di accreditamento, che dovranno tenere conto dei criteri di certificazione nell'ottica dell'accreditamento degli organismi di certificazione in conformità della norma EN-ISO/IEC 17065/2012 e dei requisiti aggiuntivi in conformità dell'articolo 43, e

    - i titolari del trattamento e i responsabili del trattamento durante la definizione della propria strategia di conformità al regolamento generale sulla protezione dei dati e la valutazione della certificazione come mezzo per dimostrare la conformità.

10. Il Comitato pubblicherà linee guida separate sull'identificazione dei criteri per l'approvazione dei meccanismi di certificazione come strumenti per il trasferimento verso paesi terzi o organizzazioni internazionali in conformità dell'articolo 42, paragrafo 2.

1.2 Scopo della certificazione a norma del regolamento generale sulla protezione dei dati

11. L'articolo 42, paragrafo 1, dispone l'istituzione di meccanismi di certificazione "allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento".

12. Il regolamento generale sulla protezione dei dati esemplifica il contesto in cui i meccanismi di certificazione approvati possono essere utilizzati come elementi per dimostrare il rispetto da parte del titolare del trattamento e del responsabile del trattamento dei loro obblighi riguardanti:

    - l'attuazione e la dimostrazione delle misure tecniche e organizzative adeguate di cui all'articolo 24, paragrafi 1 e 3, articolo 25 e articolo 32, paragrafi 1 e 3,
    - le garanzie sufficienti di cui all'articolo 28, paragrafi 1 (garanzie del responsabile del trattamento nei confronti del titolare del trattamento), 4 (garanzie del sub-responsabile del trattamento nei confronti del responsabile del trattamento) e 5.

13. La certificazione in sé non è una prova della conformità, ma rappresenta piuttosto un elemento che può essere utilizzato per dimostrare la conformità; è necessario pertanto che sia realizzata in modo trasparente. La dimostrazione della conformità necessita di una documentazione giustificativa, ossia di relazioni redatte appositamente che non si limitino a ribadire i criteri, ma illustrino le modalità con cui sono soddisfatti e, qualora inizialmente i criteri non fossero soddisfatti, illustrino le correzioni e le azioni correttive e la loro adeguatezza, esplicitando le ragioni del rilascio e del mantenimento della certificazione. Nella documentazione rientra anche il progetto della singola decisione per il rilascio, il rinnovo o il ritiro di un certificato, che dovrebbe riportare le ragioni, gli argomenti e le prove derivanti dall'applicazione dei criteri, nonché le conclusioni, le opinioni e le deduzioni derivanti dai fatti e dai presupposti rilevati durante la certificazione.

1.3 Concetti chiave

14. La presente sezione esamina i concetti chiave di cui agli articoli 42 e 43. Tale analisi mira a fornire una comprensione dei termini di base e dell'ambito di applicazione della certificazione a norma del regolamento generale sulla protezione dei dati.

1.3.1 Interpretazione del concetto di "certificazione"

15. Il regolamento generale sulla protezione dei dati non fornisce una definizione di "certificazione". L'Organizzazione internazionale per la standardizzazione (ISO) fornisce una definizione universale di certificazione come "rilascio da parte di un organismo indipendente di un'assicurazione scritta (un certificato) del fatto che il prodotto, il servizio o il sistema in questione soddisfa requisiti specifici". La certificazione è nota anche come "valutazione della conformità di terza parte" mentre gli organismi di certificazione possono essere indicati anche

con il termine "organismi di valutazione della conformità". Nella norma EN-ISO/IEC 17000:2004 "Valutazione della conformità — Vocabolario e principi generali" (a cui la ISO 17065 fa riferimento), la certificazione è definita come "attestazione di terza parte [...] relativa a prodotti, processi e servizi".

16. Per attestazione si intende "l'emissione di una dichiarazione, basata su una decisione successiva al riesame, da cui risulta che è stato dimostrato il rispetto dei requisiti specificati" (sezione 5.2, ISO 17000:2004).

17. Nel contesto della certificazione a norma degli articoli 42 e 43 del regolamento generale sulla protezione dei dati si intende per certificazione l'attestazione di terza parte relativa ai trattamenti effettuati dal titolare del trattamento e dal responsabile del trattamento.

1.3.2 Meccanismi di certificazione, sigilli e marchi

18. Il regolamento generale sulla protezione dei dati non fornisce una definizione di "meccanismi di certificazione, sigilli o marchi" e utilizza i termini in senso collettivo. Un certificato è una dichiarazione di conformità. Un sigillo o un marchio può essere utilizzato per indicare che la procedura di certificazione è stata completata con esito positivo. Per sigillo o marchio si intende solitamente un logo o un simbolo la cui presenza (congiuntamente al certificato) indica che l'oggetto della certificazione è stato sottoposto a una valutazione indipendente nell'ambito di una procedura di certificazione ed è conforme a specifici requisiti fissati in documenti normativi come regolamenti, norme o specifiche tecniche. Nell'ambito della certificazione a norma del regolamento generale sulla protezione dei dati tali requisiti sono fissati nei requisiti aggiuntivi che integrano le regole per l'accreditamento degli organismi di certificazione di cui alla norma EN-ISO/IEC 17065/2012 e i criteri di certificazione approvati dall'autorità di controllo competente o dal Comitato. Un certificato, sigillo o marchio in conformità del regolamento generale sulla protezione dei dati può essere rilasciato solo a seguito di una valutazione indipendente degli elementi di prova ad opera di un organismo di certificazione accreditato o dell'autorità di controllo competente che attesti il soddisfacimento dei criteri di certificazione.

19. La tabella riporta un esempio generico di processo di certificazione.

Presentazione della domanda da parte del titolare del trattamento o del responsabile del trattamento	Controllo formale da parte dell'organismo di certificazione	Valutazione Valutazione preliminare	Valutazione Valutazione dell'obiettivo di valutazione	Valutazione Convalida dei risultati	Comunicazione all'autorità di controllo competente	Certificazione	Monitoraggio	Rinnovo della certificazione
La descrizione dell'obiettivo di valutazione è inequivocabile e completa, nonché comprensiva delle interfacce?	La descrizione dell'obiettivo di valutazione può essere accettata?	Quali sono i criteri applicabili?	L'obiettivo di valutazione soddisfa i criteri?	L'obiettivo di valutazione rispecchia tutti i criteri pertinenti specificati?	Sono state fornite motivazioni per il rilascio o la revoca della certificazione?	Il certificato può essere rilasciato?	L'obiettivo di valutazione continua a soddisfare i criteri?	Il trattamento soddisfa ancora i criteri di certificazione?
È possibile accedere alle attività di trattamento dell'obiettivo di valutazione?	Tutti i documenti sono completi e aggiornati?	Quali sono i metodi di valutazione applicabili?	La documentazione dell'obiettivo di valutazione è corretta?	La valutazione è stata sufficientemente documentata?		Le relazioni sono pronte per la pubblicazione?	Il certificato/ sigillo/marchio di fiducia è utilizzato correttamente?	Gli ambiti di sviluppo sono stati adeguatamente presi in considerazione?
Articolo 42, paragrafo 6	Articolo 43, paragrafo 4	Articolo 43, paragrafo 4	Articolo 42, paragrafo 5, articolo 43, paragrafo 4	Articolo 43, paragrafo 4	Articolo 43, paragrafi 1 e 5	Articolo 43, paragrafo 1, articolo 42, paragrafo 7	Articolo 42, paragrafo 7	Articolo 42, paragrafo 7

2 IL RUOLO DELLE AUTORITÀ DI CONTROLLO

20. L'articolo 42, paragrafo 5, dispone che la certificazione sia rilasciata da un organismo di certificazione accreditato o da un'autorità di controllo competente. A norma del regolamento generale sulla protezione dei dati il rilascio delle certificazioni non è un compito obbligatorio delle autorità di controllo. Il regolamento prevede anzi una serie di modelli diversi. Un'autorità di controllo per esempio può optare per una o più delle seguenti soluzioni:

    - rilasciare essa stessa la certificazione, nel rispetto del proprio schema di certificazione,
    - rilasciare essa stessa la certificazione, nel rispetto del proprio schema di certificazione, ma delegare integralmente o parzialmente a terzi la procedura di valutazione,
    - predisporre un proprio schema di certificazione e affidare la procedura di certificazione per il rilascio della certificazione a organismi di certificazione, e
    - incoraggiare lo sviluppo di meccanismi di certificazione sul mercato.

