D.Lgs. 7 marzo 2005, n. 82

Codice dell'amministrazione digitale

G.U. 16 maggio 2005, n. 112, S.O.

Capo I - PRINCIPI GENERALI

Sezione I - Definizioni, finalità e ambito di applicazione

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:

0a) AgID: l'Agenzia per l'Italia digitale di cui all'articolo 19 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;

[a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;)]

[b) autenticazione del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;]

c) carta d'identità elettronica: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

[e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;]

[f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;]

[g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;]

[h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;]

[i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;]

i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

i-sexies) dati territoriali: i dati che attengono, direttamente o indirettamente, a una località o a un'area geografica specifica;

[l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;)]

l-bis) formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi; ([1])

l-ter) dati di tipo aperto: i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36; ([1])

[m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;]

[n) dato pubblico: il dato conoscibile da chiunque;]

n-bis) riutilizzo: uso del dato di cui all'articolo 2, comma 1, lettera e), del decreto legislativo 24 gennaio 2006, n. 36;

n-ter) domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Regolamento eIDAS",valido ai fini delle comunicazioni elettroniche aventi valore legale; ([2])

n-quater) servizio in rete o on-line: qualsiasi servizio di una amministrazione pubblica fruibile a distanza per via elettronica; ([3])

[o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;]

p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

[q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;]

[q-bis) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;]

[r) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;]

s) firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici; ([4])

[t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;]

[u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;]

u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;

[u-ter) identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;]

u-quater) identità digitale: la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64;

v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

[z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;)]

aa) titolare di firma elettronica: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione nonché alle applicazioni per la sua apposizione della firma elettronica; ([5])

[bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;]

cc) titolare del dato: uno dei soggetti di cui all'articolo 2, comma 2, che ha originariamente formato per uso proprio o commissionato ad altro soggetto il documento che rappresenta il dato, o che ne ha la disponibilità;
dd) interoperabilità: caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;
ee) cooperazione applicativa: la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informatici dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi;
ff) Linee guida: le regole tecniche e di indirizzo adottate secondo il procedimento di cui all'articolo 71 ([6]).
1-bis. Ai fini del presente Codice, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS.
1-ter. Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS. ([7])

(1) Lettera inserita dall' art. 1, comma 1, lett. a), n. 1), D.Lgs. 13 dicembre 2017, n. 217.
(2) Lettera, da ultimo, sostituita dall' art. 1, comma 1, lett. a), n. 2), D.Lgs. 13 dicembre 2017, n. 217.
(3) Lettera inserita dall' art. 1, comma 1, lett. a), n. 3), D.Lgs. 13 dicembre 2017, n. 217.
(4) La presente lettera è stata così modificata dall' art. 1, comma 1, lett. a), n. 4), D.Lgs. 13 dicembre 2017, n. 217.
(5) Lettera così modificata dall' art. 1, comma 1, lett. a), n. 5), D.Lgs. 13 dicembre 2017, n. 217.
(6) Lettera aggiunta dall' art. 1, comma 1, lett. a), n. 6), D.Lgs. 13 dicembre 2017, n. 217.
(7) Comma così modificato dall' art. 1, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.

Art. 2. Finalità e ambito di applicazione
1. Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione.
2. Le disposizioni del presente Codice si applicano:
a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b). ([1])
[2-bis. Tutte le disposizioni previste dal presente codice per le pubbliche amministrazioni si applicano, ove possibile tecnicamente e a condizione che non si producano nuovi o maggiori oneri per la finanza pubblica ovvero, direttamente o indirettamente, aumenti di costi a carico degli utenti, anche ai soggetti privati preposti all'esercizio di attività amministrative.]
3. Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto. ([2])
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici e la fruibilità delle informazioni digitali, si applicano anche agli organismi di diritto pubblico. ([3])
5. Le disposizioni del presente Codice si applicano nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196.
6. Le disposizioni del presente Codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile. Le disposizioni del presente Codice si applicano al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico. ([4])
6-bis. Ferma restando l'applicabilità delle disposizioni del presente decreto agli atti di liquidazione, rettifica, accertamento e di irrogazione delle sanzioni di natura tributaria, con decreto del Presidente del Consiglio dei ministri o del Ministro delegato, adottato su proposta del Ministro dell'economia e delle finanze, sono stabiliti le modalità e i termini di applicazione delle disposizioni del presente Codice alle attività e funzioni ispettive e di controllo fiscale. ([5])

(1) Comma così stato sostituito dall' art. 2, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(2) Comma sostituito dall' art. 2, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma così modificato dall' art. 2, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.
(4) Comma così modificato dall' art. 2, comma 1, lett. d), D.Lgs. 13 dicembre 2017, n. 217.
(5) Comma aggiunto dall' art. 2, comma 1, lett. e), D.Lgs. 13 dicembre 2017, n. 217.

