Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP

Office fédéral de la justice
Ambito direzionale Diritto pubblico

31 agosto 2022

Ordinanza sulle certificazioni in materia di protezione dei dati (OCPD)

Rapporto esplicativo

BJ-D-83643401/176

Indice

1 Situazione iniziale

1.1 Contesto

In seguito alla valutazione della legge federale del 19 giugno 1992[1] sulla protezione dei dati (LPD) e in considerazione degli sviluppi tecnologici e dell'evoluzione del diritto europeo, il Consiglio federale ha deciso di rivedere parte della legislazione federale sulla protezione dei dati. Il 15 settembre 2017 ha quindi adottato il messaggio concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati[2]. Il progetto di legge comprende da una parte la revisione totale della LPD e dall'altra la revisione parziale di altre leggi federali, al fine di attuare la direttiva (UE) 2016/680[3]. Il Parlamento ha diviso in due tappe il progetto del Consiglio federale. La prima tappa attua la direttiva (UE) 2016/680 riguardante la protezione dei dati in materia penale: la legge federale del 28 settembre 2018[4] sulla protezione dei dati personali nell'ambito dell'applicazione dell'acquis di Schengen in materia penale (Legge sulla protezione dei dati in ambito Schengen, LPDS) è entrata in vigore il 1° marzo 2019. In una seconda tappa il Parlamento ha dibattuto la nuova legge sulla protezione dei dati (nLPD), adottata il 25 settembre 2020[5].

In virtù della revisione totale della LPD vanno adeguate anche le relative ordinanze, in particolare l'ordinanza del 14 giugno 1993[6] relativa alla legge federale sulla protezione dei dati (OLPD) e l'ordinanza del 28 settembre 2007[7] sulle certificazioni in materia di protezione dei dati (OCPD).

1.2 Modifiche della nLPD relative alla certificazione

L'articolo 13 nLPD, riguardante la certificazione, riprende l'articolo 11 LPD aggiungendo la possibilità di far certificare prodotti e servizi. In realtà, l'unica novità materiale è l'introduzione dei «servizi», poiché i «prodotti» sono già menzionati nella legislazione in vigore dalla OCPD. Come nel diritto vigente, il capoverso 2 incarica il Consiglio federale di emanare disposizioni sul riconoscimento delle procedure di certificazione e sull'introduzione di un marchio di qualità inerente alla protezione dei dati, tenendo conto del diritto internazionale e delle norme tecniche riconosciute a livello internazionale. Inoltre, come previsto dall'articolo 22 capoverso 5 nLPD, il titolare privato del trattamento può rinunciare a una valutazione d'impatto se si avvale di un sistema, un prodotto o un servizio che dispone di una certificazione secondo l'articolo 13 nLPD per l'impiego previsto. Inoltre, la nuova versione dell'OLPD (rinominata «ordinanza sulla protezione dei dati» [OPDa]) consente anche la comunicazione dei dati all'estero sulla base di una certificazione (cfr. art. 12 OPDa che si fonda sull'art. 16 cpv. 3 nLPD).

1.3 Costituzionalità e compatibilità con gli obblighi internazionali

La nuova ordinanza sulle certificazioni in materia di protezione dei dati (nOCPD) è un'ordinanza esecutiva della versione riveduta della legge federale sulla protezione dei dati adottata dal Parlamento il 25 settembre 2020 e adempie il mandato conferito al Consiglio federale

---

1 RS **235.1**

2 FF **2017** 5939

3 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 119 del 4.5.2016, pag. 89.

4 RS **235.3**

5 FF **2020** 6695

6 RS **235.11**

7 RS **235.13**

dall'articolo 13 capoverso 2 nLPD. In questo senso, l'ordinanza è conforme alla legge e per quanto riguarda gli aspetti giuridici si può rinviare alle spiegazioni contenute nel messaggio (cfr. FF *2017* 5939, in particolare 6165 segg.).

2 Punti essenziali del progetto

Le modifiche principali della OCPD riguardano diversi aspetti. Innanzitutto viene semplificata e uniformata la terminologia usata. Ad esempio, nella nLPD si fa distinzione tra la funzione dell'Incaricato federale della protezione dei dati e della trasparenza e l'istituzione nel suo complesso. L'istituzione è indicata con l'abbreviazione «IFPDT», mentre il termine «Incaricato» è riservato al capo dell'istituzione. I necessari adeguamenti sono stati quindi riportati nella nOCPD.

