diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

Le linee guida dell'AGID sulla formazione e la conservazione dei documenti informatici.

Autore: Muia' Pier Paolo
In: Diritto civile e commerciale

AGID: Linee guida sulla formazione, gestione e conservazione dei documenti informatici 2020

Premessa

I documenti digitali hanno assunto ormai un ruolo predominante nella formazione dei documenti aziendali e della pubblica amministrazione: per garantire maggiore efficienza e economicità dei processi aziendali e degli enti pubblici, infatti, l'uso della carta è stato ormai in gran parte sostituito dell'uso dei documenti informatici, formati attraverso strumenti telematici e analogamente conservati.

Da anni si è posto, quindi, il problema di disciplinare in maniera uniforme le modalità di formazione e di conservazione di tali documenti, in modo da garantirne soprattutto la integrità e la genuinità. A tal fine, già diversi anni fa è stato prima emanato il Codice dell'amministrazione digitale (c.d. CAD), che ha la funzione di disciplinare – fra le altre cose – anche la validità e l'efficacia dei documenti informatici della PA e successivamente l'Agenzia governativa per il digitale (c.d. AGID) ha adottato delle prime linee guida volte proprio a dare applicazione tecnica alle regole del CAD e stabilire le modalità di formazione, gestione e conservazione dei documenti informatici da parte delle PA, ma anche dei soggetti privati.

Nel 2020 l'AGID ha emanato delle nuove linee guida sul punto, le quali hanno proprio lo scopo di aggiornare le regole tecniche sulla formazione, protocollazione, gestione e conservazione dei documenti informatici in applicazione del Codice dell'amministrazione digitale nonché di creare un unico testo contenente tutte dette regole, accorpando le varie disposizioni che si sono stratificate nel tempo sull'argomento.

Le linee guida dell'AGID

Il primo aspetto da prendere in considerazione riguarda l'ambito soggettivo di applicazione delle linee guida.

Diritto & Diritti ISSN 1127-8579

Detto corpo normativo, infatti, è applicabile non solo alle pubbliche amministrazioni, ai gestori di servizi pubblici e alle società sottoposte a controllo pubblico, ma anche ai soggetti privati (ove non diversamente previsto dalla legge).

Per quanto attiene, invece, l'ambito oggettivo delle linee guida, esse contengono le regole tecniche necessarie all'applicazione degli articoli del CAD che disciplinano – fra le altre cose – la validità ed efficacia probatoria dei documenti informatici, la sottoscrizione con firma elettronica, le copie informatiche dei documenti analogici, le copie analogiche di documenti informatici e i duplicati e le copie informatiche di documenti informatici, la formazione dei documenti informatici e il relativo protocollo, il fascicolo informatico e la conservazione dei documenti e dei fascicoli informatici.

Alle linee guida, inoltre, sono allegati ben 6 documenti che costituiscono parte integrante delle stesse, di cui, fra gli altri: quello relativo ai formati di file utilizzabili per la formazione del documento informatico e quello sui metadati relativi a detti documenti.

Circa i file utilizzabili, gli allegati individuano i formati digitali che devono avere i documenti fra quelli che sono utilizzati dai vari software oggi conosciuti: quali, per esempio, .doc, .docx, .pdf ecc.

Circa i metadati, gli allegati individuano il set minimo di informazioni relative al file/documento che devono essere associate al file medesimo: quali, per esempio, l'Id, il soggetto produttore, la data, il titolo, l'oggetto ecc.

Per quanto concerne l'efficacia delle linee guida, viene previsto che le medesime abbiano carattere vincolante e assumano valenza generale nei confronti di tutti i consociati.

In considerazione di ciò, le linee guida si inseriscono all'interno della gerarchia delle fonti del nostro ordinamento alla pari di un atto regolamentare, avente natura tecnica, che, in quanto tali, possono dunque essere fatte valere dinanzi al giudice amministrativo qualora fossero violate.

Il documento oggetto di commento stabilisce, inoltre, dei principi generali che devono essere rispetti nella gestione dei documenti.