21. Un'autorità di controllo dovrà inoltre considerare il proprio ruolo alla luce delle decisioni nazionali relative ai meccanismi di accreditamento, soprattutto laddove l'autorità di controllo ha essa stessa il potere di accreditare gli organismi di certificazione a norma dell'articolo 43, paragrafo 1, del regolamento generale sulla protezione dei dati. In questo modo ogni autorità di controllo deciderà quale approccio adottare per perseguire l'ampio obiettivo della certificazione conformemente al regolamento generale sulla protezione dei dati. Tale approccio sarà definito nell'ottica non solo dei compiti e dei poteri di cui gli articoli 57 e 58, ma anche del fatto che la certificazione dovrà essere considerata come un fattore di cui tenere conto nella determinazione delle sanzioni amministrative pecuniarie e più in generale come uno strumento per la dimostrazione della conformità.

2.1 L'autorità di controllo come organismo di certificazione

22. Un'autorità di controllo, se decide di effettuare certificazioni, dovrà valutare attentamente il proprio ruolo in relazione ai propri compiti previsti dal regolamento generale sulla protezione dei dati. Essa dovrà esercitare le proprie funzioni in modo trasparente, prestando particolare attenzione alla separazione dei poteri di indagine e di esecuzione, al fine di evitare ogni potenziale conflitto di interessi.

23. Se agisce in qualità di organismo di certificazione, l'autorità di controllo dovrà garantire l'adeguata istituzione di un meccanismo di certificazione e adottare criteri di certificazione o svilupparne di propri. Ogni autorità di controllo che rilascia certificazioni ha inoltre il compito di sottoporle a un riesame periodico (articolo 57, paragrafo 1, lettera o)) e il potere di revocarle se i requisiti per la certificazione non sono o non sono più soddisfatti (articolo 58, paragrafo 2, lettera h)). Per il soddisfacimento di tali requisiti è utile istituire una procedura di certificazione e requisiti procedurali, nonché, se non altrimenti disposto, ad esempio dalla legislazione nazionale, stipulare con le singole organizzazioni richiedenti un accordo legalmente valido per l'erogazione delle attività di certificazione. È auspicabile assicurarsi che tale accordo di certificazione imponga al richiedente di rispettare perlomeno i criteri di certificazione tra cui rientrano gli accorgimenti necessari per lo svolgimento della valutazione, il monitoraggio dell'adesione ai criteri e il riesame periodico, compreso l'accesso alle informazioni e/o ai locali, la documentazione e la pubblicazione delle relazioni e dei risultati, nonché lo svolgimento di indagini sui reclami. Si presume inoltre che l'autorità di controllo rispetti, oltre ai requisiti di cui all'articolo 43, paragrafo 2, anche i requisiti contenuti nelle linee guida relative all'accreditamento degli organismi di certificazione.

2.2 Ulteriori compiti dell'autorità di controllo in materia di certificazione

24. Negli Stati membri in cui operano organismi di certificazione l'autorità di controllo, indipendentemente dalle proprie attività, ha il potere e il compito di:

    - valutare i criteri dello schema di certificazione e predisporre un progetto di decisione (articolo 42, paragrafo 5),
    - comunicare al Comitato il progetto di decisione, qualora la decisione sia finalizzata ad approvare i criteri per la certificazione (articolo 64, paragrafo 1, lettera c) e articolo 64, paragrafo 7)), e tenere conto del parere del Comitato (articolo 64, paragrafo 1, lettera c) e articolo 70, paragrafo 1, lettera t)),
    - approvare i criteri per la certificazione (articolo 58, paragrafo 3, lettera f)) prima che possano essere effettuati accreditamenti o certificazioni (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b)),
    - pubblicare i criteri di certificazione (articolo 43, paragrafo 6),
    - agire da autorità competente per gli schemi di certificazione a livello dell'UE, che possono risultare in un sigillo europeo per la protezione dei dati approvato dal Comitato (articolo 42, paragrafo 5, e articolo 70, paragrafo 1, lettera o)), e

- ingiungere all'organismo di certificazione a) di non rilasciare la certificazione o b) di ritirare la certificazione qualora i requisiti per la certificazione (procedure o criteri di certificazione) non siano o non siano più soddisfatti (articolo 58, paragrafo 2, lettera h)).

25. Il regolamento generale sulla protezione dei dati attribuisce all'autorità di controllo il compito di approvare i criteri di certificazione, ma non di svilupparli. Per approvare i criteri di certificazione a norma dell'articolo 42, paragrafo 5, un'autorità di controllo deve avere una comprensione chiara di quanto aspettarsi, segnatamente in termini di ambito di applicazione e contenuti della dimostrazione di conformità al regolamento generale sulla protezione dei dati, nonché in merito al proprio compito di sorvegliare e assicurare l'applicazione del regolamento. L'allegato fornisce orientamenti mirati a garantire un approccio armonizzato nella valutazione dei criteri ai fini dell'approvazione.

26. A norma dell'articolo 43, paragrafo 1, gli organismi di certificazione sono tenuti a informare la propria autorità di controllo competente prima di rilasciare o rinnovare le certificazioni, al fine di consentire alla stessa di esercitare i propri poteri correttivi di cui all'articolo 58, paragrafo 2, lettera h). L'articolo 43, paragrafo 5, impone inoltre agli organismi di certificazione di trasmettere all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta. Sebbene il regolamento generale sulla protezione dei dati consenta alle autorità di controllo di determinare le modalità operative con cui ricevono, riconoscono, riesaminano e gestiscono tali informazioni (tra cui per esempio soluzioni tecnologiche per consentire agli organismi di certificazione la trasmissione delle relazioni), è possibile istituire una procedura e i relativi criteri per il trattamento delle informazioni e delle relazioni fornite su ciascun progetto di certificazione andato a buon fine da parte dell'organismo di certificazione in conformità all'articolo 43, paragrafo 1. Sulla base di tali informazioni l'autorità di controllo può esercitare il proprio potere di ingiungere all'organismo di certificazione di ritirare o non rilasciare una certificazione (articolo 58, paragrafo 2, lettera h)) e di sorvegliare e assicurare l'applicazione dei requisiti e dei criteri della certificazione a norma del regolamento generale sulla protezione dei dati (articolo 57, paragrafo 1, lettera a) e articolo 58, paragrafo 2, lettera h)). Ciò agevolerà un approccio armonizzato e la comparabilità delle certificazioni rilasciate da organismi di certificazione diversi, nonché contribuirà a garantire che le autorità di controllo siano a conoscenza delle informazioni relative allo stato della certificazione di un'organizzazione.

3 IL RUOLO DELL'ORGANISMO DI CERTIFICAZIONE

27. Il ruolo di un organismo di certificazione è quello di rilasciare, riesaminare, rinnovare e revocare le certificazioni (articolo 42, paragrafi 5 e 7) sulla base di un meccanismo di certificazione e di criteri approvati (articolo 43, paragrafo 1). L'organismo di certificazione o il proprietario dello schema di certificazione è tenuto pertanto a definire criteri di certificazione e a istituire procedure di certificazione, incluse procedure per il monitoraggio dell'adesione, lo svolgimento dei riesami, la gestione dei reclami e le revoche. I criteri di certificazione sono sottoposti a un riesame nell'ambito del processo di accreditamento, che tiene conto delle

norme e delle procedure per il rilascio delle certificazioni, dei sigilli o dei marchi (articolo 43, paragrafo 2, lettera c)).

28. L'esistenza di un meccanismo di certificazione e di criteri di certificazione è indispensabile affinché l'organismo di certificazione possa essere accreditato a norma dell'articolo 43. L'attività dell'organismo di certificazione dipende in gran parte dall'ambito di applicazione e dal tipo di criteri di certificazione, che si ripercuotono sulle procedure di certificazione e viceversa. Determinati criteri per esempio potrebbero richiedere metodi di valutazione specifici, come sopralluoghi e riesami dei codici. Tali procedure sono obbligatorie ai fini dell'accreditamento e vengono illustrate più in dettaglio nelle linee guida relative all'accreditamento.