Al fine di designare i soggetti idonei alla certificazione, la nOCPD ha ripreso anche i termini dell'articolo 13 della nLPD, ovvero «fornitori di programmi o sistemi di trattamento di dati personali», «titolari del trattamento» e «responsabili del trattamento». Pertanto, si rinuncia al termine «organismo certificato», utilizzato in passato nel contesto della OCPD, in particolare perché il termine «organismo» può essere confuso con «organismo di certificazione». Tuttavia, va chiarito che l'espressione «fornitore di programmi o sistemi di trattamento di dati personali» comprende anche i fornitori di prodotti (compresi i sistemi e i programmi per il trattamento dei dati [software] e i prodotti hardware), servizi e processi.

Per quanto riguarda il termine «sistemi» ai sensi dell'articolo 13 capoverso 1 nLPD, la nOCPD utilizza il termine «sistemi di gestione». Tuttavia, ciò non comporta alcuna modifica materiale rispetto al diritto vigente. Le nozioni di «organizzazione» e «procedura», contenute nella OCPD, sono mantenute come precisazione. Per il resto, la nOCPD utilizza al riguardo soltanto il termine «sistemi di gestione». Inoltre, poiché la nLPD ha introdotto la possibilità di certificare i servizi, sono precisati i requisiti per tali certificazioni. Per rispondere alle esigenze della prassi, la nOCPD prevede anche la possibilità di certificare i «processi». Questi non sono menzionati nell'articolo 13 capoverso 1 nLPD, ma la base giuridica sarà adeguata non appena possibile. Infine, questo approccio ha anche il vantaggio di essere conforme sia con la norma UNI CEI EN ISO/IEC 17021-1 (Valutazione della conformità – Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione – Parte 1: Requisiti) per la certificazione dei sistemi di gestione che con la norma UNI CEI EN ISO//IEC 17065 (Valutazione della conformità – Requisiti per organismi che certificano prodotti, processi e servizi) per prodotti, servizi e processi. In generale, gli oggetti della certificazione sono stati meglio delimitati. Sebbene non sia esplicitamente previsto dall'articolo 13 capoverso 1 nLPD, si tiene conto anche della possibilità di certificare il trattamento dei dati personali, in particolare nel contesto della certificazione di prodotti o servizi. Questo avvicina il sistema di certificazione svizzero al diritto europeo e pertanto le certificazioni svizzere relative al trattamento dei dati personali dovrebbero poter essere riconosciute dalle autorità europee.

Vengono introdotti ulteriori requisiti per il programma di certificazione (chiamato «programma di controllo» nella OCPD) di cui devono disporre gli organismi di certificazione, così come requisiti per la certificazione dei servizi e dei processi. Sono aggiornati i requisiti relativi alla certificazione dei sistemi di gestione e dei prodotti, nonché il periodo di validità della certificazione.

La nLPD introduce l'esenzione dall'obbligo di effettuare una valutazione d'impatto per i titolari privati del trattamento dei dati. Tale esenzione sostituisce la possibilità, prevista dal diritto vigente, di essere esentati dall'obbligo di dichiarare le proprie collezioni di dati (un concetto che non esiste più nella nLPD). Le pertinenti disposizioni sono state quindi adattate nella nOCPD.

Infine, con la menzione di un marchio di qualità inerente alla protezione dei dati nell'articolo 13 capoverso 2 nLPD, è stata ripresa la norma di delega già prevista dal diritto vigente. Analogamente alla OCPD, tuttavia, anche la nOCPD non contiene disposizioni in merito a tale marchio. Finora non si è ritenuto necessario introdurre un marchio generale inerente la protezione dei dati.

3 Commento della nuova ordinanza

3.1 Struttura dell'ordinanza

La nuova ordinanza mantiene la stessa struttura di quella in vigore: la prima sezione riguarda gli organismi di certificazione, la seconda l'ogetto e la procedura di certificazione, la terza le sanzioni e l'ultima le disposizioni finali.

3.2 Sezione 1: Organismi di certificazione

La prima sezione stabilisce il principio dell'accreditamento degli organismi di certificazione. L'articolo 1 specifica i requisiti che questi organismi devono soddisfare per essere accreditati; l'articolo 2 specifica quali istituzioni sono competenti per la procedura di accreditamento; infine, l'articolo 3 affronta la questione del riconoscimento degli organismi di certificazione stranieri in Svizzera.