A tal proposito, viene previsto che la gestione del documento informatico si sostanzia in un processo articolato in tre diverse fasi: la formazione, la gestione e la conservazione del documento.

Durante la fase di formazione del documento, **il soggetto che lo forma deve perseguire obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza rispetto alle regole tecniche relative alla formazione del documento medesimo**, bilanciando tale esigenza con i bisogni pratici che il soggetto ha nello svolgimento del proprio lavoro quotidiano.

Il sistema per gestire il documento informatico può anche essere affidato a soggetti terzi

Diritto & Diritti ISSN 1127-8579

rispetto a colui il quale ha l'obbligo di gestire il documento, ma in ogni caso deve essere regolamentato da specifiche procedure e strumenti informatici che possano disciplinare qualsiasi evento che possa in qualche in modo coinvolgere la vita del documento stesso, in modo da garantire l'efficienza e la sicurezza del sistema medesimo. Inoltre, **il sistema di gestione deve garantire che il documento venga tenuto nel rispetto dei principi generali in materia di trattamento dei dati personali**. Inoltre, viene previsto che durante la fase di gestione del documento possano essere necessarie delle attività di riversamento dei documenti dal formato originale ad un altro formato: si tratta, in altri termini, di casi in cui è necessario che il formato originale del documento venga modificato in altro formato per ragioni di gestione e/o conservazione (es. il formato doc. viene trasformato in un formato .pdf). In tali casi, le linee guida stabiliscono che il riversamento possa essere fatto più volte e in diversi momenti durante la gestione del documento.

Infine, il processo si conclude con **il trasferimento del documento informatico all'interno di un sistema di conservazione, che deve essere realizzato nel rispetto di quanto viene previsto in proposito dal CAD e dalle linee guida medesime e deve essere appositamente dedicato a tale funzione**.

Per quanto concerne gli obblighi di pubblicazione degli atti e dei documenti amministrativi ai fini di dare loro effetto di pubblicità legale, infine, le linee guida precisano che dette pubblicazioni devono avvenire sui siti web istituzionali dell'Ente pubblico e che il procedimento deve garantire che il documento informatico pubblicato sia conforme all'originale e rimanga tale nel tempo.

La formazione del documento informatico.

Il primo aspetto di cui si occupano le linee guida, come detto, riguarda la formazione del documento informatico, individuando le modalità attraverso cui deve essere realizzato un documento informatico per essere ritenuto valido.

In particolare, vengono previste quattro diverse modalità:

- **la creazione del documento attraverso dei software (es. office, openoffice ecc.) oppure dei servizi cloud (es. google documents) qualificati e che siano in grado di garantire che i documenti siano prodotti in dei formati che permettano la interoperabilità tra sistemi**;

- **la acquisizione di un documento informatico per via telematica oppure su un supporto informatico (quindi, per esempio, la ricezione tramite email oppure tramite download da una pen drive del documento) oppure la creazione di una copia di un documento analogico attraverso la scansione del medesimo (quindi la creazione di una copia per immagine) e la successiva acquisizione su un supporto informatico oppure ancora la diretta acquisizione**

Diritto & Diritti ISSN 1127-8579

della copia informatica di un documento analogico;

- la memorizzazione su un supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione di dati attraverso moduli o formulari resi disponibili all'utente;

- la generazione o il raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, provenienti da una o più banche dati, secondo una struttura logica predeterminata e memorizzata in forma statica.

In secondo luogo, **viene previsto che il documento informatico deve essere identificato in modo univoco e persistente**.

Per quanto riguarda la pubblica amministrazione, tale processo di identificazione viene indicato dalle stesse linee guida, le quali richiedono che **l'identificazione avvenga attraverso la protocollazione del documento e cioè la assegnazione di un numero univoco di protocollo a quel documento**. Nel caso di eventuali documenti non protocollati, invece, l'identificazione viene affidata alle funzioni del sistema di gestione informatica dei documenti.

Le linee guida prevedono, altresì, un sistema di identificazione diverso dal protocollo, che può essere utilizzato in alternativa al primo: in particolare, **l'identificazione univoca del documento può avvenire anche attraverso la associazione al documento di un'impronta crittografica basata su funzioni hash che siano ritenute crittograficamente sicure**.