Sezione II - Carta della cittadinanza digitale ([1])

Art. 3. Diritto all'uso delle tecnologie
1. Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute.
[1-bis. Il principio di cui al comma 1 si applica alle amministrazioni regionali e locali nei limiti delle risorse tecnologiche ed organizzative disponibili e nel rispetto della loro autonomia normativa.]
1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.
[1-quater. La gestione dei procedimenti amministrativi è attuata dai soggetti di cui all'articolo 2, comma 2, in modo da consentire, mediante strumenti informatici, la possibilità per il cittadino di verificare anche con mezzi telematici i termini previsti ed effettivi per lo specifico procedimento e il relativo stato di avanzamento, nonché di individuare l'ufficio e il funzionario responsabile del procedimento. ([3])]
[1-quinquies. Tutti i cittadini e le imprese hanno il diritto all'assegnazione di un'identità digitale attraverso la quale accedere e utilizzare i servizi erogati in rete dai soggetti di cui all'articolo 2, comma 2, alle condizioni di cui all'articolo 64. ([3])]
[1-sexies. Tutti gli iscritti all'Anagrafe nazionale della popolazione residente (ANPR) hanno il diritto di essere identificati dalle pubbliche amministrazioni tramite l'identità digitale di cui al comma 1-quinquies, nonché di inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse tramite un domicilio digitale, alle condizioni di cui all'articolo 3-bis. ([3])]

(1) Rubrica così sostituita dall' art. 3, comma 1, D.Lgs. 13 dicembre 2017, n. 217. Precedentemente la rubrica era la seguente: «Diritti dei cittadini e delle imprese».
(2) Il presente comma è stato così modificato dall' art. 4, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma abrogato dall' art. 4, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.

Art. 3-bis. Identità digitale e Domicilio digitale ([1])
01. Chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, tramite la propria identità digitale e anche attraverso il punto di accesso telematico di cui all'articolo 64-bis.
1. I soggetti di cui all'articolo 2, comma 2, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese hanno l'obbligo di dotarsi di un domicilio digitale iscritto nell'elenco di cui agli articoli 6-bis o 6-ter.

Art. 18. Piattaforma nazionale per la governance della trasformazione digitale (1)

1. È realizzata presso l'AgID una piattaforma per la consultazione pubblica e il confronto tra i portatori di interesse in relazione ai provvedimenti connessi all'attuazione dell'agenda digitale.
2. AgID identifica le caratteristiche tecnico-funzionali della piattaforma in maniera tale da garantire che la stessa sia accessibile ai portatori di interessi pubblici e privati e che sia idonea a raccogliere suggerimenti e proposte emendative in maniera trasparente, qualificata ed efficace.
3. Il Piano triennale per l'informatica nella pubblica amministrazione di cui all'articolo 14-bis è pubblicato sulla piattaforma e aggiornato di anno in anno.
4. Tutti i soggetti di cui all'articolo 2, comma 2, lettera a), possono pubblicare sulla piattaforma i provvedimenti che intendono adottare o, qualora si tratti di provvedimenti soggetti a modifiche e aggiornamenti periodici, già adottati, aventi ad oggetto l'attuazione dell'agenda digitale.
5. I soggetti di cui all'articolo 2, comma 2, lettera a), tengono conto di suggerimenti e proposte emendative raccolte attraverso la piattaforma.

(1) Il presente articolo è stato così sostituito dall' art. 18, comma 1, D.Lgs. 13 dicembre 2017, n. 217.

Art. 19. Banca dati per la legislazione in materia di pubblico impiego

[1. E' istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.
2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.
3. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 3, della legge 29 luglio 2003, n. 229.]

