PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4983 di Venerdì 23 luglio 2021

GDPR e certificazione dei trattamenti di dati

Disponibili le Faq con i primi chiarimenti messe a punto da Garante privacy e Accredia

Che cos'è la certificazione a fini privacy? Quali garanzie fornisce l'accreditamento? Chi può rilasciare certificazioni sul trattamento dei dati e chi può richiederle? Un singolo prodotto, come un software per la gestione dei dati dei dipendenti, può essere certificato ai sensi del GDPR?

A queste e ad altre domande rispondono le FAQ pubblicate dal Garante per la protezione dei dati personali e da Accredia, l'ente unico nazionale di accreditamento degli organismi di certificazione (OdC). Queste prime FAQ, dedicate ad aspetti generali e a cui seguiranno altre più specifiche, sono state elaborate nell'ambito di una convenzione finalizzata allo scambio di informazioni riguardanti le attività di certificazione e accreditamento previste dal Regolamento Ue sul trattamento dei dati.

Il documento fornisce chiarimenti utili a tutti i titolari o responsabili del trattamento dei dati, sia del settore imprenditoriale che di quello della pubblica amministrazione, che desiderano ricorrere a una certificazione per dimostrare il loro impegno nel rispettare gli obblighi di protezione dei dati e la conformità dei trattamenti ai requisiti previsti dal GDPR.

Le FAQ sono consultabili sui siti internet del Garante per la privacy www.gpdp.it o di Accredia www.accredia.it. Nelle pagine dedicate è possibile scaricare anche un opuscolo in formato digitale, realizzato per renderne più agevole la consultazione e la stampa.

Che cos'è la certificazione?

La certificazione è una attestazione rilasciata da una parte terza (organismo di certificazione - OdC) relativa a un oggetto (prodotto, processo, servizio, persona o sistema) sottoposto a valutazione della conformità rispetto a requisiti contenuti in una norma tecnica (standard) o in un disciplinare specifico.
La certificazione si dice "accreditata" quando viene data dimostrazione, da parte dell'ente unico nazionale di accreditamento istituito ai sensi del Regolamento (CE) n. 765/2008, in Italia Accredia, della terzietà, competenza, imparzialità e adeguatezza dell'OdC.

Riferimenti normativi: ISO/IEC 17000:2020 - punti 7.6 e 7.7

Che cosa è l'accreditamento?

L'accreditamento è una forma indipendente e autorevole di attestazione dell'imparzialità, competenza e adeguatezza degli organismi di valutazione della conformità (organismi di certificazione, ispezione e verifica e laboratori di prova e taratura).

L'attività di accreditamento è disciplinata a livello europeo e internazionale, rispettivamente, dal Regolamento (CE) n. 765/2008 e dalla norma tecnica ISO/IEC 17011, e in Italia è svolta da Accredia, l'ente unico nazionale designato dal Governo.

Riferimenti normativi: art. 2 Regolamento (CE) n. 765/2008 ISO/IEC 17000:2020 - punto 7.7 { } ISO/IEC 17011:201

Quali sono i vantaggi della certificazione?

La certificazione consente all'azienda, all'ente o alla persona che si certifica di dimostrare al mercato, rispettivamente:

a) la capacità di strutturarsi e gestire le proprie risorse e i propri processi produttivi in modo tale da riconoscere e soddisfare i bisogni dei clienti, inclusi quelli relativi al rispetto dei requisiti cogenti, nonché l'impegno a migliorare continuativamente tale capacità (certificazione di sistemi di gestione);

b) la capacità di ottenere e mantenere la conformità dei prodotti realizzati o dei servizi erogati. A tal fine, il marchio della conformità può essere apposto sulla confezione del prodotto o altri supporti afferenti al servizio oggetto della certificazione (certificazione di prodotto, processo o servizio);

c) il possesso, e il mantenimento nel tempo, delle abilità, delle conoscenze e delle competenze (es. autonomia e responsabilità) richieste per lo svolgimento di determinate attività professionali (certificazione di persone). Tale certificazione è uno strumento primario alla base dei processi di costruzione della qualità e motiva il professionista ad acquisire, mantenere e migliorare con continuità, nel tempo, le competenze professionali.

Ottenere la certificazione attraverso un organismo accreditato da Accredia (c.d. certificazione accreditata) permette, inoltre, di:

? esibire sul mercato un'attestazione autorevole, di terza parte, accettata a livello internazionale in virtù degli Accordi di mutuo riconoscimento;

? soddisfare i requisiti di bandi di gara predisposti dalle stazioni appaltanti pubbliche e private;

? svolgere specifiche attività in settori cogenti e regolamentati gestiti dalla PA attraverso autorizzazioni, abilitazioni e notifiche.

Riferimenti normativi: "Expected outcomes for accredited certification to ISO management system standards such as ISO 9001 and ISO 14001", ISO, 2018 - ISO/IEC 17065:2012-Introduzione - ISO/IEC 17024:2012-Introduzione

Quali sono i vantaggi della certificazione ai sensi del GDPR?