Art. 1 Requisiti

L'articolo 1 nOCPD disciplina i requisiti che devono essere soddisfatti dagli organismi che effettuano la certificazione (organismi di certificazione). In primo luogo, questi organismi devono essere accreditati dal Servizio d'accreditamento svizzero (SAS). Come già previsto dalla OCPD, questi organismi devono essere accreditati separatamente in base agli oggetti che intendono certificare.

Il capoverso 2 è stato ampliato rispetto alla OCPD vigente per chiarire che l'accreditamento è richiesto non solo per la certificazione dell'organizzazione e delle procedure relative al trattamento dei dati (lett. a) e dei prodotti, ma anche per i servizi e i processi relativi al trattamento dei dati (lett. b).

Gli ambiti di cui alle lettere a e b sono oggetto di accreditamenti separati: l'accreditamento ai sensi della lettera a si basa sulle norme UNI CEI EN ISO/IEC 17021-1 (cfr. *sopra*) e UNI CEI EN ISO/IEC 27006 (Tecnologie informatiche – Tecniche di sicurezza – Requisiti per gli enti che forniscono servizi di audit e certificazione dei sistemi di gestione per la sicurezza delle informazioni) nonché su un corrispondente programma di certificazione. I requisiti della lettera b sono contemplati dalla norma UNI CEI EN ISO/IEC 17065 (cfr. *sopra*) e da un corrispondente programma di certificazione.

L'aggiunta alla lettera b dei servizi e dei processi è necessaria per adeguare l'ordinanza all'articolo 13 nLPD e più in generale alla prassi e alle varie norme ISO sopra menzionate. Il concetto di «servizi» è nuovo e significa, ad esempio, archiviazione di dati in un cloud o raccolta di dati per un concorso a premi. È stata aggiunta anche la nozione di «processo», per conformarsi alle varie norme ISO, in particolare alla UNI EN ISO 9001 (Sistemi di gestione per la qualità – Requisiti), che in genere distinguono tra il processo («entrata, uscita, attività») e la procedura («descrizione» di questi elementi).

Alla lettera a, una parentesi introduce la nozione di «sistemi di gestione». Ciò è in linea con la legge, che ora fa riferimento a «sistemi», «prodotti» e «servizi». Il concetto di «sistemi di gestione», più preciso, viene poi utilizzato in tutto il testo dell'ordinanza.

Il capoverso 3 viene modificato per concentrarsi esclusivamente sul programma di certificazione, i cui requisiti sono specificamente disciplinati negli articoli 5-7 nOCPD. Il termine «programma di certificazione» sostituisce «programma di controllo» per avere una terminologia corrispondente a quella utilizzata nelle norme ISO (p. es. UNI CEI EN ISO/IEC 17065, cfr. *sopra*). A differenza della OCPD, i requisiti materiali per il programma di certificazione sono ora inclusi nel nuovo articolo 5, di modo che tutti i requisiti per il programma di certificazione siano riuniti in un unico articolo.

Il contenuto del capoverso 4 OCPD è ora incorporato nel capoverso 3 nOCPD. Gli articoli menzionati sono adattati alla numerazione modificata della nOCPD. Il riferimento all'ordinanza del 17 giugno 1996[8] sul sistema svizzero di accreditamento e la designazione di laboratori di prova e di organismi di valutazione della conformità, di registrazione e d'omologazione (OAccD) è ora introdotto anche nell'articolo 5.

Infine, il capoverso 5 OCPD, che tratta dei requisiti minimi concernenti la qualifica del personale addetto alla certificazione e rimanda all'allegato, viene rinumerato come capoverso 4. Rende inoltre normativo il fatto che gli organismi di certificazione devono dimostrare di avere personale che soddisfa tali criteri.

Art. 2 Procedura di accreditamento

Rispetto alla OCPD, è stata introdotta solo l'abbreviazione «IFPDT» (che si riferisce all'istituzione dell'Incaricato federale della protezione dei dati), in sostituzione del termine «Incaricato» (che ora si riferisce alla funzione dirigenziale dell'istituzione). In merito a questa modifica terminologica, si veda il numero 2.

Art. 3 Organismi di certificazione esteri

Il capoverso 1 stabilisce i requisiti che gli organismi di certificazione stranieri devono soddisfare per poter operare in Svizzera. Rispetto alla OCPD, la disposizione è stata riorganizzata in modo da disciplinare tutte le condizioni nella stessa disposizione. Oltre a dimostrare di essere in possesso di una qualifica equivalente, di soddisfare i requisiti del programma di certificazione e di avere sufficiente familiarità con la legislazione svizzera in materia di protezione dei dati, gli organismi di certificazione stranieri devono ora anche dimostrare di soddisfare i requisiti concernenti la qualifica del personale addetto alla certificazione.