Capo II - DOCUMENTO INFORMATICO, FIRME ELETTRONICHE, SERVIZI FIDUCIARI E TRASFERIMENTI DI FONDI (1)

Sezione I - Documento informatico

Art. 20. Validità ed efficacia probatoria dei documenti informatici

[1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.]
1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida. (2)
1-ter. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria. (4)
1-quater. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico. (4)
[2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.]
3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica, sono stabilite con le Linee guida. (3)
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.
5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle Linee guida.

(1) Rubrica così sostituita dall' art. 19, comma 1, D.Lgs. 13 dicembre 2017, n. 217.
(2) Comma così sostituito dall' art. 20, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma modificato dall' art. 20, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.
(4) Comma inserito dall'art. 20, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.

Art. 21. Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale (1)

[1. Il documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. (3)]
[2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha altresì l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico. (3)]
2-bis. Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo. (2)
2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.
[3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.]
[4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.]
5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con

uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

(1) La presente rubrica è stata così sostituita dall' art. 21, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(2) Il presente comma è stato così modificato dall' art. 21, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma abrogato dall' art. 21, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.

Art. 22. Copie informatiche di documenti analogici

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se sono formati ai sensi dell'articolo 20, comma 1-bis, primo periodo. La loro esibizione e produzione sostituisce quella dell'originale. ([1])

1-bis. La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia. ([2])

2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le Linee guida ([3])

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle Linee guida hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

4. Le copie formate ai sensi dei commi 1, 1-bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5. ([4])

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

[6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.]

(1) Comma così modificato dall' art. 22, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(2) Comma inserito dall' art. 22, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma così modificato dall' art. 22, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.
(4) Comma così modificato dall' art. 22, comma 1, lett. d), D.Lgs. 13 dicembre 2017, n. 217.

Art. 23. Copie analogiche di documenti informatici

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

2-bis. Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le Linee guida, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I soggetti che procedono all'apposizione del contrassegno rendono disponibili gratuitamente sul proprio sito Internet istituzionale idonee soluzioni per la verifica del contrassegno medesimo. ([1])

(1) Comma così modificato dall' art. 23, comma 1, D.Lgs. 13 dicembre 2017, n. 217.

Art. 23-bis. Duplicati e copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle Linee guida

2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti Linee guida, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Art. 23-ter. Documenti amministrativi informatici

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

1-bis. La copia su supporto informatico di documenti formati dalle pubbliche amministrazioni in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia. ([2])

[2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.]

3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle Linee guida; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.

4. In materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, le Linee guida sono definite anche sentito il Ministero dei beni e delle attività culturali e del turismo. ([1])

[5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.]

5-bis. I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4.

6. Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22, 23 e 23-bis.

(1) Comma sostituito dall' art. 24, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217.
(2) Comma inserito dall' art. 24, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.

Art. 23-quater. Riproduzioni informatiche
1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».

Sezione II - Firme elettroniche, certificati e prestatori di servizi fiduciari ([1])

Art. 24. Firma digitale
1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida ([3]), la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma. ([2])
4-bis. L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione, salvo che lo stato di sospensione sia stato annullato. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4-ter. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
a) il certificatore possiede i requisiti previsti dal regolamento eIDAS ed è qualificato in uno Stato membro
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui al medesimo regolamento;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

(1) Rubrica così sostituita dall' art. 25, comma 1, D.Lgs. 13 dicembre 2017, n. 217.
(2) Comma così modificato modificato dall' art. 26, comma 1, D.Lgs. 13 dicembre 2017, n. 217.

Art. 25. Firma autenticata
1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.
3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23.

Art. 26. Certificatori
[1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, qualora emettano certificati qualificati, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.]

Art. 27. Certificatori qualificati
[1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1, devono inoltre:
a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;
c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;
e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.
3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività a DigitPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.
4. DigitPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.]