Una volta che il documento informatico viene formato e identificato univocamente, le linee guida stabiliscono che lo stesso debba essere immodificabile.

Per raggiungere tale obiettivo, viene stabilito che **il documento venga memorizzato su un supporto informatico in formato digitale che non possa essere alterato nel suo accesso, gestione e conservazione**.

Le linee guida, quindi, stabiliscono per ognuno delle 4 tipologie di formazione di documenti informatici sopra descritte, le operazioni che devono essere compiute per garantire l'immodificabilità e l'integrità del documento informatico nonché la certezza del suo autore. A tale ultimo proposito, viene precisato che la certezza dell'autore si sostanzia nella capacità di associare in maniera certa e permanente al documento informatico il soggetto che lo ha sottoscritto.

Per quanto riguarda il documento informatico realizzato secondo la prima modalità, l'autore deve compiere una o piò delle seguenti operazioni:

Diritto & Diritti ISSN 1127-8579

- apporre sul documento una firma elettronica qualificata, una firma digitale o un sigillo elettronico qualificato o una firma elettronica avanzata;
- memorizzare il documento su sistemi di gestione documentale che adottino delle misure di sicurezza idonee secondo quanto previsto dalle medesime linee guida;
- trasferire il documento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato;
- versare il documento in un sistema di conservazione.

Per quanto riguarda il documento informatico realizzato secondo la seconda delle suddette modalità, l'autore deve compiere una o piò delle seguenti operazioni:

- apporre sul documento una firma elettronica qualificata, una firma digitale o un sigillo elettronico qualificato o una firma elettronica avanzata;
- memorizzare il documento su sistemi di gestione documentale che adottino delle misure di sicurezza idonee secondo quanto previsto dalle medesime linee guida;
- versare il documento in un sistema di conservazione.

Per quanto riguarda il documento informatico realizzato secondo la terza e la quarta delle suddette modalità, l'autore deve compiere una o piò delle seguenti operazioni:

- apporre sul documento una firma elettronica qualificata, una firma digitale o un sigillo elettronico qualificato o una firma elettronica avanzata;
- registrare l'esito dell'operazione di formazione del documento informatico nei file log del sistema;
- produrre una estrazione statica dei dati del documento e trasferire detta estrazione nel sistema di conservazione.

Le linee guida si occupano, poi, di disciplinare in maniera specifica la formazione delle **copie per immagine su supporto informatico di documenti analogici** (cioè la c.d. scansione di documenti

Diritto & Diritti ISSN 1127-8579

cartacei).

A tal proposito, viene previsto che la "copia scansionata" di un documento cartaceo e salvata su un supporto informatico (come l'hard disk o un cloud o un server di un internet service provider) deve essere formata attraverso dei processi e degli strumenti che siano idonei a garantire che il documento "scansionato" abbia lo stesso identico contenuto e forma del documento cartaceo.

Tale identicità deve essere riscontrabile attraverso il confronto tra i due documenti oppure **attraverso una apposita certificazione del processo di "scansione"**, per il caso in cui siano "scansionati" un numero elevato di documenti: in quest'ultimo caso si parla di una "certificazione di processo".

Tale certificazione di conformità deve essere effettuata da un pubblico ufficiale oppure, nel caso in cui non vi sia tale certificazione del pubblico ufficiale, **la conformità della copia "scansionata" rispetto all'originale cartaceo deve essere garantita attraverso l'apposizione da parte del soggetto che ha effettuato il confronto tra i due documenti della propria firma digitale** o della propria firma elettronica qualificata o della propria firma elettronica avanzata o di altro tipo di firma digitale valida di tale soggetto oppure del sigillo elettronico qualificato. Detta attestazione di conformità può anche essere inserita all'interno del documento informatico creato attraverso la "scansione" oppure può essere prodotta come un documento informatico separato che contiene un riferimento temporale e l'impronta di ogni copia per immagine effettuata. Infine, il documento informatico contenente la certificazione deve essere sottoscritto attraverso la firma digitale del notaio o del pubblico ufficiale a ciò autorizzato.