29. A norma del regolamento generale sulla protezione dei dati l'organismo di certificazione è tenuto a trasmettere alle autorità di controllo le informazioni, soprattutto relative alle singole certificazioni, necessarie per sorvegliare l'applicazione del meccanismo di certificazione (articolo 42, paragrafo 7, articolo 43, paragrafo 5, articolo 58, paragrafo 2, lettera h)).

4 L'APPROVAZIONE DEI CRITERI DI CERTIFICAZIONE

30. I criteri di certificazione sono parte integrante di qualsiasi meccanismo di certificazione. Il regolamento generale sulla protezione dei dati pertanto prevede che i criteri di certificazione di un meccanismo di certificazione debbano essere approvati dall'autorità di controllo competente (articolo 42, paragrafo 5, e articolo 43, paragrafo 2, lettera b)). Nel caso del sigillo europeo per la protezione dei dati i criteri di certificazione sono approvati dal Comitato (articolo 42, paragrafo 5, e articolo 70, paragrafo 1, lettera o)). Entrambe le modalità di approvazione dei criteri di certificazione sono illustrate di seguito.

31. Il Comitato riconosce le seguenti finalità per l'approvazione dei criteri di certificazione:

    - rispecchiare adeguatamente i requisiti e i principi relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali stabiliti dal regolamento (UE) n. 2016/679; e
    - contribuire alla coerente applicazione del regolamento generale sulla protezione dei dati.

32. L'approvazione è concessa se i criteri di certificazione rispecchiano perfettamente il requisito del regolamento generale sulla protezione dei dati per cui il meccanismo di certificazione consente ai titolari del trattamento e ai responsabili del trattamento di dimostrare la conformità al regolamento.

4.1 Approvazione dei criteri da parte dell'autorità di controllo competente

33. I criteri di certificazione devono essere approvati dall'autorità di controllo competente prima del processo di accreditamento di un organismo di certificazione o nel corso dello stesso. Anche gli schemi o gli insiemi di criteri aggiornati o aggiuntivi in conformità della norma

ISO 17065 devono essere approvati a cura dello stesso organismo di certificazione prima che i meccanismi di certificazione modificati siano utilizzati (articolo 42, paragrafo 5 e articolo 43, paragrafo 2, lettera b)). Le autorità di controllo sono tenute a trattare tutte le richieste di approvazione dei criteri di certificazione in modo equo e non discriminatorio, in conformità di una procedura pubblica che specifichi le condizioni generali che dovranno essere soddisfatte e che descriva il processo di approvazione.

34. Un organismo di certificazione può rilasciare certificazioni solo in un determinato Stato membro in conformità dei criteri approvati dall'autorità di controllo di tale Stato membro. In altre parole i criteri di certificazione devono essere approvati dall'autorità di controllo competente del luogo in cui l'organismo di certificazione intende offrire la certificazione e ottiene l'accreditamento. Per i sistemi di certificazione a livello europeo si rimanda alla sezione seguente.

4.2 Approvazione dei criteri relativi al sigillo europeo per la protezione dei dati da parte del Comitato

35. Un organismo di certificazione può inoltre rilasciare certificazioni conformemente ai criteri relativi al sigillo europeo per la protezione dei dati approvati dal Comitato. I criteri di certificazione approvati dal Comitato in conformità dell'articolo 63 possono risultare in un sigillo europeo per la protezione dei dati (articolo 42, paragrafo 5). Alla luce delle convenzioni attuali in materia di certificazione e accreditamento il Comitato riconosce che è auspicabile evitare una frammentazione del mercato delle certificazioni relative alla protezione dei dati. Il Comitato sottolinea come l'articolo 42, paragrafo 1, dispone che gli Stati membri, le autorità di controllo, il Comitato e la Commissione incoraggino l'istituzione di meccanismi di certificazione, in particolare a livello di Unione.

4.2.1 Domanda di approvazione

36. La domanda per l'approvazione dei criteri da parte del Comitato a norma dell'articolo 42, paragrafo 5, e dell'articolo 70, paragrafo 1, lettera o), deve essere presentata tramite un'autorità di controllo competente e dovrebbe esplicitare l'intenzione del proprietario dello schema, del candidato o dell'organismo di certificazione accreditato di predisporre i criteri nell'ambito di un meccanismo di certificazione destinato ai titolari del trattamento e ai responsabili del trattamento in tutti gli Stati membri. L'autorità di controllo competente, se ritiene che i criteri possono essere approvati dal Comitato, trasmette al Comitato un progetto.

37. La scelta del luogo in cui presentare la domanda per l'approvazione dei criteri si baserà sulla sede principale dell'organizzazione proprietaria dello schema di certificazione o dell'organismo di certificazione.

38. Se un organismo di certificazione presenta una domanda, esso starà di norma richiedendo l'accreditamento o sarà già accreditato dall'autorità di controllo competente o dall'organismo nazionale di accreditamento del proprio Stato membro. Il fatto che un organismo di

certificazione sia già accreditato per un meccanismo di certificazione a norma del regolamento generale sulla protezione dei dati può contribuire a velocizzare il processo di approvazione.

4.2.2 Criteri relativi al sigillo europeo per la protezione dei dati

39. Il Comitato coordinerà il processo di valutazione e approverà i criteri relativi al sigillo europeo per la protezione dei dati come previsto. Tale valutazione prenderà in considerazione aspetti quali l'ambito di applicazione dei criteri e la loro idoneità a fungere da certificazione comune. Qualora i criteri siano approvati dal Comitato, è previsto che sia l'autorità di controllo competente per la sede principale dell'organismo di certificazione all'interno dell'UE a gestire i reclami riguardanti il meccanismo stesso e a informare le altre autorità di controllo. Tale autorità di controllo inoltre ha il compito di adottare provvedimenti nei confronti dell'organismo di certificazione. Ove opportuno, l'autorità di controllo competente informerà le altre autorità di controllo e il Comitato.

40. I criteri di certificazione per una certificazione comune sono richiesti in tutta l'UE e pertanto dovrebbero contemplare un meccanismo specifico atto a far fronte a tale richiesta. I meccanismi di certificazione europei devono essere progettati per l'utilizzo in tutti gli Stati membri. In virtù dell'articolo 42, paragrafo 5, è necessario che il meccanismo del sigillo europeo per la protezione dei dati e i relativi criteri siano adattabili in modo da poter tenere conto, se del caso, delle regolamentazioni settoriali nazionali, per esempio in materia di trattamento dei dati nelle scuole, e che contemplino l'applicazione su tutto il territorio europeo.

41. Esempio: una scuola internazionale che offre servizi di istruzione a interessati nell'Unione europea ha la propria sede nello Stato membro "A". La scuola desidera certificare la propria procedura di domanda online tramite uno schema di certificazione a livello europeo per ottenere il sigillo europeo per la protezione dei dati. La scuola intende richiedere la certificazione delle proprie operazioni di trattamento a un organismo di certificazione avente sede in uno Stato membro "B" sulla base del sigillo europeo per la protezione dei dati. I criteri per il sigillo progettati e documentati nell'ambito del meccanismo pertinente devono poter tener conto delle regolamentazioni relative alle scuole applicabili nello Stato membro "A". I criteri inoltre dovrebbero prevedere che la procedura di domanda online fornisca informazioni e tenga conto dei requisiti di protezione dei dati applicabili nello Stato membro, che potrebbero differire da quelle degli altri Stati membri, ad esempio in termini di insiemi di dati personali da presentare ai fini della candidatura, come valutazioni o risultati dei test presso la scuola dell'infanzia, periodi di conservazione, raccolta o trattamento di dati finanziari o biometrici e ulteriori limitazioni del trattamento.

    - Tra i criteri di alto livello per l'approvazione di un meccanismo relativo al sigillo europeo per la protezione dei dati figurano:
        - criteri approvati dal Comitato,
        - l'applicazione in tutte le giurisdizioni, che tenga conto, se del caso, dei requisiti di legge e delle regolamentazioni settoriali nazionali,
        -

- criteri armonizzati adattabili in modo da rispecchiare i requisiti nazionali,
    - una descrizione del meccanismo di certificazione che specifichi:
    - gli accordi di certificazione che riconoscono requisiti paneuropei,
    - le procedure atte a garantire la diversificazione nazionale e a fornire soluzioni in tal senso, nonché ad assicurare che il sigillo agevoli la dimostrazione della conformità al regolamento generale sulla protezione dei dati, e
    - la lingua delle relazioni indirizzate a tutte le autorità di controllo interessate.