Art. 28. Certificati di firma elettronica qualificata
[1. I certificati qualificati devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;
e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.]
2. In aggiunta alle informazioni previste nel Regolamento eIDAS nel certificato di firma elettronica qualificata può essere inserito il codice fiscale. Per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si può indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo univoco. ([4])
3. Il certificato di firma elettronica qualificata può contenere, ove richiesto dal titolare di firma elettronica o dal terzo interessato, le seguenti informazioni, se pertinenti e non eccedenti rispetto allo scopo per il quale il certificato è richiesto: ([1])
a) le qualifiche specifiche del titolare di firma elettronica, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza; ([2])

b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3;
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili;
c-bis) uno pseudonimo, qualificato come tale ([5]).
3-bis. Le informazioni di cui al comma 3 sono riconoscibili da parte dei terzi e chiaramente evidenziati nel certificato. Le informazioni di cui al comma 3 possono anche essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con le Linee guida sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali. ([3])
4. Il titolare di firma elettronica, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo. ([6])
4-bis. Il certificatore ha l'obbligo di conservare le informazioni di cui ai commi 3 e 4 per almeno venti anni decorrenti dalla scadenza del certificato di firma. ([7])

(1) Comma così modificato dall' art. 27, comma 1, lett. b), n. 1), D.Lgs. 13 dicembre 2017, n. 217.
(2) Lettera così modificata dall' art. 27, comma 1, lett. b), n. 2), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma così modificato dall' art. 27, comma 1, lett. c), nn. 1), 2) e 3), D.Lgs. 13 dicembre 2017, n. 217.
(4) Comma sostituito dall' art. 27, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(5) Lettera aggiunta dall' art. 27, comma 1, lett. b), n. 3), D.Lgs. 13 dicembre 2017, n. 217.
(6) Comma così modificato dall' art. 27, comma 1, lett. d), D.Lgs. 13 dicembre 2017, n. 217.

Art. 29. Qualificazione dei fornitori di servizi ([1])
1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida.
2. Ai fini della qualificazione, i soggetti di cui al comma 1 devono possedere i requisiti di cui all'articolo 24 del Regolamento (UE) 23 luglio 2014, n. 910/2014, disporre di requisiti di onorabilità, affidabilità, tecnologici e organizzativi compatibili con la disciplina europea, nonché di garanzie assicurative adeguate rispetto all'attività svolta. Con decreto del Presidente del Consiglio dei ministri, o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, sentita l'AgID, nel rispetto della disciplina europea, sono definiti i predetti requisiti in relazione alla specifica attività che i soggetti di cui al comma 1 intendono svolgere. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche.
[3. Fatto salvo quanto previsto dall'articolo 44-bis, comma 3, del presente decreto e dall'articolo 14, comma 3, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, il richiedente deve inoltre possedere i requisiti individuati con decreto del Presidente del Consiglio dei ministri da fissare in base ai seguenti criteri:
a) per quanto riguarda il capitale sociale, graduazione entro il limite massimo di cinque milioni di euro, in proporzione al livello di servizio offerto;
b) per quanto riguarda le garanzie assicurative, graduazione in modo da assicurarne l'adeguatezza in proporzione al livello di servizio offerto.]
4. La domanda di qualificazione si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità di AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
6. A seguito dell'accoglimento della domanda, AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto da AgID (276) stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
[7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.]
[8. Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo.]
9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse di AgID (276), senza nuovi o maggiori oneri per la finanza pubblica.

(1) Il presente articolo è stato così modificato dal D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

Art. 30. Responsabilità dei prestatori di servizi fiduciari qualificati, dei gestori di posta elettronica certificata, dei gestori dell'identità digitale e dei conservatori ([2])
1. I prestatori di servizi fiduciari qualificati e i gestori di posta elettronica certificata, iscritti nell'elenco di cui all'articolo 29, comma 6, nonché i gestori dell'identità digitale e i conservatori di documenti informatici, che cagionano danno ad altri nello svolgimento della loro attività, sono tenuti al risarcimento, se non provano di avere adottato tutte le misure idonee a evitare il danno. ([3])
[2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.]
3. Il prestatore di servizi di firma digitale o di altra firma elettronica qualificata non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti eventualmente posti dallo stesso ai sensi dell'articolo 28, comma 3, a condizione che limiti d'uso e di valore siano chiaramente riconoscibili secondo quanto previsto dall'articolo 28, comma 3bis. ([1])

(1) Comma così modificato dall' art. 29, comma 1, lett. c), nn. 1) e 2), D.Lgs. 13 dicembre 2017, n. 217.
(2) La presente rubrica è stata così modificata dall' art. 29, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma così modificato dall' art. 29, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217. Successivamente, il presente comma è stato così modificato dall' art. 29, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217 e dall' art. 25, comma 1, lett. c), D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120; per l'applicabilità di tale ultima disposizione vedi l'art. 25, comma 2, del medesimo D.L. n. 76/2020.