Il capoverso 2, abbreviato rispetto alla OCPD in linea con le spiegazioni fornite per il capoverso 1, si concentra ora sul riconoscimento di organismi di certificazione stranieri da parte dell'IFPDT previa consultazione del Servizio di accreditamento svizzero.

Il capoverso 3 prevede che l'IFPDT possa limitare il riconoscimento nel tempo e subordinarlo a oneri. Il termine «condizioni», utilizzato nella OCPD, viene qui eliminato, poiché un riconoscimento può essere accompagnato solo da oneri. A differenza delle condizioni che devono essere soddisfatte per ottenere il riconoscimento, gli oneri sono imposti dopo il riconoscimento in modo che questo mantenga la sua validità giuridica.

Il capoverso 4, invece, prevede che l'IFPDT possa revocare il riconoscimento se le condizioni e gli oneri non sono più adempiti.

---

[8] RS **946.512**

3.3 Sezione 2: Oggetto e procedura di certificazione

All'inizio della sezione 2, in cui sono trattati in dettaglio le diverse certificazioni e i loro requisiti, vengono introdotti due nuovi articoli: l'articolo 4 riguarda l'oggetto della certificazione e l'articolo 5 i requisiti del programma di certificazione. Gli articoli 6-10 nOCPD riprendono gli articoli 4-8 OCPD con alcune modifiche.

Art. 4 Oggetto della certificazione

Questo nuovo articolo ha lo scopo di raccogliere in un'unica disposizione ciò che può essere certificato in termini di protezione dei dati. Si tratta dei sistemi di gestione, dei prodotti, dei servizi e dei processi relativi al trattamento dei dati (cpv. 1).

Questi diversi oggetti sono definiti in modo più dettagliato riprendendo la definizione di sistemi di gestione (cpv. 2) dall'articolo 4 capoverso 1 OCPD (con modifiche puramente formali).

La certificazione dei prodotti è disciplinata al capoverso 3 lettera a e corrisponde all'articolo 5 capoverso 1 OCPD. Si pensi in particolare ai browser, ai software per la gestione dei server, alle applicazioni per gestire siti web, ma anche ai sistemi di logistica basati su tecnologie RFID o GPS. Il capoverso 3 lettera b chiarisce che i servizi e i processi certificabili sono quelli che trattano principalmente dati personali o generano dati personali.

Art. 5 Requisiti per il programma di certificazione

L'articolo definisce i requisiti per il programma di certificazione. Come menzionato in precedenza (cfr. art. 1 cpv. 3), l'espressione «programma di controllo» è sostituita da «programma di certificazione» e i requisiti di cui all'articolo 1 capoverso 3 lettere a e b OCPD sono spostati nel capoverso 1 di questo nuovo articolo. La formulazione è leggermente modificata senza cambiamenti materiali (p. es. stralcio della nozione di «prova» poiché è sufficiente «perizia»).

Il nuovo articolo integra i requisiti vigenti elencando al capoverso 2 alcuni aspetti di cui va necessariamente tenuto conto nella determinazione del programma di certificazione. Si tratta in particolare di tre punti: in primo luogo, i dati personali trattati (ossia l'ambito materiale); in secondo luogo, l'infrastruttura elettronica utilizzata per il trattamento dei dati personali (ossia i sistemi tecnici, come software e hardware); infine, le misure organizzative relative al trattamento dei dati personali. Tutti e tre gli aspetti sono rilevanti per la progettazione di criteri e procedure di certificazione. La misura in cui vengono presi in considerazione può variare a seconda dello scopo della certificazione.

Secondo il capoverso 3, il programma di certificazione deve ora dimostrare che i criteri di perizia sono conformi a tutti i principi della protezione dei dati definiti nell'articolo 6 LPD. Ciò significa che quando queste misure (criteri di perizia, procedure, ecc.) vengono messe in atto, devono essere presi in considerazione i principi del diritto in materia di protezione dei dati, come la legittimità, la proporzionalità e la finalità del trattamento o l'accuratezza dei dati.