Le linee guida si occupano, poi, di disciplinare in maniera specifica la formazione dei **duplicati, delle copie e degli estratti informatici di documenti informatici**.

A tal proposito, viene previsto che **il duplicato informatico viene creato attraverso la memorizzazione della medesima evidenza informatica del documento informatico di cui si tratta**, all'interno del medesimo dispositivo digitale su cui quest'ultimo si trova oppure su un diverso dispositivo. **Il duplicato informatico formato nelle modalità di cui si è appena detto ha lo stesso valore giuridico del documento informatico da cui è estratto**.

Invece, l**a copia informatica di un documento informatico viene realizzata attraverso la formazione di un documento informatico che ha il medesimo contenuto del documento originale, ma che ha una diversa evidenza informatica rispetto all'originale**: è il caso, per esempio, in cui un file con estensione .doc viene trasformato in un file con estensione .pdf.

Infine, **l'estratto di un documento informatico si sostanzia nella formazione di un documento nel quale è contenuta una parte del contenuto del documento originale e che ha una diversa**

Diritto & Diritti ISSN 1127-8579

evidenza informatica rispetto a quest'ultimo.

Le copie informatiche e gli estratti informatici di un documento informatico originale hanno lo stesso valore giuridico dell'originale, a meno che non ne venga espressamente disconosciuta la conformità.

Anche in questo caso, **la validità del documento informatico che sia copia o estratto del documento originale informatico e la conformità tra i due documenti è consentita attraverso il confronto tra i due documenti** oppure **attraverso una apposita certificazione del processo di copia o di estrazione**.

Tale certificazione di conformità deve essere effettuata da un pubblico ufficiale oppure, nel caso in cui non vi sia tale certificazione del pubblico ufficiale, **la conformità della copia informatica o dell'estratto rispetto all'originale informatico deve essere garantita attraverso l'apposizione da parte del soggetto che ha effettuato il confronto tra i due documenti della propria firma digitale** o della propria firma elettronica qualificata o della propria firma elettronica avanzata o di altro tipo di firma digitale valida di tale soggetto oppure del sigillo elettronico qualificato. Detta attestazione di conformità può anche essere inserita all'interno del documento informatico contenente la copia o l'estratto oppure può essere prodotta come un documento informatico separato che contiene un riferimento temporale e l'impronta di ogni copia per immagine effettuata. Infine, il documento informatico contenente la certificazione deve essere sottoscritto attraverso la firma digitale del notaio o del pubblico ufficiale a ciò autorizzato.

Il documento amministrativo informatico.

Le linee guida prevedono anche una disciplina più specifica per il documento amministrativo informatico, prevedendo che a tale tipologia di documento informatico formato dalla pubblica amministrazione si applicano le stesse regole che valgono per l'ordinario documento informatico, fatte salve alcune peculiarità che vengono previste dalle stesse linee guida.

In particolare, le linee guida prevedono che l'immodificabilità e l'integrità di tale tipo di documento può essere realizzata anche attraverso la sua registrazione nel registro di protocollo dell'ente oppure negli ulteriori registri, repertori, albi, elenchi archivi o raccolte di dati che sono contenute nel sistema di gestione informatica dei documenti dell'ente.

Inoltre, viene previsto che al file informatico del documento amministrativo venga associato l'insieme dei metadati previsti per la registrazione di protocollo e quelli per la classificazione e la conservazione.

Per quanto riguarda le copie informatiche di documenti amministrativi analogici (la c.d. "scansione" o

Diritto & Diritti ISSN 1127-8579

copia per immagine del documento amministrativo cartaceo), viene previsto che all'interno di detta copia informatica sia inserita l'attestazione di conformità della copia "scansionata" medesima oppure che tale attestazione sia prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Infine, il documento informatico così composto e formato deve essere sottoscritto dal funzionario delegato tramite la firma digitale o la firma elettronica qualificata o avanzata.

La gestione del documento informatico.

La terza parte delle linee guida si occupa di disciplinare la fase della gestione del documento informatico.

