IfinSistemi
Conservatore Accreditato AgID

IfinConsulting

SETTEMBRE 2016

# IfinConsulting News

## IL NUOVO CODICE DELL'AMMINISTRAZIONE DIGITALE

È stato pubblicato nella Gazzetta ufficiale del 13 settembre 2016 il decreto legislativo n. 179 del 26 agosto 2016, dove sono riportate le modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.

Nei giorni scorsi il Ministro per le riforme costituzionali e per i rapporti con il Parlamento aveva aggiornato il Governo sullo stato di attuazione del programma. Dalle dichiarazioni fatte, si apprendeva che con le modifiche al decreto ci sarà un cambiamento sostanziale dei rapporti tra cittadini e pubblica amministrazione, poiché questi saranno affidati sia ad un'identità digitale, attraverso la quale la popolazione residente potrà interfacciarsi con la pubblica amministrazione per utilizzare i servizi erogati in rete da quest'ultima, sia al domicilio digitale (l'indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato di cui al Regolamento (UE) 23 luglio 2014 n. 910 «Regolamento eIDAS», che consenta la prova del momento di ricezione di una comunicazione tra i soggetti privati e pubblica amministrazione, che sia basato su standard o norme riconosciute nell'ambito dell'unione europea).

Tra le altre principali novità introdotte: lo SPID, l'identificativo con cui un cittadino si farà riconoscere dalla pubblica amministrazione; il domicilio digitale, che sarà l'indirizzo on line al quale potrà essere raggiunto dalle pubbliche amministrazioni, definito come "mezzo esclusivo di comunicazione e notifica da parte dei soggetti" regolati dal CAD (art.4 c. 1 lett. c) (ovvero tutte le amministrazioni dello Stato, le Regioni, le Province, i Comuni, le Comunità montane, i loro consorzi e associazioni, gli istituti e scuole di ogni ordine e grado, le istituzioni educative, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le università, gli Istituti autonomi case popolari, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale...); è stata mantenuta la norma dell'art. 43 per cui il cittadino non è più tenuto a conservare il documento informatico conservato per legge da PP.AA. e partecipate e può richiedere accesso; viene ribadita la necessità dell'esistenza dell' interoperabilità fra i sistemi della PA, le cui regole, secondo le linee guida europee, sono rimandate a regole tecniche di imminente attuazione; la reintroduzione del concetto di "documento informatico", che all'art. 1 viene definito «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

Oltre queste novità, il decreto prevede l'istituzione della figura del commissario dell'Agenda digitale, individuata nella persona di Diego Piacentini, vicepresidente di Amazon, che dovrà garantire l'avanzamento dei progetti dell'Agenda digitale italiana; inoltre potrà svolgere una funzione suppletiva nel caso in cui l'amministrazione sia inadempiente.

## SOMMARIO

L'incarico dura tre anni e la sua attività sarà aiutata con la realizzazione da parte di AgID di una banca dati degli obiettivi e degli indicatori delle performance delle amministrazioni pubbliche, che fungerà da strumento per monitorare l'avanzamento dei lavori, in modo da avere la situazione generale sotto controllo.

Infine **sono anche previste la responsabilità disciplinare per i dirigenti in caso di mancato invio dei dati, che sarà definita con l'approvazione di un decreto dove verranno definite sanzioni; la responsabilità in capo ai dirigenti delle amministrazioni che non applicheranno quanto previsto dal Codice** (cui si aggiunge, sempre per i dirigenti, l'obbligo della formazione continua sui temi del digitale e delle nuove tecnologie) e la sospensione dell'obbligo per le amministrazioni pubbliche di adeguare i propri sistemi di gestione informatica dei documenti (prevista inizialmente per lo scorso 12 agosto dall'articolo 17 del DPCM del 13 novembre 2014) fino all' approvazione di un nuovo decreto di aggiornamento e coordinamento delle regole tecniche. **Quest'ultimo provvedimento sarà adottato entro quattro mesi dalla data di entrata in vigore del decreto legislativo di modifica del CAD.**

## SPID IL SISTEMA PUBBLICO DI IDENTITA' DIGITALE


Il Sistema Pubblico per l'Identità Digitale promosso da AgID permetterà a cittadini e imprese di accedere con un unico login a tutti i servizi online di pubbliche amministrazioni e imprese aderenti. Questo sistema nasce per facilitare la diffusione di servizi online e facilitarne l'utilizzazione da parte di cittadini e imprese, attraverso un ambiente sicuro, efficace ed economico. Lo SPID prevede la partecipazione di numerosi attori: gestori dell'identità digitale (o Identity Provider); fornitori di servizi (o Service Provider); l'utente stesso; l'Agenzia per l'Italia Digitale; gli *Attribute provider ( i gestori di attributi qualificati)* e le PA.