Infine, come già menzionato, il capoverso 4 riprende l'articolo 1 capoverso 4 OCPD e fa riferimento ai requisiti di base stabiliti dalle norme ISO elencate nell'allegato 2 OAccD. Questo capoverso è completato per chiarire che l'allegato 2 OAccD non è esaustivo e che sono applicabili altre norme tecniche. Per l'accreditamento di prodotti, servizi e processi basati sulla norma ISO/IEC 17065 (cfr. *sopra*) sono previsti programmi di certificazione per soddisfare i requisiti. Questi programmi possono basarsi sulle norme internazionali UNI CEI EN ISO/IEC 17067 (Valutazione della conformità – Elementi fondamentali della certificazione di prodotto e

linee guida per gli schemi di certificazione di prodotto) UNI CEI ISO/IEC TR 17028 (Valutazione della conformità - Linee guida ed esempi di uno schema di certificazione per servizi) e UNI CEI ISO/IEC TR 17032 (Valutazione della conformità - Linee guida ed esempi di uno schema di certificazione di processi). I programmi di certificazione sono emanati dall'IFPDT sotto forma di direttive.

Art. 6 Requisiti per la certificazione dei sistemi di gestione

L'articolo 6 riprende in larga misura l'articolo 4 OCPD. Il capoverso 1 corrisponde sostanzialmente all'articolo 4 capoverso 2 OCPD, con l'aggiunta alla lettera b della documentazione dei rischi. Inoltre, sono state apportate modifiche formali (p. es., l'uso dell'espressione «sistemi di gestione» o l'eliminazione della nozione di «prova», e la sostituzione di «perizia» con «valutazione» nel testo italiano). Il testo francese è stato adattato affinché la lettera a, che si riferiva alla «charte de protection des données», rimandi ora alla «politique en matière de protection des données» e corrisponda al testo tedesco e italiano vigente (Datenschutzpolitik / politica di protezione dei dati).

L'articolo 4 capoverso 3 OCPD, che specifica le norme tecniche a cui l'IFPDT deve fare riferimento nell'emanazione delle direttive, è stato incorporato nell'articolo 6 capoverso 2 nOCPD, con alcuni adeguamenti formali, e integrato con una lettera c che rimanda alla norma UNI CEI EN ISO/IEC 27701, Tecniche di sicurezza – Estensione a ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni in ambito privacy – Requisiti e linee guida.

L'articolo 4 capoverso 1 OCPD è stato incorporato nell'articolo 4 capoverso 2 nOCPD. Oltre a un adeguamento strutturale e terminologico, viene chiarito che la certificazione dei sistemi di gestione può riguardare l'intero sistema, parti dell'organizzazione o singole procedure specifiche. L'articolo 4 capoverso 4 OCPD non è più pertinente in seguito alla soppressione dell'articolo 11*a* capoverso 5 lettera f LPD (cfr. il commento all'art. 10).

Art. 7 Requisiti per la certificazione di prodotti, servizi e processi

L'articolo riprende in gran parte l'articolo 5 OCPD, ampliandone tuttavia il campo di applicazione materiale per includere non solo i prodotti, ma anche i servizi e i processi.

Il capoverso 1 si basa sull'articolo 5 capoverso 2 OCPD. La lettera a viene modificata per introdurre la nozione di tracciabilità che, in collegamento con quella di integrità, comprende il concetto di autenticità. Non è quindi più necessario menzionarlo esplicitamente. Non è ripreso nemmeno il riferimento al fatto che questi requisiti devono essere garantiti alla luce dello scopo di impiego del prodotto, in quanto sono comunque richiesti dalla protezione dei dati, indipendentemente dalle finalità del trattamento.

La lettera b subisce le stesse modifiche per quanto riguarda il campo di applicazione materiale, che comprende ora prodotti, servizi e processi. Inoltre, basandosi sul principio dell'economicità e della minimizzazione dei dati, ne è stata semplificata la formulazione, senza modifiche materiali: «generare» e «memorizzare» i dati rientrano nel concetto più ampio di «trattare» i dati, i due termini sono pertanto eliminati.