Art. 31. Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata
[1. DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.]

Art. 32. Obblighi del titolare di firma elettronica qualificata e del prestatore di servizi di firma elettronica qualificata ([1])
1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.
2. Il prestatore di servizi di firma elettronica qualificata è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
3. Il prestatore di servizi di firma elettronica qualificata che rilascia certificati qualificati deve comunque: ([2])
a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle Linee guida, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;
c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
d) attenersi alle Linee guida;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
[f) non rendersi depositario di dati per la creazione della firma del titolare]
g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare di firma elettronica qualificata o del terzo dal quale derivino i poteri del titolare di firma elettronica qualificata medesimo, di perdita del possesso o della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare di firma elettronica qualificata, di sospetti abusi o falsificazioni, secondo quanto previsto dalle Linee guida ([3])
h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
k) non copiare, né conservare, le chiavi private di firma del soggetto cui il prestatore di servizi di firma elettronica qualificata ha fornito il servizio di certificazione;
l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il prestatore di servizi di firma elettronica qualificata;
m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.
4. Il prestatore di servizi di firma elettronica qualificata è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il prestatore di servizi di firma elettronica qualificata raccoglie i dati personali direttamente dalla persona cui si riferiscono o, previo suo esplicito consenso, tramite il terzo, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

(1) La presente rubrica è stata così modificata dall' art. 30, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.
(2) Il presente comma è stato così modificato dall' art. 30, comma 1, lett. b), n. 1), D.Lgs. 13 dicembre 2017, n. 217.
(3) La presente lettera è stata così modificata dall' art. 30, comma 1, lett. b), n. 2), D.Lgs. 13 dicembre 2017, n. 217.

Art. 32-bis. Sanzioni per i prestatori di servizi fiduciari qualificati, per i gestori di posta elettronica certificata, per i gestori dell'identità digitale e per i conservatori
1. L'AgID può irrogare ai prestatori di servizi fiduciari qualificati, ai gestori di posta elettronica certificata, ai gestori dell'identità digitale e ai soggetti di cui all'articolo 34, comma 1-bis, lettera b), che abbiano violato gli obblighi del Regolamento eIDAS o del presente Codice relative alla prestazione dei predetti servizi, sanzioni amministrative in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza, per importi da un minimo di euro 40.000,00 a un massimo di euro 400.000,00, fermo restando il diritto al risarcimento del maggior danno. Le sanzioni per le violazioni commesse dai soggetti di cui all'articolo 34, comma 1-bis, lettera b), sono fissate nel minimo in euro 4.000,00 e nel massimo in euro 40.000,00. Le violazioni del presente Codice idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio si considerano gravi. AgID, laddove accerti tali gravi violazioni, dispone altresì la cancellazione del fornitore del servizio dall'elenco dei soggetti qualificati e il divieto di accreditamento o qualificazione per un periodo fino ad un massimo di due anni. Le sanzioni vengono irrogate dal direttore generale dell'AgID, sentito il Comitato di indirizzo. Si applica, in quanto compatibile, la disciplina della legge 24 novembre 1981, n. 689. ([1])
1bis. L'AgID irroga la sanzione amministrativa di cui al comma 1 e diffida i soggetti a conformare la propria condotta agli obblighi previsti dalla disciplina vigente. ([2])
2. Fatti salvi i casi di forza maggiore o di caso fortuito, qualora si verifichi un malfunzionamento nei servizi forniti dai soggetti di cui al comma 1 che determini l'interruzione del servizio, ovvero in caso di mancata o intempestiva comunicazione dello stesso disservizio a AgID o agli utenti, ai sensi dell'articolo 32, comma 3, lettera mbis), AgID, ferma restando l'irrogazione delle sanzioni amministrative, diffida altresì i soggetti di cui al comma 1 a ripristinare la regolarità del servizio o ad effettuare le comunicazioni previste. Se l'interruzione del servizio ovvero la mancata o intempestiva comunicazione sono reiterati nel corso di un biennio, successivamente alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico. ([3])
3. Nei casi di cui ai commi 1, 1bis e 2 può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione secondo la legislazione vigente in materia di pubblicità legale.
[4. Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto da DigitPA nell'esercizio delle attività di vigilanza di cui all'articolo 31 si applica la disposizione di cui al comma 2.]