Le pubbliche amministrazioni, in qualità di fornitori di servizi, devono aderire allo SPID entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale (art.14 DPCM 24 ottobre 2014-definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese). Il 21 dicembre 2015 i primi tre gestori di identità digitale si sono accreditati (Infocert, Poste italiane e TI Trust Technologies S.r.l), quindi per le PA tale scadenza è prevista entro il **21 dicembre 2017**. Oltre a tale scadenza, nel DPCM del 24 ottobre 2014 sono previsti numerosi obblighi, sia per i gestori dell'identità digitali sia per i fornitori di servizi, definiti nella convenzione per l'adesione al sistema pubblico per la gestione dell'identità digitale, cui si aggiungono quelli previsti per le PA, da cui si evince che l'amministrazione, a seguito dell'iscrizione nel Registro SPID, è obbligata:

- a comunicare ad AgID l'elenco dei servizi qualificati erogati in rete attivi;
- a comunicare ad AgID, per ciascuno dei servizi qualificati erogati in rete compresi nell'elenco, la lista degli attributi SPID necessari alla fruizione, i quali devono risultare pertinenti e non eccedenti in relazione alla tipologia e alle funzionalità offerte dal servizio;
- inviare ad AgID una sintetica nota che, ai sensi di quanto previsto dal regolamento AgID sulle modalità attuative, fornisca una motivazione in merito ai livelli di sicurezza adottati e agli attributi (identificativi, non identificativi e qualificati) richiesti per ciascuno dei servizi erogati;
- a porre in essere ogni attività strumentale all'adesione allo SPID e connessa al corretto accesso al Registro, nel rispetto delle modalità definite da AgID in conformità al Regolamento recante le regole tecniche;
- a rispettare quanto specificato nell'Appendice D2 del Regolamento sulle modalità attuative;
- a comunicare tempestivamente all'indirizzo protocollo@pec.agid.gov.it ogni malfunzionamento o incidente sulla sicurezza occorso al sistema di autenticazione, fermo restando l'obbligo per le pubbliche amministrazioni di comunicare - entro e non oltre 24 ore dall'avvenuta conoscenza dall'accaduto – al Garante per la protezione dei dati personali e ad AgID eventuali violazioni ed intrusioni nei dati personali dei soggetti per i quali chiede la verifica dell'identità digitale riguardante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche";
- a vincolarsi alla scrupolosa osservanza delle disposizioni contenute nel Decreto Legislativo 30 giugno 2003, n. 196;

- a registrare gli eventi relativi a richieste di accesso ai servizi (log) secondo quanto previsto nei regolamenti AgID; a garantire che agli eventi registrati (log) sia apposto un riferimento temporale che corrisponda alla scala di tempo UTC (IEN) di cui al decreto del Ministro dell'Industria del commercio ed artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo;
- a garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali secondo le disposizioni previste dal DPCM e dai Regolamenti attuativi AgID;
- ad assistere l'utente nella risoluzione di eventuali problematiche che si dovessero verificare nel corso dell'autenticazione (help desk di primo livello), facendosi carico, se necessario, di sentire il gestore delle identità digitali coinvolto nella transazione (help desk di secondo livello).

L'Amministrazione, inoltre, si impegna a collaborare con AgID nell'attività di monitoraggio e controllo e, in particolare, si obbliga:

- ad inviare ad AgID, in forma aggregata, i dati da questa richiesti, che possono esser utilizzati esclusivamente a fini statistici, che possono essere resi pubblici in forma aggregata. AgID, prima della pubblicazione, verifica che i dati resi pubblici siano effettivamente anonimi nel loro complesso;
- a dare immediata comunicazione ad AgID di ogni circostanza che possa avere influenza sull'esecuzione delle attività di cui alla presente Convenzione.

Attualmente, dai dati pubblicati sul sito AgID, le amministrazioni attive sono 3593; gli identity provider accreditati sono 3; i servizi disponibili tramite SPID ammontano a 3693; e le identità SPID erogate sono 90375.
Tra i numerosi servizi disponibili tramite SPID, si ricordano quelli dell'Agenzia delle Entrate (dichiarazione precompilata; le fatture e i corrispettivi); quelli previsti nelle università (immatricolazioni, bollettini, prenotazioni esami, certificati ecc.) di cui i primi esempi sono stati l'università La Sapienza e il Politecnico di Milano; mentre per quanto riguarda le amministrazioni pubbliche i servizi saranno molteplici (il pagamento della Tasi, il bollo auto, le prestazioni sanitarie, il fascicolo dell'Inps, il riscatto della laurea, la richiesta degli assegni familiari, la consultazione Cud, il saldo dei tributi regionali, al pagamento delle mensa scolastica e ticket sanitari via web ecc.). Una sola password e un solo username permetteranno reali servizi per tutti e miglioreranno i legami dei cittadini con la PA e con le imprese.