Anche la lettera c è semplificata. Il concetto di «riproducibilità» e la precisazione che si riferisce al trattamento «automatizzato» sono superflui. Il principio della trasparenza del trattamento è importante anche se il trattamento non dovesse essere automatizzato (cosa improbabile). L'importante è che l'utente sia in grado di riconoscere quali dati personali vengono trattati, come vengono trattati e a chi vengono comunicati. I requisiti saranno quindi definiti

in base alla cerchia di utenti a cui è destinato il prodotto, il servizio o il processo. Saranno quindi più alti per un prodotto, un servizio o un processo che riguarda un'ampia gamma di utenti rispetto a quelli che riguardano solo gli specialisti. Sebbene questa precisazione sia stata eliminata nella lettera c, occorre sottolineare che la perizia riguarda il trattamento effettuato nell'ambito della funzionalità di un prodotto, un servizio o un processo. Se il prodotto, il servizio o il processo è progettato in modo tale da poter essere utilizzato per scopi diversi, occorre verificare che non si possano aggirare o disattivare i meccanismi che garantiscono la trasparenza.

La lettera d è stata integrata con l'aggiunta che si deve tener conto in particolare dei diritti delle persone interessate.

Infine, il capoverso 2 prevede, come nella OCPD (art. 5 cpv. 3), che l'IFPDT emani direttive che stabiliscano ulteriori criteri di protezione dei dati che un prodotto, un servizio o un processo deve soddisfare nell'ambito della certificazione. Il termine «Incaricato» è sostituito da quella dell'IFPDT (per questa modifica terminologica cfr. n. 2). Tuttavia, l'elenco degli oggetti della certificazione contenuto nella OCPD è stato eliminato, poiché, in considerazione della rubrica dell'articolo, è superfluo.

Art. 8 Rilascio e validità della certificazione

L'articolo 8 capoverso 1 nOCPD riprende l'articolo 6 capoverso 1 OCPD in versione ridotta, ma senza modifiche materiali, ad eccezione del termine «processo». L'elenco degli oggetti della certificazione di cui all'articolo 1 capoverso 2 chiarisce che il regolamento si applica a tutti questi oggetti. Nell'ultima frase, il termine «condizioni» viene eliminato (cfr. il commento all'art. 3). Il fatto che la certificazione possa essere soggetta a oneri, consente a un fornitore di programmi o sistemi di trattamento dei dati personali, un titolare del trattamento o un responsabile del trattamento che voglia far accreditare un sistema di gestione, un prodotto, un servizio o un processo, di aggiornarsi entro un certo lasso di tempo.

Il capoverso 2 viene modificato affinché tutti gli oggetti che possono essere certificati abbiano lo stesso periodo di certificazione di tre anni. Il periodo di certificazione dei prodotti è ora uguale a quello degli altri oggetti. Questa modifica consente, tra le altre cose, di adeguarsi alla normativa europea. Come nella OCPD, ogni anno va verificato se le condizioni per la certificazione sono ancora soddisfatte. Il carattere «sommario» della verifica, come previsto dall'articolo 6 capoversi 2 e 3 OCPD, è stato eliminato poiché l'ampiezza della verifica dipende dall'oggetto certificato.

Art. 9 Riconoscimento di certificazioni estere

Non sono state apportate modifiche materiali all'articolo 9. Oltre ad alcune modifiche formali rispetto all'articolo 7 OCPD, il termine «Incaricato» è sostituito da «IFPDT» (cfr. n. 2).

Art. 10 Esenzione dall'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati

Secondo l'articolo 4 capoverso 4 OCPD un organismo di certificazione può essere esentato dall'obbligo di notificare le proprie collezioni di dati ai sensi dell'articolo 11*a* capoverso 5 lettera f LPD, a condizione che siano state certificate tutte le procedure di trattamento dei dati cui è destinata una collezione di dati. A seguito della revisione della legge, questa possibilità non esiste più. Secondo il nuovo diritto (art. 22 cpv. 5 nLPD), il titolare del trattamento può invece «rinunciare a una valutazione d'impatto se si avvale di un sistema, un prodotto o un ser-

vizio che dispone di una certificazione secondo l'articolo 13 per l'impiego previsto». L'articolo 4 capoverso 4 OCPD non è quindi più pertinente e viene soppresso. Di contro si procede a una modifica nell' articolo 10 nOCPD per adeguarlo all'articolo 22 caporverso 5 nLPD: il titolare privato del trattamento può rinunciare a una valutazione d'impatto sulla protezione dei dati conformemente all'articolo 22 capoverso 5 LPD soltanto se la certificazione include il trattamento per il quale deve essere effettuata la valutazione d'impatto (cfr. il messaggio concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati; FF *2017* 5939, in particolare 6050). In effetti, una certificazione non dovrebbe essere troppo generica e dovrebbe invece includere il trattamento per il quale il titolare del trattamento desidera essere esonerato dall'effettuare una valutazione d'impatto.