Il Regolamento prevede e incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati personali allo scopo di dimostrare la conformità, al Regolamento Generale per la Protezione dei Dati Personali (GDPR), dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

La certificazione rappresenta uno strumento utile per i titolari e i responsabili del trattamento a dimostrare il rispetto degli obblighi, le garanzie sufficienti e la conformità ai requisiti di protezione dei dati.

Riferimenti normativi: considerando 77, 81 e 100 GDPR - artt. 24 (3), 25(3), 28(5), 32(3), 35(8), 42, 43, 46(2) e 83(2) GDPR

Chi sono i soggetti coinvolti nel processo di certificazione ai sensi del GDPR?

I soggetti di regola coinvolti nel processo di certificazione sono:

? l'azienda/l'ente che richiede la certificazione;

? l'organismo di certificazione (OdC) accreditato che rilascia i certificati sulla base dei risultati di verifiche, e vigila sulla corretta gestione dei certificati;

? l'ente di accreditamento che accredita gli enti di certificazione e controlla periodicamente il mantenimento dei requisiti previsti da parte di tali soggetti, tra cui l'imparzialità, competenza e adeguatezza.

Il Regolamento Generale per la Protezione dei Dati Personali (GDPR) richiede che l'OdC debba essere accreditato dall'autorità di controllo competente o dall'ente nazionale di accreditamento designato in virtù del Regolamento (CE) n. 765/2008 o da entrambi.

Il quadro legislativo vigente prevede che il ruolo di ente di accreditamento sia svolto da Accredia, quale ente unico nazionale di accreditamento istituito ai sensi del Regolamento (CE) n. 765/2008, fatto salvo il potere del Garante per la Protezione dei Dati Personali (GPDP) di assumere direttamente l'esercizio di tali funzioni con riferimento a una o più categorie di trattamenti.

La certificazione ai sensi del GDPR deve essere rilasciata in base a schemi di certificazione approvati dall'autorità di controllo competente.

Riferimenti normativi: artt. 43 (1), 42(5) GDPR

Cosa posso certificare in ambito protezione dati?

In base a quanto previsto dal Regolamento Generale per la Protezione dei Dati Personali (GDPR), e alla luce delle linee-guida 1/2018 dell'EDPB (European Data Protection Board) in materia, l'oggetto della certificazione è un trattamento di dati personali. Poiché la definizione di "trattamento" di dati personali è molto ampia, anche l'oggetto della certificazione può variare in misura considerevole e può comprendere una sola operazione di trattamento (es. la conservazione di dati personali) ovvero più operazioni di trattamento (es. raccolta, conservazione, messa a disposizione) svolte dal titolare o dal responsabile del trattamento.

Nella misura in cui uno o più trattamenti configurino un "servizio" o un "prodotto", la certificazione può avere come oggetto tale servizio o prodotto (es. il servizio di gestione del personale di un'azienda).

Una certificazione ai sensi del GDPR non può, tuttavia, riguardare un singolo prodotto in quanto tale (es. un software per la gestione dei dati dei dipendenti, a prescindere dal suo utilizzo concreto) bensì in quanto parte integrante di un trattamento di dati personali svolto da un titolare o responsabile (es. il trattamento dei dati dei dipendenti svolto dal datore di lavoro in quanto titolare attraverso il suddetto software, che quindi diviene oggetto della certificazione).

È essenziale (vedi linee guida 1/2018 dell'EDPB) che l'oggetto specifico della certificazione richiesta dal singolo titolare o responsabile sia indicato con chiarezza nel certificato rilasciato dall'organismo di certificazione (vedi FAQ n. 5).

Riferimenti normativi: artt. 4(2), 42(1) GDPR

Cosa è un sigillo europeo?

Un sigillo europeo per la protezione dei dati è uno schema di certificazione sviluppato per essere utilizzato in tutti gli Stati membri dell'Unione europea. A tal fine, viene preso in considerazione l'ambito di applicazione dei criteri dello schema di certificazione e, più in generale, l'idoneità dello stesso a fungere da certificazione comune europea.

In particolare, lo schema e i relativi criteri devono essere adattabili così da tenere conto, se del caso, delle diverse regolamentazioni settoriali nazionali, applicabili ai trattamenti di dati oggetto della certificazione.

Riferimenti normativi: art. 42(5) GDPR

Il Garante può rilasciare certificazioni secondo il GDPR?

I soggetti legittimati al rilascio della certificazione possono essere, oltre agli organismi di certificazione (OdC) accreditati, anche le Autorità di controllo competenti.

Sebbene il Regolamento Generale per la Protezione dei Dati Personali (GDPR) preveda questa possibilità, allo stato, il Garante per la Protezione dei Dati Personali (GPDP) non rilascia certificazioni. Una volta che Accredia avrà rilasciato l'accreditamento agli OdC ?sulla base dei requisiti di accreditamento stabiliti dal GPDP - saranno dunque questi ultimi i soggetti deputati a rilasciare le certificazioni della protezione dati ad aziende, enti o altri soggetti a vario titolo interessati che ne facciano richiesta in qualità di titolari o responsabili del trattamento.