A tal proposito, in primo luogo, viene disciplinata **la registrazione informatica dei documenti**, stabilendo le regole tecniche, i criteri e le specifiche delle informazioni che devono essere rispettati nel registrare i documenti informatici e la applicazione di un protocollo.

Ogni pubblica amministrazione deve nominare il responsabile della gestione documentale nonché il coordinatore della gestione documentale, che abbiano delle competenze giuridiche, informatiche e archivistiche. Inoltre, attraverso il responsabile della gestione documentale, deve adottare un manuale di gestione documentale (che raccoglie le modalità di formazione, gestione trasmissione, interscambio e accesso ai documenti amministrativi nonché le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico e contiene altresì il piano per la sicurezza informatica).

Le linee guida stabiliscono che **la registrazione informatica dei documenti viene effettuata attraverso la applicazione di dati elettronici allegati o connessi al documento informatico che servono per poterlo identificare in maniera univoca**. Una volta che viene compiuta la registrazione, il documento sarà identificato con l'insieme dei suddetti dati in formato elettronico.

La registrazione di protocollo, quindi, si sostanzia nell'insieme di metadati applicati ai documenti ricevuti o spediti dalla PA che vengono memorizzati nel registro di protocollo Il formato della registrazione. Tali dati vengono associati in forma permanente e non modificabile.

Per quanto concerne il formato e i tipi di informazioni minime da associare ai documenti registrati con il protocollo vengono definiti, relativamente alle Pubbliche amministrazioni, dall'allegato 6.

Inoltre, viene previsto che **il protocollo di registrazione debba assicurare che ogni operazione di "protocollazione" che viene compiuta sia tracciata, storicizzata e attribuita all'operatore che**

Diritto & Diritti ISSN 1127-8579

l'ha compiuta.

In particolare, deve essere assicurato che le informazioni circa l'oggetto, il mittente e il destinatario di un documento "protocollato" non possano essere modificate, né annullate, e che le uniche informazioni modificabili siano soltanto quelle relative all'assegnazione interna all'amministrazione e alla classificazione.

In ogni caso, tutte le operazioni di modifica o di annullamento siano storicizzate e sempre visibili.

Le linee guida si occupano altresì dei requisiti minimi di sicurezza che deve avere il sistema di protocollazione informatica.

A tal proposito, il sistema usato per la protocollazione deve essere sviluppato nel rispetto delle disposizioni previste in materia di cyber sicurezza previste dalle linee guida medesime e in particolare deve garantire:

1. l'univoca identificazione ed autenticazione degli utenti;

2. la garanzia di accesso alle risorse esclusivamente agli utenti che sono abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;

- il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Ogni giorno deve essere inviato al sistema di conservazione il registro giornaliero del protocollo relativo al giorno precedente, attraverso modalità di trasmissione che garantiscono l'immodificabilità del contenuto.

Infine, viene previsto che la classificazione dei documenti informatici venga effettuata per organizzare in maniera logica tutti i documenti amministrativi informatici che sono prodotti o ricevuti da un ente nello svolgimento delle sue funzioni.

La Pubblica amministrazione, inoltre, gestisce i flussi dei propri documenti attraverso la formazione dei fascicoli informatici, anche per quanto concerne documenti che non riguardano degli specifici procedimenti, oppure attraverso delle diverse aggregazioni informatiche che riuniscono documenti accorpati per criterio funzionale.

Diritto & Diritti ISSN 1127-8579

I formati di file

Per quanto concerne i formati di file che devono essere utilizzati per la creazione, la gestione e la conservazione dei documenti informatici, le linee guida rimandano all'allegato 2 delle medesime, che individuano i più comuni formati (come per esempio .doc, .docx, .pdf ecc.).

Anche le pubbliche amministrazioni, quindi, devono sempre garantire di poter gestire i formati indicati nel suddetto allegato.

Per il caso in cui una diversa norma giuridica stabilisca degli obblighi circa l'uso di specifici formati di file oppure dei vincoli particolari sui formati generici di cui all'allegato, le pubbliche amministrazioni devono accettare i documenti informatici solo se rispettano i formati specifici o contengono i particolari vincoli previsti dalla norma speciale.