In questo contesto viene soppresso anche l'articolo 8 OCPD, che specifica le condizioni alle quali è possibile essere esonerati dall'obbligo di notificare le collezioni, ossia principalmente informando l'IFPDT della certificazione e fornendo i documenti necessari. Non si è ritenuto necessario reintrodurre l'obbligo di informare l'IFPDT nel caso dell'articolo 22 capoverso 5 nLPD, poiché i risultati della valutazione d'impatto non devono essergli comunicati. L'IFPDT avrebbe voluto che il titolare privato fosse obbligato a chiedere preventivamente il suo parere se da un'analisi risultassero rischi elevati per la personalità o i diritti fondamentali delle persone interessate. Tuttavia, ciò avrebbe significato reintrodurre per il titolare privato l'obbligo di informare l'IFPDT, contrariamente all'intenzione del Legislatore. Poiché la certificazione non deve essere comunicata all'IFPDT, i capoversi 2 e 3 dell'articolo 8 OCPD non sono più pertinenti. Anche la pubblicazione di un elenco di organizzazioni certificate non è considerata utile, poiché le organizzazioni certificate hanno interesse a informare direttamente su questo tema e quindi non hanno bisogno di essere elencate sul sito web dell'IFPDT.

3.4 Sezione 3: Sanzioni

Gli articoli 11 e 12 nOCPD riprendono in generale gli articoli 9 e 10 OCPD, con alcune singole modifiche.

Art. 11 Sospensione e revoca della certificazione

Il capoverso 1 viene modificato sotto due aspetti rispetto all'articolo 9 capoverso 1 OCPD. In primo luogo, viene eliminato il rimando interno, dal momento che è chiaro dal contesto che si tratta di una verifica ai sensi dell'articolo 8 capoverso 2. In secondo luogo, la lettera b viene leggermente riformulata, senza che ciò comporti alcuna modifica materiale.

Il termine «segnatamente», presente nell'articolo 9 capoverso 1 OCPD, è sostituito da «in particolare» poiché si tratta soltanto di un esempio e possono verificarsi anche altre situazioni. Ad esempio, la certificazione può essere sospesa o ritirata in caso di verifica speciale o spontanea di un prodotto difettoso, anche se i difetti non sono stati scoperti nel corso di una procedura formale di verifica annuale.

Il capoverso 2 subisce solo la modifica formale della sostituzione di «organismo certificato» con la terminologia dell'articolo 13 nLPD, ossia «il fornitore di programmi o sistemi di trattamento dei dati personali, il titolare del trattamento o il responsabile del trattamento certificati», il che permette di designare le persone che possono beneficiare di una certificazione (cfr. n. 2)

Il capoverso 3 è stato eliminato, in quanto l'IFPDT non è più tenuto a essere informato se la certificazione è stata concessa e a tenere un registro dei titolari privati del trattamento certificati che sono esenti dall'obbligo di redigere una valutazione d'impatto sulla protezione dei

dati. L'IFPDT avrebbe voluto che il titolare della certificazione fosse obbligato a informarlo della sospensione o della revoca della sospensione, nella misura in cui avrebbe dovuto chiedere una notifica preventiva se sussistevano ancora rischi elevati per la personalità o i diritti fondamentali dell'interessato (cfr. il commento all'art. 10).

Art. 12 Misure di sorveglianza dell'IFPDT: procedura

L'articolo riprende sostanzialmente l'articolo 10 OCPD. La rubrica è modificata per utilizzare il termine IFPDT invece di «Incaricato» (cfr. n. 2).

Il capoverso 1 subisce una modifica formale. La precisazione contenuta nella OCPD secondo cui le lacune vengono rilevate nel *contesto dell'attività di sorveglianza dell'IFPDT* viene eliminata in quanto non necessaria, dal momento che la verifica rientra in ogni caso nelle competenze dell'IFPDT ai sensi degli articoli 4 e 49-51 nLPD. Inoltre, come per l'articolo 11 capoverso 2, la terminologia è adeguata all'articolo 13 nLPD.

Il capoverso 2 viene modificato solo formalmente, in particolare per quanto riguarda il termine «Incaricato» e la terminologia adattata all'articolo 13 nLPD.

Anche il capoverso 3 subisce solo lievi modifiche redazionali. In particolare, la durata del periodo di 30 giorni per rimediare ai difetti viene nuovamente menzionata in modo esplicito per motivi di certezza giuridica.