Riferimenti normativi: artt. 42(5), 43 GDPR

Chi può richiedere una certificazione ai sensi del GDPR?

Qualsiasi ente o azienda, o comunque soggetto a vario titolo interessato, che operi in qualità di titolare e/o responsabile del trattamento di dati personali può richiedere una certificazione al fine di dimostrare la conformità dei trattamenti (o di parte di questi, vedi FAQ n. 6) ad alcune disposizioni o ad alcuni principi del Regolamento Generale per la Protezione dei Dati Personali (GDPR), o al GDPR nel suo insieme.

I titolari e/o responsabili del trattamento, infatti, possono aderire a meccanismi di certificazione al fine di dimostrare di aver improntato la propria attività ai principi del GDPR, e tale adesione può costituire un valido elemento di responsabilizzazione (c.d. accountability) (vedi FAQ n. 1).

Riferimenti normativi: artt. 4(1) nn. 7 e 8, 24, 42 GDPR

A chi devo rivolgermi per ottenere una certificazione ai sensi del GDPR?

Per ottenere una certificazione basata su uno schema di certificazione approvato dall'autorità di controllo italiana, il Garante per la Protezione dei Dati Personali (GPDP), occorre rivolgersi agli organismi di certificazione (OdC) accreditati da Accredia in base alla norma tecnica ISO/IEC 17065:2012 e ai requisiti aggiuntivi stabiliti dal GPDP (vedi FAQ n. 8).

Si ricorda che il quadro legislativo vigente prevede che il ruolo di ente di accreditamento sia svolto da Accredia, quale ente unico nazionale di accreditamento istituito ai sensi del Regolamento (CE) n. 765/2008, fatto salvo il potere del GPDP di assumere direttamente l'esercizio di tali funzioni con riferimento a una o più categorie di trattamenti (vedi FAQ n. 5).

Riferimenti normativi: art. 2-septiesdecies D.Lgs. 196/2003 - artt. 42(5), 43(1)(b), 43(3) GDPR - Provvedimento n. 148 del 29 luglio 2020

La certificazione ai sensi del GDPR può essere sospesa/revocata e perché?

Qualora si rilevi una non conformità (NC), rispetto ai requisiti di certificazione, come risultato della sorveglianza o per un qualsiasi altro motivo, l'organismo di certificazione (OdC) deve esaminare la NC e decidere le azioni appropriate, che possono consistere nel:

? mantenimento della certificazione sotto condizioni specificate dall'OdC, in primo luogo: la valutazione del rischio relativo alla NC, le azioni appropriate immediate per il contenimento degli effetti, l'analisi della causa radice e la pianificazione e applicazione delle azioni definite. L'OdC può anche prevedere provvedimenti aggiuntivi (per esempio la sorveglianza incrementata);

? sospensione della certificazione in attesa di azioni correttive da parte dell'organizzazione certificata;

? revoca della certificazione o riduzione del campo di applicazione della certificazione, quando l'organizzazione certificata non ottemperi alla pianificazione delle azioni necessarie a ripristinare la conformità dei trattamenti o non sussistano più le conformità dei trattamenti di dati personali ai criteri dello schema di certificazione dei trattamenti stessi e questi siano in essere e non siano previste le azioni necessarie e immediate conseguenti. La certificazione è quindi revocata, se del caso, dallo stesso OdC che l'ha rilasciata, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Anche il Garante per la Protezione dei Dati Personali (GPDP) ha il potere di ingiungere a un OdC di revocare o non rilasciare una determinata certificazione, qualora non siano o non siano più soddisfatti i relativi requisiti.

Riferimenti normativi: artt. 42(7), 58(2), lettera (h) GDPR - UNI CEI EN ISO/IEC 17065:2012-punto 7.11.1

La certificazione secondo la norma tecnica UNI 11697 è una certificazione ai sensi del GDPR?

La norma UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza" e la Prassi di riferimento UNI/PdR 66:2019 "Raccomandazioni per la valutazione di conformità ai requisiti definiti dalla UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza" definiscono, rispettivamente, i requisiti di competenza e le regole per la valutazione della conformità di alcune figure professionali che operano nel settore del trattamento e della protezione dei dati personali: Responsabile della protezione dei dati, Manager Privacy, Specialista Privacy e Valutatore Privacy.

In quanto orientata alla certificazione di persone, tale certificazione non rientra tra quelle disciplinate dall'art. 42 del Regolamento Generale per la Protezione dei Dati Personali (GDPR), ma può rappresentare comunque, al pari di altri titoli, un valido strumento ai fini della dimostrazione del possesso, e del mantenimento, delle conoscenze, abilità e competenze da parte dei professionisti.

Inoltre, per alcune figure che svolgono un ruolo importante negli organismi di certificazione (il personale responsabile delle decisioni e il personale responsabile delle valutazioni) il possesso di una certificazione a fronte della norma UNI 11697 è un elemento idoneo a dimostrare i requisiti di competenza ed esperienza in materia.

Riferimenti normativi: Provvedimento n. 148 del 29 luglio 2020

Scarica il BOOKLET (pdf)

Fonte: Garante Privacy