42. L'allegato inoltre contiene indicazioni sui criteri relativi al sigillo europeo per la protezione dei dati.

4.2.3 Ruolo dell'accreditamento

43. Come evidenziato al punto 4.2.1, se i criteri sono stati ritenuti adatti alla certificazione comune e sono stati approvati come tali dal Comitato a norma dell'articolo 42, paragrafo 5, gli organismi di certificazione possono essere accreditati per lo svolgimento delle certificazioni a livello europeo in conformità di tali criteri.

44. Gli schemi progettati per essere offerti solo in determinati Stati membri non possono candidarsi per ottenere il sigillo UE. L'accreditamento per l'ambito di applicazione del sigillo europeo per la protezione dei dati richiederà l'accreditamento nello Stato membro della sede principale dell'organismo di certificazione che intende utilizzare lo schema, ossia l'organismo responsabile del rilascio delle certificazioni e della gestione delle attività di certificazione delle proprie entità e affiliate in altri Stati membri. Laddove altri stabilimenti o uffici gestiscano ed effettuino certificazioni in autonomia, ciascuno di tali stabilimenti o uffici dovrà essere accreditato separatamente nello Stato membro in cui ha sede. In altre parole se è solo la sede principale a rilasciare i certificati l'accreditamento è necessario esclusivamente nello Stato membro della sede principale. Se invece i certificati sono rilasciati anche da altri stabilimenti dell'organismo di certificazione, anche tali stabilimenti devono essere accreditati.

45. Di conseguenza, se un organismo di certificazione non è stato accreditato per lo svolgimento di attività di certificazione a norma del sigillo europeo per la protezione dei dati, i criteri approvati dal Comitato non possono essere utilizzati e il sigillo non può essere rilasciato.

5 SVILUPPO DEI CRITERI DI CERTIFICAZIONE

46. Il regolamento generale sulla protezione dei dati ha istituito un quadro per lo sviluppo dei criteri di certificazione. Sebbene gli articoli 42 e 43 stabiliscano le prescrizioni fondamentali relative alla procedura di certificazione nonché i criteri essenziali per le procedure di certificazione, la base di partenza per la definizione dei criteri di certificazione dev'essere

costituita dai principi e dalle norme del regolamento generale sulla protezione dei dati e deve contribuire a garantire che tali criteri siano soddisfatti.

47. Lo sviluppo dei criteri di certificazione dovrebbe concentrarsi sulla verificabilità, la rilevanza e l'idoneità dei criteri di certificazione ai fini della dimostrazione della conformità al regolamento. I criteri di certificazione dovrebbero essere formulati in modo tale da essere chiari, comprensibili e applicabili nella pratica.

48. Nella definizione dei criteri di certificazione si dovrebbe tenere conto tra l'altro dei seguenti aspetti di conformità a sostegno della valutazione dell'operazione di trattamento, se applicabili:

    - la liceità del trattamento a norma dell'articolo 6,
    - i principi del trattamento di dati personali a norma dell'articolo 5,
    - i diritti degli interessati a norma degli articoli da 12 a 23,
    - l'obbligo di notifica delle violazioni dei dati a norma dell'articolo 33,
    - l'obbligo della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita a norma dell'articolo 25,
    - se è stata effettuata o meno una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35, paragrafo 7, lettera d), se pertinente, e
    - le misure tecniche e organizzative messe in atto a norma dell'articolo 32.

49. La misura in cui i criteri prendono in esame tali aspetti può variare in base all'ambito di applicazione della certificazione, in cui possono rientrare il tipo di trattamento o trattamenti e il settore della certificazione (per esempio il settore sanitario).

5.1 Che cosa può essere certificato a norma del regolamento generale sulla protezione dei dati?

50. Il Comitato ritiene che il regolamento generale sulla protezione dei dati offra un vasto ambito di applicazione in termini di ciò che può essere certificato a norma del regolamento stesso, purché la certificazione sia mirata a dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42, paragrafo 1).

51. Nella valutazione di un trattamento devono essere presi in considerazione, se pertinenti, i tre elementi chiave seguenti:

    1. dati personali (ambito di applicazione materiale del regolamento generale sulla protezione dei dati);
    2. sistemi tecnici, ovvero le infrastrutture, ad esempio strumenti hardware e software, utilizzate per trattare i dati personali; e
    3. i processi e le procedure relative al trattamento o ai trattamenti.

52. Ciascun elemento utilizzato nei trattamenti deve essere sottoposto a una valutazione sulla base dell'insieme di criteri. Almeno quattro diversi fattori significativi possono influire sul trattamento: 1) l'organizzazione e la struttura giuridica del titolare del trattamento o del responsabile del trattamento; 2) il reparto, l'ambiente e le persone coinvolte nel trattamento o nei trattamenti; 3) la descrizione tecnica degli elementi oggetto della valutazione; e infine 4) l'infrastruttura informatica a sostegno del trattamento, compresi sistemi operativi, sistemi virtuali, banche dati, sistemi di autenticazione e autorizzazione, router e firewall, sistemi di archiviazione, infrastrutture di comunicazione o accesso a Internet e misure tecniche correlate.

53. Tutti e tre gli elementi chiave sono rilevanti ai fini della progettazione delle procedure e dei criteri di certificazione. La misura in cui sono presi in considerazione varia a seconda dell'oggetto della certificazione. In taluni casi ad esempio alcuni elementi possono non essere considerati, se non sono ritenuti pertinenti per l'oggetto della certificazione.

54. Il regolamento generale sulla protezione dei dati riporta ulteriori orientamenti volti a specificare maggiormente che cosa può essere certificato a norma del regolamento. In base all'articolo 42, paragrafo 7, le certificazioni a norma del regolamento generale sulla protezione dei dati sono rilasciate solo ai titolari del trattamento o ai responsabili del trattamento, cosa che esclude ad esempio i responsabili della protezione dei dati. L'articolo 43, paragrafo 1, lettera b), cita la norma ISO 17065, che disciplina l'accreditamento degli organismi di certificazione che valutano la conformità di prodotti, servizi e processi. Un trattamento o un insieme di trattamenti potrebbero dare luogo a un prodotto o a un servizio quali definiti dalla norma ISO 17065 e pertanto possono essere sottoposti alla certificazione. Il trattamento dei dati dei dipendenti ai fini del versamento dello stipendio o della gestione delle ferie per esempio è un insieme di operazioni ai sensi del regolamento generale sulla protezione dei dati e può dare luogo a un prodotto, processo o servizio quale definito dall'ISO.

55. Sulla base di tali considerazioni il Comitato ritiene che l'ambito di applicazione della certificazione a norma del regolamento generale sulla protezione dei dati si estenda ai trattamenti e agli insiemi di trattamenti. Tra questi possono rientrare i processi di governance intesi come misure organizzative, quindi come parti integranti di un trattamento (ad esempio il processo di governance istituito per la gestione dei reclami nell'ambito del trattamento dei dati dei dipendenti ai fini del versamento dello stipendio).

56. Per valutare la conformità del trattamento ai criteri di certificazione è necessario indicare un caso d'uso. La conformità dell'utilizzo di un'infrastruttura tecnica nell'ambito di un trattamento per esempio dipende dalle categorie di dati da trattare per cui l'infrastruttura è progettata. Le misure organizzative dipendono dalle categorie e dalla quantità dei dati e dall'infrastruttura utilizzata per il trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, oltre che dei rischi per i diritti e le libertà degli interessati.

57. Occorre tenere presente inoltre che le applicazioni informatiche possono differire di gran lunga le une dalle altre anche quando sono destinate alle stesse finalità di trattamento. Tale aspetto deve essere pertanto tenuto in considerazione nel definire l'ambito di applicazione dei meccanismi di certificazione e i criteri di certificazione; in altre parole l'ambito di applicazione della certificazione e i criteri non dovrebbero essere tanto ristretti da escludere applicazioni informatiche progettate diversamente.