Soltanto nel caso in cui sia possibile l'interoperabilità dei formati diversi da quelli "consentiti" (per come indicati dalle linee guida), è possibile utilizzare detti formati diversi per la creazione, la gestione e la conservazione dei documenti informatici (previa, comunque, valutazione che sia possibile la interoperabilità).

Dopo che sia stata effettuata detta valutazione e quindi sia ritenuta possibile l'interoperabilità, i soggetti privati e le pubbliche amministrazioni devono valutare se sia necessario o comunque opportuno riversare i file dal formato diverso in un altro formato "consentito" dalle linee guida oppure se mantenerli nel formato diverso.

Infine, i file debbono essere trasferiti al sistema di conservazione, secondo le tempistiche e i termini che vengono indicati dal piano di conservazione e della normativa vigente.

Le misure di sicurezza

Le linee guida stabiliscono che le pubbliche amministrazioni nella formazione, gestione e conservazione dei documenti informatici debbano applicare e rispettare le minime misure di sicurezza ICT che sono previste nella circolare n. 2/2017 emanata dall'AGID il 18 aprile 2017.

A tal proposito, viene previsto che il coordinatore della gestione documentale e il responsabile della conservazione debbano **predisporre un piano di sicurezza del sistema di gestione informatica dei**

Diritto & Diritti ISSN 1127-8579

documenti, all'interno del quale devono essere previste delle opportune misure tecniche e organizzative che siano in grado di garantire un livello di sicurezza adeguato rispetto al rischio di violazione della normativa in materia di protezione dei dati personali (tenendo conto anche della tipologia di dati trattati).

L'obbligo di adottare le suddette misure di sicurezza informatica grava sul titolare del trattamento o del responsabile del trattamento (qualora il trattamento sia effettuato dal responsabile per conto del titolare). Per l'individuazione di tali figure (cioè titolare e responsabile del trattamento), le linee guida rinviano alla disciplina di cui al GDPR (precisamente l'art. 28 del Regolamento UE 679/2016).

Il Piano di sicurezza deve contenere anche la descrizione della procedura da adottarsi in caso di violazione dei dati personali, secondo quanto previsto dalle apposite disposizioni del GDPR (cioè il c.d. data breach, di cui agli art. 33 e 34 del citato Regolamento UE).

Le linee guida prevedono, inoltre, che qualora la tenuta del sistema di gestione informatica dei documenti venga affidato a soggetti esterni, questi ultimi sono individuati come Responsabili del trattamento dati e pertanto devono dare delle garanzie sufficienti per poter attuare delle misure tecniche e organizzative adeguate per rispettare il GDPR e garantire la tutela dei dati personali dell'interessato e i suoi diritti in merito.

La conservazione del documento informatico

Le linee guida disciplinano il sistema di conservazione della Pubblica Amministrazione, stabilendo che il sistema di gestione informatica dei documenti deve trasferire al sistema di conservazione i fascicoli informatici chiusi e i fascicoli informatici e le serie non ancora chiusi, trasferendo i documenti informatici in essi contenuti in base a specifiche esigenze dell'ente.

La funzione del sistema di conservazione è quella di garantire la conservazione dei documenti informatici e dei documenti amministrativi informatici con i relativi metadati nonché delle aggregazioni documentali informatiche (cioè i fascicoli e le serie) e gli archivi informatici con i relativi metadati fino all'eventuale scarto di tali file informatici, **attraverso l'adozione di regole, procedure e tecnologie in modo tale da garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei medesimi**.

Inoltre, il sistema di conservazione deve avere funzionalità e requisiti tali da garantire che sia possibile accedere ai documenti conservati per tutto il periodo che viene previsto dal piano di conservazione del titolare e dalla normativa vigente oppure per un tempo superiore eventualmente concordato tra le parti.

Tale sistema di conservazione deve essere diverso e separato dal sistema di gestione dei documenti.