## LA TUTELA DEI DATI SENSIBILI E LA CONDANNA DELLA CORTE DEI CONTI PER ILLECITA DIFFUSIONE DI DATI SANITARI

Il Codice della Privacy all'art. 4 classifica i vari tipi di dati riguardanti l'individuo ed esprime un sistema di tutele, che sono connesse alla natura del dato e alla sua capacità di incidere nello stile di vita degli interessati.
Infatti, nel Codice i dati sono suddivisi in dati personali, sensibili e giudiziari; nello specifico i dati cd. personali identificano un individuo tramite degli elementi, quali nome, cognome, oppure anche un numero di identificazione personale (come il numero di matricola); mentre i dati sensibili permettono di conoscere *"(...) l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"* (DLgs. 196/2003 art.4 c.1 lett. d).
La delicatezza del trattamento di quest'ultimi è tale che ne viene riconosciuta una particolare tutela; lo stesso Codice della privacy ne vieta la diffusione al pubblico e proprio quei dati, idonei a divulgare lo stato di salute, vengono definiti generalmente sensibilissimi. Secondo quanto stabilito dal codice della Privacy, i dati sensibilissimi *tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili, anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità* (art.22 c.6). Il garante inoltre si è espresso in merito al trattamento dei dati sensibilissimi anche facendo ricorso alle Linee guida pubblicate con provvedimento il 15 maggio 2014, dove ha chiarito che è vietata la pubblicazione di qualsiasi informazione da cui si possono ottenere informazioni riguardo lo stato di salute del soggetto interessato.

Ciò detto, la corte di Cassazione ha di recente condannato la Corte dei Conti per aver illecitamente diffuso dei dati sanitari in una sentenza che interessava un soggetto privato, titolare dei dati, dopo che quest'ultimo aveva presentato ricorso in materia pensionistica alla Corte dei Conti, sezione giurisdizionale di Palermo.
Dopo aver comparato tra loro il diritto alla riservatezza del privato con il diritto generale e pubblico di conoscere il precedente giudiziario (rispettivamente art.22 e art.52 del Codice della Privacy), la Cassazione ha affermato che il divieto di diffusione di dati sensibili prevale sull'interesse alla pubblicazione dei provvedimenti giurisdizionali a scopo di informativa giuridica e non ammette eccezioni, aggiungendo inoltre che *"(…) l'oscuramento dei dati idonei a rivelare lo stato di salute non pregiudica la finalità di informazione giuridica, ma può risultare necessaria nella prospettiva di un bilanciamento dei diversi interessi per tutelare la sfera di riservatezza dei soggetti coinvolti"*. Da ultimo la Cassazione ha rimandato al tribunale di Palermo la valutazione dell'esistenza e la consistenza del danno recato al titolare dei dati e l'indicazione del soggetto responsabile.
Questa decisione fa capire come il trattamento della privacy sia un argomento sempre più delicato da trattare; per questo motivo la legislazione europea ha introdotto con l'art.39 del regolamento 2016/679 la figura del *Data Protection Officer*, figura di cui dovranno dotarsi tutte le amministrazioni pubbliche e le imprese che trattano dati sensibili o controllano sistematicamente gli interessati.

## I SERVIZI DI IFINCONSULTING

**Consulenza**
Consulenza normativa
Consulenza archivistica e archivistico-informatica
Redazione di documenti (atti di nomina del responsabile della conservazione e del responsabile del trattamento dei dati personali) di pareri e di contratti
Verifica della rispondenza alle prescrizioni normative (Audit)
Supporto per il conseguimento dell'accreditamento presso AgID

**Formazione**
Corsi sulla dematerializzazione (ambito privato, pubblico e settore clinico)
Corsi di formazione sul responsabile della conservazione
Corsi di aggiornamento normativo

**IFIN SISTEMI srl a socio unico**
**PADOVA . MILANO . ROMA**

PD. Via G. Medici 9/A 35138
Tel. 049.5001500
Fax 049.5001692
www.ifin.it
www.conservazionesostitutiva.it