5.2 Determinazione dell'oggetto della certificazione

58. L'ambito di applicazione di un meccanismo di certificazione dev'essere distinto dall'oggetto, anche detto obiettivo di valutazione, nel singolo progetto di certificazione in conformità di un meccanismo di certificazione. Un meccanismo di certificazione può definire il proprio ambito di applicazione in linea generale oppure in riferimento a uno specifico tipo o settore di trattamento, in questo modo può già identificare gli oggetti della certificazione che rientrano nell'ambito di applicazione del meccanismo di certificazione (ad esempio conservazione sicura e protezione dei dati personali contenuti nelle cassette di sicurezza digitali). In ogni caso una valutazione affidabile e significativa della conformità può avvenire solo previa descrizione precisa del singolo oggetto di un progetto di certificazione. Devono essere descritti chiaramente i trattamenti inclusi nell'oggetto della certificazione e quindi gli elementi chiave, ossia quali dati, processi e infrastrutture tecniche saranno sottoposti alla valutazione e quali no. In tale quadro dovranno sempre essere prese in considerazione e descritte le eventuali interfacce con altri processi. Ovviamente ciò che non è noto non può essere parte della valutazione e quindi non potrà essere certificato. In ogni caso il singolo oggetto della certificazione deve essere significativo rispetto al messaggio o allo slogan della certificazione, e non dovrebbe trarre in inganno l'utente, il cliente o il consumatore.

59. [Esempio 1]

    Una banca offre ai propri clienti un sito Internet per effettuare operazioni bancarie online. Tale servizio permette di effettuare bonifici, comprare azioni, avviare ordini permanenti e gestire il conto. La banca desidera certificare quanto segue in conformità di un meccanismo di certificazione in materia di protezione dei dati con un ambito di applicazione generale basato su criteri generici.

    a) Log-in sicuro

       Il log-in sicuro rappresenta un'operazione di trattamento comprensibile per l'utente finale e pertinente sotto il profilo della protezione dei dati in quanto riveste un ruolo importante nella garanzia della sicurezza dei dati personali in questione. Tale trattamento pertanto è necessario per garantire la sicurezza del login e perciò può rappresentare un obiettivo di valutazione significativo, a condizione che il certificato indichi chiaramente che viene certificato solo il trattamento del log-in.

    b) Front-end web

       Pur essendo rilevante sotto il profilo della protezione dei dati, il front-end web non è comprensibile per l'utente finale e pertanto non può costituire un obiettivo di valutazione significativo. Per l'utente inoltre non è chiaro quali dei servizi disponibili sul sito web, e quindi quali trattamenti, siano coperti dalla certificazione.

    c) Servizi bancari online

       Front-end e back-end web, se considerati congiuntamente, rappresentano trattamenti erogati nell'ambito dei servizi bancari online potenzialmente significativi per l'utente finale. In tale contesto entrambi devono essere inseriti nell'obiettivo di valutazione. Al

contrario i trattamenti non direttamente collegati alla fornitura di servizi bancari online, come ad esempio i trattamenti finalizzati alla prevenzione del riciclaggio di denaro, possono essere esclusi dall'obiettivo di valutazione.

È possibile tuttavia che tra i servizi di operazioni bancarie online offerti dalla banca tramite il proprio sito web rientrino altri servizi che a loro volta richiedono propri trattamenti. Un altro esempio di servizio che rientra in tale contesto può essere l'offerta di un prodotto assicurativo. Tale servizio aggiuntivo non è collegato direttamente con la finalità di fornire servizi bancari online e perciò può essere escluso dall'obiettivo di valutazione. Sebbene tale servizio aggiuntivo (assicurazione) sia escluso dall'obiettivo di valutazione, le interfacce per l'accesso a tale servizio integrate sul sito web rientrano nell'obiettivo di valutazione e pertanto devono essere descritte in modo da consentire una netta distinzione tra i servizi. Tale descrizione è necessaria per identificare e valutare possibili flussi di dati tra i due servizi.

60. [Esempio 2]

    Una banca offre ai propri clienti un servizio che consente loro di aggregare informazioni relative a conti diversi e a carte di credito emesse da più banche (aggregazione dei conti). La banca desidera certificare il proprio servizio in conformità del regolamento generale sulla protezione dei dati. L'autorità di controllo competente ha approvato un insieme di criteri di certificazione specifici per questo tipo di attività. Nell'ambito di applicazione del meccanismo di certificazione rientrano solo i seguenti aspetti di conformità:

    - autenticazione dell'utente, e
    - modalità accettabili per ottenere dalle altre banche/dagli altri servizi i dati che devono essere aggregati.

    Poiché l'ambito di applicazione di tale meccanismo di certificazione già di per sé definisce l'obiettivo di valutazione, non è possibile restringerlo ulteriormente in maniera significativa all'interno dell'ambito di applicazione proposto e certificare solo caratteristiche specifiche o una singola attività di trattamento. In questo caso l'obiettivo di valutazione coincide con un ambito di applicazione specifico.

5.3 Metodi di valutazione e metodologia della valutazione

61. Per una valutazione di conformità finalizzata a dimostrare la conformità dei trattamenti occorre identificare e definire i metodi per la valutazione e la metodologia della valutazione. È importante stabilire se le informazioni alla base della valutazione sono raccolte esclusivamente a partire dalla documentazione (cosa che in sé non sarebbe sufficiente) o se le informazioni sono raccolte attivamente in loco e tramite accesso diretto o indiretto. La modalità di raccolta delle informazioni si ripercuote sulla rilevanza della certificazione e pertanto dovrebbe essere definita e descritta.

    Le procedure per il rilascio e il riesame periodico delle certificazioni dovrebbero comprendere specifiche atte a identificare il livello di valutazione adeguato (in termini di profondità e granularità) per soddisfare i criteri di certificazione, nonché contemplare:

- informazioni e indicazioni specifiche sui metodi di valutazione applicati e sulle risultanze raccolte, per esempio nell'ambito di controlli in loco o a partire dalla documentazione,
- metodi di valutazione incentrati sui trattamenti (dati, sistemi, processi) e sulle finalità del trattamento,
- l'identificazione delle categorie di dati, delle esigenze di protezione e dell'eventuale coinvolgimento di responsabili del trattamento o di terzi,
- l'identificazione dei ruoli e l'esistenza di un meccanismo di controllo degli accessi che definisca ruoli e responsabilità.

62. La profondità della valutazione si ripercuote sulla rilevanza e sul valore della certificazione. Una riduzione della profondità della valutazione per scopi pratici o per contenere i costi si tradurrà in una minore rilevanza della certificazione in materia di protezione dei dati. Le decisioni sulla granularità della valutazione d'altro canto potrebbero superare la capacità finanziaria del richiedente e spesso anche le capacità di valutatori e revisori. Ai fini della dimostrazione della conformità, per mantenere la significatività potrebbe non essere sempre indispensabile raggiungere un livello molto dettagliato di analisi dei sistemi informatici utilizzati.

5.4 Documentazione della valutazione

63. La documentazione di certificazione dovrebbe essere accurata ed esauriente. Una lacuna nella documentazione si traduce nell'impossibilità di effettuare una valutazione corretta. La funzione essenziale della documentazione di certificazione è garantire la trasparenza del processo di valutazione nel quadro del meccanismo di certificazione. La documentazione fornisce risposte relative ai requisiti previsti per legge. I meccanismi di certificazione dovrebbero prevedere una metodologia di documentazione standardizzata. Successivamente la valutazione consentirà di confrontare la documentazione di certificazione con la situazione corrente in loco e con i criteri di certificazione.

64. Una documentazione esauriente di quanto è stato certificato e della metodologia utilizzata è funzionale a una maggiore trasparenza. A norma dell'articolo 43, paragrafo 2, lettera c), i meccanismi di certificazione dovrebbero istituire procedure che consentano il riesame delle certificazioni. Una documentazione dettagliata potrebbe essere il mezzo di comunicazione più indicato per consentire all'autorità di controllo di valutare se e in quale misura la certificazione possa essere riconosciuta nell'ambito di indagini formali. È pertanto opportuno che la documentazione prodotta nel corso della valutazione si concentri su tre aspetti fondamentali:
    - coerenza dei metodi di valutazione impiegati,
    - metodi di valutazione mirati a dimostrare la conformità dell'oggetto della certificazione ai criteri di certificazione e quindi al regolamento, e
    - convalida dei risultati della valutazione da parte di un organismo di certificazione indipendente e imparziale.