Il capoverso 4 viene modificato per rinviare al pertinente articolo della nLPD (art. 51 cpv. 1), il che significa che i termini che qualificano l'azione dell'IFPDT devono essere modificati. Infatti, non può più «formulare una raccomandazione», ma può «ordinare una misura» nei confronti di un fornitore di programmi o sistemi di trattamento dei dati personali, un titolare del trattamento o un responsabile del trattamento certificati o dell'organismo di certificazione interessato. Inoltre, nell'ultima frase, non può più «raccomandare», ma può «ordinare» all'organismo di certificazione di sospendere o evocare la certificazione se quest'ultimo non ha sospeso o revocato a sua volta la certificazione nonostante il persistere della lacuna. In questo caso, dovrà informare il Servizio di accreditamento svizzero, come già previsto dalla OCPD.

3.5 Sezione 4: Disposizioni finali

L'articolo 13 disciplina l'abrogazione della OCPD e l'articolo 14 fissa la data di entrata in vigore della nOCPD.

3.6 Allegato

Il titolo, così come i numeri 1 e 2 dell'allegato, subiscono solo poche modifiche formali rispetto alla OCPD vigente e vengono chiariti alcuni punti.

1 Certificazione dei sistemi di gestione

Il titolo, la frase introduttiva e la frase finale sono adeguati alla terminologia della nOCPD (cfr. comento all'art. 1 cpv. 2 lett. a). Inoltre, la frase introduttiva, i testi dei trattini e la frase finale sono modificati nella misura in cui il requisito della prova che il personale che effettua le certificazioni adempie le condizioni è ora parte del testo dell'ordinanza (cfr. il commento all'art. 1 cpv. 5). Nella frase introduttiva, l'espressione «complessivamente», già utilizzata nella OCPD, deve essere intesa nel senso che l'intero team che esegue gli esami deve soddisfare tutte le qualifiche e non ogni singolo individuo, poiché difficilmente esistono specialisti che soddisfano tutti i requisiti.

Inoltre, il testo del primo trattino viene modificato solo formalmente («conoscenze in materia di…») per essere coerente con il testo del secondo trattino.

Nel testo del secondo trattino il termine «sicurezza informatica», ormai obsoleto, è sostituito da «sicurezza dell'informazione» (cfr. anche la nuova legge sulla sicurezza delle informazioni, LSIn; FF *2020* 8755).

Viene introdotto un nuovo terzo trattino in cui si specifica che il personale che certifica i sistemi di gestione, oltre ad avere conoscenze nel campo della protezione dei dati e della sicurezza delle informazioni, comprovate da un'attività pratica o da un diploma, deve anche essere aggiornato sugli sviluppi in questi campi, in particolare attraverso la formazione continua e il perfezionamento professionale.

Infine, l'ultimo trattino è riorganizzato e completato dalla menzione di due ulteriori norme ISO: UNI CEI EN ISO/IEC 17021-3 (Valutazione della conformità – Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione – Parte 3: Requisiti di competenza per le attività di audit e la certificazione di sistemi di gestione per la qualità) e UNI CEI EN ISO/IEC 27006 (cfr. *sopra*).

Si noti inoltre che il termine «settore» nell'ultima frase (che è modificata parzialmente soltanto in tedesco) si riferisce ai due «settori» menzionati nei primi due trattini, ossia la protezione dei dati e la sicurezza delle informazioni. Come nella OCPD, si specifica che è consentita la perizia dei sistemi di gestione da parte di un gruppo interdisciplinare.

2 Certificazione di prodotti, servizi e processi

Tutti gli adeguamenti apportati al numero 1 dell'allegato, relativo alla certificazione dei sistemi di gestione, valgono anche per questa seconda parte dell'allegato, relativa alla certificazione di prodotti, servizi e processi, ad eccezione dell'aggiunta, nell'ultimo trattino, di riferimenti al programma di certificazione, alle direttive dell'IFPDT e alle nuove norme ISO. Queste aggiunte sono necessarie perché la norma ISO UNI CEI EN ISO/IEC 17065 (cfr. *sopra*), già citata nella OCPD, non contiene tutti i requisiti necessari per la certificazione di prodotti, servizi e processi per quanto riguarda le conoscenze tecniche del personale che esegue le certificazioni. Per il resto, si rimanda per analogia alle spiegazioni fornite per il numero 1.