(1) Comma così modificato dall' art. 31, comma 1, lett. a) e b), D.Lgs. 13 dicembre 2017, n. 217. Successivamente, il presente comma è stato così modificato dall' art. 31, comma 1, lett. a) e b), D.Lgs. 13 dicembre 2017, n. 217 e dall' art. 25, comma 1, lett. d), D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120; per l'applicabilità di tale ultima disposizione vedi l' art. 25, comma 2, del medesimo D.L. n. 76/2020.
(2) Comma così modificato dall' art. 31, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.
(3) Comma così sostituito dall' art. 31, comma 1, lett. d), D.Lgs. 13 dicembre 2017, n. 217.

Art. 33. Uso di pseudonimi ([1])
[1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno venti anni decorrenti dall'emissione del certificato stesso.]

(1) Articolo abrogato dall' art. 64, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.

Art. 34. Norme particolari per le pubbliche amministrazioni
1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di qualificarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati;
b) possono rivolgersi a prestatori di servizi di firma digitale o di altra firma elettronica qualificata, secondo la vigente normativa in materia di contratti pubblici ([1]).
1bis. Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:
a) all'interno della propria struttura organizzativa;

b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art. 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione. ([2])

[2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71. ([3])]

[3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.]

[4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.]

[5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.]

(1) Lettera così modificata dall' art. 32, comma 1, lett. a), D.Lgs. 13 dicembre 2017, n. 217.

(2) Comma inserito dall' art. 32, comma 1, lett. b), D.Lgs. 13 dicembre 2017, n. 217. Lettera così modificata dall' art. 25, comma 1, lett. e), D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120; per l'applicabilità di tale disposizione vedi l' art. 25, comma 2, del medesimo D.L. n. 76/2020.

(3) Comma abrogato dall' art. 32, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.

Art. 35. Dispositivi sicuri e procedure per la generazione della firma qualificata

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

a) sia riservata;

b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;

c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

1-bis. Fermo restando quanto previsto dal comma 1, i dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico soddisfano i requisiti di cui all'Allegato II del Regolamento eIDAS.

2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare di firma elettronica, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle Linee guida ([1])

3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.

4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5.

5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico prescritti dall'Allegato II del regolamento eIDAS è accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto. La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'Agenzia per l'Italia digitale in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica.

6. La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 30, comma 2, del Regolamento eIDAS. Ove previsto dall'organismo di cui al periodo precedente, la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'AgID in conformità alle linee guida di cui al comma 5.

(1) Comma così modificato dall' art. 33, comma 1, D.Lgs. 13 dicembre 2017, n. 217.

Art. 36. Revoca e sospensione dei certificati qualificati

1. Il certificato qualificato deve essere a cura del certificatore:

a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;

b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;

d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle Linee guida, per violazione delle regole tecniche ivi contenute. ([1])

3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

4. Le modalità di revoca o sospensione sono previste nelle Linee guida ([1]).

(1) Comma così modificato dall' art. 34, comma 1, D.Lgs. 13 dicembre 2017, n. 217.

Art. 37. Cessazione dell'attività

1. Il prestatore di servizi fiduciari qualificato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso a AgID e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.

2. Il prestatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un prestatore di servizi fiduciari qualificato sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.

3. Il prestatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.

4. AgID rende nota la data di cessazione dell'attività del prestatore di cui al comma 1 tramite l'elenco di cui all'articolo 29, comma 6.

4-bis. Qualora il prestatore di cui al comma 1 cessi la propria attività senza indicare, ai sensi del comma 2, un prestatore di servizi fiduciari qualificato sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso AgID che ne garantisce la conservazione e la disponibilità.

4-ter. Nel caso in cui il prestatore di cui al comma 1 non ottemperi agli obblighi previsti dal presente articolo, AgID intima al prestatore di ottemperarvi entro un termine non superiore a trenta giorni. In caso di mancata ottemperanza entro il suddetto termine, si applicano le sanzioni di cui all'articolo 32-bis; le sanzioni pecuniarie previste dal predetto articolo sono aumentate fino al doppio.