5.5 Documentazione dei risultati

65. Il considerando 100 fornisce informazioni sugli obiettivi perseguiti con l'introduzione della certificazione.

"Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi."

66. La documentazione e la comunicazione dei risultati rivestono un ruolo importante ai fini del miglioramento della trasparenza. Gli organismi di certificazione che utilizzano meccanismi di certificazione, sigilli o marchi rivolti agli interessati (in qualità di consumatori o clienti) dovrebbero fornire informazioni facilmente accessibili, comprensibili e significative riguardo al trattamento o ai trattamenti certificati. Tali informazioni pubbliche dovrebbero comprendere almeno:

    - la descrizione dell'obiettivo di valutazione,
    - l'indicazione dei criteri approvati applicati all'obiettivo di valutazione in questione,
    - la metodologia di valutazione dei criteri (valutazione in loco, documentazione ecc.), e
    - la durata della validità del certificato, e
    - dovrebbe consentire alle autorità di controllo e al pubblico la comparabilità dei risultati.

6 ORIENTAMENTI PER LA DEFINIZIONE DEI CRITERI DI CERTIFICAZIONE

67. I criteri di certificazione sono parte integrante di un meccanismo di certificazione. Nella procedura di certificazione rientrano requisiti riguardanti le modalità, gli autori, l'entità e la granularità della valutazione che sarà effettuata all'interno dei singoli progetti di certificazione relativi a uno specifico obiettivo di valutazione. I criteri di certificazione stabiliscono i requisiti nominali a fronte dei quali è valutato il trattamento effettivo definito nell'obiettivo di valutazione. Le presenti linee guida per la definizione dei criteri di certificazione forniscono indicazioni di massima per agevolare la valutazione dei criteri di certificazione ai fini dell'approvazione.

    - Nell'ambito dell'approvazione o della definizione dei criteri di certificazione è opportuno tenere presenti le considerazioni generali illustrate di seguito. I criteri di certificazione dovrebbero:
    - essere uniformi e verificabili,

- specificare in particolare i propri obiettivi e gli orientamenti attuativi per raggiungere tali obiettivi, in modo tale da poter essere sottoposti a controlli volti ad agevolare la valutazione dei trattamenti a norma del regolamento generale sulla protezione dei dati,
- essere pertinenti rispetto al pubblico a cui si rivolgono (relazioni tra imprese oppure relazioni tra imprese e clienti),
- tenere conto di eventuali altre norme (ad esempio norme ISO o norme a livello nazionale) e laddove opportuno essere interoperabili con le stesse,
- essere flessibili e scalabili in modo da applicarsi a organizzazioni di diverso tipo e dimensione, comprese le micro, piccole e medie imprese in conformità dell'articolo 42, paragrafo 1, nonché da rispecchiare l'approccio basato sul rischio di cui al considerando 77.

68. Una piccola società locale, ad esempio un rivenditore al dettaglio, di norma effettuerà trattamenti meno complessi di una grande multinazionale di vendita. Sebbene le prescrizioni relative alla liceità del trattamento siano le stesse, occorre tenere conto dell'ambito di applicazione del trattamento dei dati e della sua complessità; è necessario pertanto che i meccanismi di certificazione e i loro criteri siano scalabili sulla base dell'attività di trattamento in questione.

6.1 Norme attuali

69. Gli organismi di certificazione dovranno considerare il modo in cui i criteri specifici tengono conto degli attuali strumenti pertinenti, come ad esempio codici di condotta, norme tecniche o iniziative legislative e di regolamentazione a livello nazionale. Idealmente i criteri saranno interoperabili con le attuali norme atte ad agevolare un titolare del trattamento o un responsabile del trattamento nell'ottemperanza ai propri obblighi previsti dal regolamento generale sulla protezione dei dati. Tuttavia, anche se le norme di settore spesso si concentrano sulla protezione e sulla sicurezza delle organizzazioni nei confronti di eventuali minacce, il regolamento generale sulla protezione dei dati è incentrato sulla protezione dei diritti fondamentali delle persone fisiche. Nella progettazione dei criteri o nell'approvazione dei criteri o dei meccanismi di certificazione sulla base delle norme di settore si dovrà tener conto di tale differenza di prospettiva.

6.2 Definizione dei criteri

70. I criteri di certificazione devono corrispondere alla dichiarazione di certificazione (messaggio o indicazione) di un dato meccanismo o schema di certificazione e soddisfare le aspettative create dalla stessa. La denominazione di un meccanismo di certificazione può già identificare l'ambito di applicazione e ripercuotersi sulla definizione dei criteri.

71. [Esempio 3]

L'ambito di applicazione di un meccanismo denominato "MarchioPrivacySanità" dovrebbe essere ristretto al solo settore sanitario. Dato il nome del sigillo ci si aspetta infatti che siano stati esaminati i requisiti di protezione dei dati relativi ai dati sanitari. Di conseguenza i criteri di tale meccanismo dovranno essere adeguati a valutare i requisiti di protezione dei dati in tale settore.

72. [Esempio 4]

    Un meccanismo relativo alla certificazione dei trattamenti che prevedono sistemi di governance nell'ambito del trattamento dei dati dovrebbe identificare criteri che consentano il riconoscimento e la valutazione dei processi di governance e delle misure tecniche e organizzative a sostegno degli stessi.

73. [Esempio 5]

    I criteri di un meccanismo relativo al cloud computing dovranno tener conto degli speciali requisiti tecnici necessari per l'utilizzo dei servizi basati sul cloud. Se per esempio i server sono utilizzati al di fuori dell'UE i criteri dovranno tenere in considerazione le condizioni relative al trasferimento di dati personali verso paesi terzi stabilite al capo V del regolamento generale sulla protezione dei dati.

74. I criteri progettati per adattarsi a diversi obiettivi di valutazione in diversi settori e/o Stati membri dovrebbero poter essere applicati a diversi contesti, consentire l'identificazione di misure idonee per l'adeguamento a trattamenti di piccola, media o grande entità e riflettere i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, in linea con il regolamento generale sulla protezione dei dati. Di conseguenza le procedure di certificazione (ad esempio riguardanti la documentazione, la verifica o il metodo e la profondità della valutazione) che integrano i criteri devono rispondere a tali esigenze e consentire la definizione e l'attuazione di regole, ad esempio per quanto riguarda l'applicazione dei criteri pertinenti ai singoli progetti di certificazione. I criteri devono permettere di valutare più facilmente se sono state fornite o meno garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate.

6.3 Periodo di validità dei criteri di certificazione

75. I criteri di certificazione devono essere affidabili nel tempo, ma non per questo dovrebbero essere immutabili. Una loro revisione dovrà essere effettuata per esempio in caso di:

    - modifiche del quadro giuridico,
    - interpretazione dei termini e delle condizioni nell'ambito di sentenze della Corte di giustizia dell'Unione europea, o
    - avanzamento dello stato della tecnica.

Per il Comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

ALLEGATO 1: COMPITI E POTERI DELLE AUTORITÀ DI CONTROLLO IN RELAZIONE ALLA CERTIFICAZIONE IN CONFORMITÀ DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

	Disposizioni	Prescrizioni
Compiti	Articolo 43, paragrafo 6	L'autorità di controllo è tenuta a rendere pubblici i criteri di cui all'articolo 42, paragrafo 5, in forma facilmente accessibile e a trasmetterli al Comitato.
	Articolo 57, paragrafo 1, lettera n)	L'autorità di controllo è tenuta ad approvare i criteri di certificazione a norma dell'articolo 42, paragrafo 5.
	Articolo 57, paragrafo 1, lettera o)	Ove applicabile (ossia qualora rilasci la certificazione), l'autorità di controllo è tenuta a effettuare un riesame periodico della certificazione rilasciata in conformità dell'articolo 42, paragrafo 7.
	Articolo 64, paragrafo 1, lettera c)	L'autorità di controllo è tenuta a comunicare il progetto di decisione al Comitato quando la decisione è finalizzata ad approvare i criteri per la certificazione di cui all'articolo 42, paragrafo 5.
Poteri	Articolo 58, paragrafo 1, lettera c)	L'autorità di controllo ha il potere di effettuare riesami delle certificazioni a norma dell'articolo 42, paragrafo 7.
	Articolo 58, paragrafo 2, lettera h)	L'autorità di controllo ha il potere di revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione.
	Articolo 58, paragrafo 3, lettera e)	L'autorità di controllo ha il potere di accreditare gli organismi di certificazione.
	Articolo 58, paragrafo 3, lettera f)	L'autorità di controllo ha il potere di rilasciare certificazioni e approvare i criteri di certificazione.

ALLEGATO 2

1 INTRODUZIONE

L'allegato 2 fornisce orientamenti per il riesame e la valutazione dei criteri di certificazione di cui all'articolo 42, paragrafo 5, e individua gli elementi che l'autorità di controllo e il Comitato prendono in considerazione e applicano per approvare i criteri di certificazione di un meccanismo di certificazione. Gli organismi di certificazione e le organizzazioni proprietarie di schemi di certificazione che desiderino elaborare tali criteri e presentarli per l'approvazione dovrebbero tenere conto delle domande sotto riportate. L'elenco non è esaustivo ma contiene il numero minimo di elementi di cui tenere conto. Sebbene non tutte siano applicabili, le domande dovrebbero essere prese in considerazione in fase di elaborazione dei criteri; potrebbe rendersi necessario illustrare le motivazioni dell'esclusione di aspetti specifici dall'ambito di tali criteri. Alcune domande sono ripetute, in quanto muovono da punti di vista diversi. I presenti orientamenti dovrebbero essere considerati alla luce delle disposizioni del regolamento generale sulla protezione dei dati e, ove applicabile, della legislazione nazionale.

2 AMBITO DI APPLICAZIONE DEL MECCANISMO DI CERTIFICAZIONE E OGGETTO DELLA VALUTAZIONE (TOE)

a. L'ambito di applicazione del meccanismo di certificazione (per il quale sono utilizzati i criteri per la protezione dei dati) è descritto chiaramente?

b. L'ambito di applicazione del meccanismo di certificazione è significativo per il pubblico destinatario ed è formulato in modo non fuorviante?

- *Esempio: un "Sigillo di affidabilità aziendale" induce a pensare che tutte le attività di trattamento della società sono state sottoposte a controllo, anche se in realtà sono soggetti a certificazione soltanto trattamenti specifici, ad esempio i processi di pagamento online. L'ambito di applicazione è pertanto fuorviante.*

c. L'ambito di applicazione del meccanismo di certificazione riflette tutti gli aspetti pertinenti dei trattamenti?

- *Esempio: un "Marchio di tutela dei dati sanitari" deve comprendere tutti i dati valutativi relativi alla salute al fine di soddisfare i requisiti di cui all'articolo 9.*

d. L'ambito di applicazione del meccanismo di certificazione consente una certificazione significativa della protezione dei dati, tenuto conto della natura, del contenuto e del rischio dei trattamenti connessi?

- *Esempio: se l'ambito di applicazione del meccanismo di certificazione riguarda soltanto aspetti specifici dei trattamenti (ad esempio la raccolta di dati ma non i trattamenti ulteriori, quali il trattamento per la creazione di profili pubblicitari o la gestione dei diritti dell'interessato) non è significativo per gli interessati.*

e. L'ambito di applicazione del meccanismo di certificazione riguarda il trattamento dei dati personali nel singolo paese o anche il trattamento e/o i trasferimenti transfrontalieri?

f. I criteri di certificazione descrivono sufficientemente in che modo dovrebbe essere definito l'oggetto della valutazione?

- *Esempio: un "Sigillo privacy" che indichi un ambito di applicazione generico in cui si prevede soltanto "la specificazione del trattamento soggetto a certificazione" non fornirebbe orientamenti sufficientemente chiari sulle modalità di definizione e descrizione dell'oggetto della valutazione.*
- *Esempio: nel caso di un ambito di applicazione (specifico) quale un "Sigillo per le cassette di sicurezza digitali", relativo alla conservazione sicura dei dati personali, i relativi criteri dovrebbero descrivere dettagliatamente i requisiti da soddisfare per ricadere nell'ambito suddetto: per esempio, presenza della definizione di cassetta di sicurezza, i requisiti di sistema, le misure tecniche e organizzative obbligatorie. In tal caso l'ambito di applicazione consente di definire chiaramente l'oggetto della valutazione.*

(1) I criteri prevedono che l'oggetto della valutazione identifichi tutti i trattamenti pertinenti, illustri i flussi di dati e definisca il settore di applicazione dell'oggetto stesso?

- *Esempio: un meccanismo di certificazione offre la certificazione dei trattamenti effettuati dai titolari del trattamento a norma del regolamento generale sulla protezione dei dati, senza specificare ulteriormente il settore di applicazione (ambito di applicazione generale). I criteri del meccanismo impongono al titolare che fa richiesta della certificazione di definire il trattamento specificamente in questione (l'oggetto della valutazione) con riferimento alle categorie di dati, ai sistemi e ai processi utilizzati.*

(2) I criteri impongono al richiedente di chiarire dove inizia e dove finisce il trattamento soggetto a valutazione? I criteri impongono che l'oggetto della valutazione preveda la presenza di interfacce qualora esso non comprenda trattamenti reciprocamente dipendenti ? Sono fornite giustificazioni soddisfacenti?

- *Esempio: un oggetto della valutazione descrive in modo sufficientemente dettagliato i trattamenti effettuati da un servizio basato in internet, e quindi include la registrazione degli utenti, la fornitura di servizi, la fatturazione, la registrazione di indirizzi IP, interfacce con gli utenti e le parti terze, ed esclude invece l'hosting dei server (includendo tuttavia gli accordi relativi al trattamento e alle misure tecniche e organizzative).*

g. I criteri garantiscono che ogni oggetto di valutazione sia comprensibile ai destinatari, compresi, ove necessario, gli interessati?

3 REQUISITI GENERALI

a. Tutti i termini pertinenti utilizzati nel catalogo dei criteri (ossia la serie completa dei criteri di certificazione) sono identificati, spiegati e descritti?

b. Tutti i riferimenti normativi sono identificati?

c. I criteri includono la definizione delle responsabilità per quanto riguarda la protezione dei dati, delle procedure e dei trattamenti che rientrano nell'ambito di applicazione del meccanismo di certificazione?

4 TRATTAMENTI, ARTICOLO 42, PARAGRAFO 1

Per quanto riguarda l'ambito di applicazione (generale o specifico) del meccanismo di certificazione, i criteri includono tutte le componenti dei trattamenti (dati, sistemi e processi)?

a. Con riguardo all'oggetto della valutazione, i criteri richiedono l'individuazione delle basi giuridiche valide per il trattamento?

b. Con riguardo all'oggetto della valutazione, i criteri tengono conto delle pertinenti fasi del trattamento e dell'intero ciclo di vita dei dati, compresa la cancellazione e/o l'anonimizzazione?

c. Con riguardo all'oggetto della valutazione, i criteri prevedono la portabilità dei dati?

d. Con riguardo all'oggetto della valutazione, i criteri consentono di individuare e tenere conto di tipologie particolari di trattamenti, quali i processi decisionali automatizzati e la profilazione?

e. Con riguardo all'oggetto della valutazione, i criteri consentono di individuare categorie particolari di dati?

f. I criteri consentono e richiedono di valutare il rischio dei singoli trattamenti e le esigenze di tutela per i diritti e le libertà degli interessati?

g. I criteri consentono e richiedono di tenere adeguatamente conto dei rischi per i diritti e le libertà delle persone fisiche?

...

5 LICEITÀ DEL TRATTAMENTO

a. I criteri richiedono di controllare la liceità dei singoli trattamenti con riguardo a finalità e necessità del trattamento stesso?

b. I criteri richiedono di controllare tutti i requisiti previsti per la base giuridica dei singoli trattamenti?

6 PRINCIPI, ARTICOLO 5

a. I criteri tengono debitamente conto di tutti i principi di protezione dei dati di cui all'articolo 5?

b. I criteri impongono la dimostrazione della minimizzazione dei dati con riguardo al singolo oggetto della valutazione?

...

7 OBBLIGHI GENERALI DEI TITOLARI E DEI RESPONSABILI DEL TRATTAMENTO

a. I criteri richiedono la prova dell'esistenza di accordi contrattuali tra i responsabili e i titolari del trattamento?

b. Gli accordi tra i titolari e i responsabili del trattamento sono soggetti a valutazione?

c. I criteri riflettono gli obblighi del titolare del trattamento previsti dal Capo IV?

d. I criteri richiedono la prova del riesame e dell'aggiornamento delle misure tecniche e organizzative attuate dal titolare del trattamento a norma dell'articolo 24, paragrafo 1?

e. I criteri richiedono di controllare se l'organizzazione abbia valutato la necessità di designare un responsabile della protezione dei dati a norma dell'articolo 37? In caso affermativo, il responsabile della protezione dei dati soddisfa i requisiti di cui agli articoli da 37 a 39?

f. I criteri richiedono di controllare se, in base a quanto previsto dall'articolo 30, paragrafo 5, occorra tenere un registro delle attività di trattamento e, in caso affermativo, se il registro è tenuto conformemente ai requisiti dell'articolo 30?

8 DIRITTI DELL'INTERESSATO

a. I criteri tengono adeguatamente conto del diritto all'informazione dell'interessato e prevedono l'attuazione delle apposite misure?

b. I criteri prevedono che gli interessati abbiano un accesso e un controllo adeguati, o anche più ampi, rispetto ai propri dati, compresa la portabilità dei dati?

c. I criteri richiedono l'adozione di misure che prevedono la possibilità di intervenire nei trattamenti al fine di garantire i diritti degli interessati e consentire rettifiche, cancellazioni o limitazioni?

...

9 RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

a. I criteri consentono e richiedono di valutare il rischio per i diritti e le libertà delle persone fisiche?

b. I criteri prevedono o richiedono una metodologia riconosciuta di valutazione del rischio? In caso affermativo, è adeguata?

c. I criteri consentono e richiedono di valutare l'impatto dei trattamenti previsti sui diritti e sulle libertà delle persone fisiche?

d. I criteri richiedono consultazioni preliminari per quanto riguarda i rischi residuali che non è stato possibile mitigare, sulla base dei risultati della valutazione d'impatto della protezione dei dati (DPIA)?

10 MISURE TECNICHE E ORGANIZZATIVE A GARANZIA DELLA PROTEZIONE

a. I criteri richiedono l'applicazione di misure tecniche e organizzative che garantiscono la riservatezza dei trattamenti?

b. I criteri richiedono l'applicazione di misure tecniche e organizzative che garantiscono l'integrità dei trattamenti?

c. I criteri richiedono l'applicazione di misure tecniche e organizzative che garantiscono la disponibilità dei trattamenti?

d. I criteri richiedono l'applicazione di misure che garantiscano la trasparenza dei trattamenti per quanto riguarda:

e. la responsabilizzazione?

f. i diritti dell'interessato?

g. la valutazione di singoli trattamenti, ad esempio la trasparenza degli algoritmi?

h. I criteri richiedono l'applicazione di misure tecniche e organizzative che garantiscono i diritti dell'interessato, ad esempio in materia di informazioni all'interessato o di portabilità dei dati?

i. I criteri richiedono l'applicazione di misure tecniche e organizzative che prevedono la possibilità di intervenire nei trattamenti per garantire i diritti dell'interessato e consentire rettifiche, cancellazioni o limitazioni?

j. I criteri richiedono l'applicazione di misure che prevedono la possibilità di intervenire nel trattamento per correggere o controllare il sistema o il processo?

k. I criteri richiedono l'applicazione di misure tecniche o organizzative per assicurare la minimizzazione dei dati, ad esempio, la separazione fra i dati e l'interessato o l'eliminazione del relativo collegamento, l'anonimizzazione o la pseudonimizzazione o l'isolamento dei sistemi di dati?

l. I criteri richiedono misure tecniche per attuare la protezione dei dati per impostazione predefinita?

m. I criteri richiedono misure tecniche e organizzative che attuino la protezione dei dati fin dalla progettazione, ad esempio un sistema di gestione dei dati atto a dimostrare, informare, controllare e far rispettare i requisiti in materia di protezione dei dati?

n. I criteri richiedono misure tecniche e organizzative che attuino una formazione adeguata e periodica per il personale che accede ai dati personali su base permanente o periodica?

o. I criteri prevedono misure di riesame?

p. I criteri richiedono un'autovalutazione/un controllo interno?

q. I criteri richiedono misure per garantire il corretto e tempestivo assolvimento degli obblighi di notifica di violazioni dei dati?

r. I criteri richiedono la sussistenza e la verifica di procedure per la gestione degli incidenti?

s. I criteri prevedono il monitoraggio delle questioni emergenti relative alla privacy e alla tecnologia e l'aggiornamento dello schema di certificazione ove necessario?

...

11 ALTRI ASPETTI SPECIFICI ATTI A PROMUOVERE LA PROTEZIONE DEI DATI

a. I criteri prevedono l'implementazione di tecniche di potenziamento della protezione dei dati? Per esempio, criteri che richiedono un potenziamento della protezione dei dati mediante l'eliminazione o la riduzione di dati personali e/o del rischio legato alla protezione dei dati.

- *Esempio: criteri che prevedessero un potenziamento della non-riconducibilità dei dati tramite tecniche di gestione dell'identità incentrate sull'utente, per esempio mediante credenziali basate su attributi dell'utente (ABC), anziché mediante tecniche incentrate sull'organizzazione, rifletterebbero l'implementazione di tecniche di potenziamento della protezione dei dati.*

b. I criteri prevedono l'implementazione di meccanismi potenziati di controllo da parte degli interessati per facilitare l'autodeterminazione e i processi decisionali?

...

12 CRITERI FINALIZZATI A DIMOSTRARE L'ESISTENZA DI GARANZIE ADEGUATE PER IL TRASFERIMENTO DEI DATI PERSONALI

Tali criteri saranno esaminati nelle linee guida di prossima pubblicazione relative all'articolo 42, paragrafo 2.

13 CRITERI AGGIUNTIVI PER IL SIGILLO EUROPEO PER LA PROTEZIONE DEI DATI

a. I criteri prevedono l'applicabilità a tutti gli Stati membri?

b. I criteri sono in grado di tener conto della legislazione in materia di protezione dei dati o dei relativi scenari di tutti gli Stati membri?

c. I criteri prevedono che lo specifico oggetto della valutazione sia considerato alla luce della legislazione settoriale degli Stati membri in materia di protezione dei dati?

d. I criteri prevedono che il titolare o il responsabile del trattamento fornisca agli interessati e alle parti interessate informazioni nelle lingue degli Stati membri:

e. sul trattamento/sull'oggetto della valutazione?

f. sulla documentazione del trattamento/dell'oggetto della valutazione?

g. sui risultati della valutazione?

...

14 VALUTAZIONE GENERALE DEI CRITERI

a. I criteri coprono integralmente l'ambito di applicazione del meccanismo di certificazione (ossia, si tratta di criteri esaustivi) in modo da fornire garanzie sufficienti dell'affidabilità della certificazione?

- *Esempio: se l'ambito di applicazione del meccanismo di certificazione riguarda i trattamenti di dati sanitari, dovrebbe essere garantito un livello elevato di protezione dei dati mediante la definizione di criteri che assicurino, ad esempio, una valutazione approfondita e l'attuazione dei principi di protezione della vita privata fin dalla progettazione e per impostazione predefinita.*

b. I criteri sono proporzionali all'entità del trattamento che ricade nell'ambito di applicazione del meccanismo di certificazione, alla sensibilità delle informazioni e al rischio del trattamento?

c. I criteri possono migliorare l'osservanza delle norme di protezione dei dati da parte dei titolari e dei responsabili del trattamento?

d. Gli interessati ne trarranno beneficio in termini di diritto all'informazione, anche attraverso l'illustrazione agli interessati stessi dei risultati auspicati?