Diritto & Diritti ISSN 1127-8579

Infine, **gli allegati 2 e 4 delle linee guida individuano gli standard e le specifiche tecniche nonché i formati utilizzabili del sistema di conservazione**.

Per quanto riguarda la Pubblica amministrazione, il processo di conservazione dei documenti informatici può essere effettuato sia internamente che esternamente alla struttura organizzativa dell'ente medesimo. Mentre il manuale di conservazione redatto dal Titolare deve individuare i requisiti che deve avere il processo di conservazione nonché le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione.

Nel caso in cui l'Ente si affidi a soggetti esterni che forniscono il servizio di conservazione, tali soggetti devono avere dei requisiti elevati dal punto di vista della qualità e della sicurezza (nel rispetto dello standard ISO/IEC 27001), in modo da garantire l'autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti.

Le linee guida individuano anche i soggetti che rivestono ruoli nel processo di conservazione.

In particolare, vengono individuate le seguenti figure: il titolare dell'oggetto della conservazione; il produttore dei PdV (PdV è l'acronimo di "pacchetto di versamento" ed equivale a un deposito di dati digitali nel sistema di conservazione, da parte della persona addetta alla conservazione, insieme alla documentazione e ai metadati necessari all'archivio per facilitarne la conservazione e la consultazione); l'utente abilitato (che è il soggetto che può richiedere al sistema di conservazione l'accesso ai documenti che vi sono ivi contenuti, per poter acquisire relative le informazioni); il responsabile della conservazione e il conservatore.

Nella pubblica amministrazione **il ruolo di responsabile della conservazione** è affidato a un dirigente o funzionario interno individuato dal titolare dell'oggetto della conservazione, che abbia competenze giuridiche, informatiche e archivistiche. Tale figura, però, può essere affidata anche ad un soggetto esterno all'Ente, purchè abbia comunque le competenze di cui si è appena detto e purchè sia soggetto terzo rispetto al Conservatore. Il compito del responsabile della conservazione è quello di definire e attuare le politiche del sistema di conservazione e di gestirlo in autonomia sotto la sua responsabilità: in particolare, egli definisce le politiche di conservazione e i requisiti funzionali che deve avere il sistema di conservazione; gestisce il processo di conservazione e assicura la sua costante conformità alla legge; genera e sottoscrive il rapporto di versamento; effettua il monitoraggio della corretta funzionalità del sistema di conservazione; effettua la verifica periodica, almeno quinquennale, dell'integrità e della leggibilità dei documenti contenuti nel sistema di conservazione; provvede alla duplicazione o copia dei documenti informatici a seconda dell'evolversi del contesto tecnologico; predispone le misure necessarie per garantire la sicurezza fisica e logica del sistema di conservazione.

Le linee guida prevedono altresì la formazione e la adozione di un **manuale di conservazione**.

Si tratta di un documento informatico che si occupa di individuare in maniera specifica quale sia

Diritto & Diritti ISSN 1127-8579

l'organizzazione, i soggetti coinvolti e i ruoli che i medesimi svolgono nonché il modello di funzionamento, la descrizione del processo e delle architetture e infrastrutture utilizzate nonché le misure di sicurezza adottate e tutte le altre informazioni utili a gestire e verificare il funzionamento del sistema di conservazione.

In particolare, detto manuale deve individuare: i dati dei soggetti che nel tempo hanno assunto ruoli e responsabilità con riferimento al sistema di conservazione, indicando in maniera specifica anche le loro funzioni; le tipologie degli oggetti digitali che sono conservati, descrivendoli in maniera puntuale e indicando i formati di file gestiti nonché dei metadati che sono associati a ogni tipologia di documento; la puntuale descrizione del processo di conservazione; la puntuale descrizione del sistema di conservazione, indicando tutte le componenti tecnologiche, fisiche e logiche di cui è formato; le modalità con cui si svolge il processo di esibizione e di esportazione di un documento dal sistema di conservazione; la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e della integrità dei suoi archivi; la descrizione delle procedure da attuare per realizzare duplicati o copie dei documenti.

Le pubbliche amministrazioni devono altresì pubblicare il Manuale sul proprio sito istituzionale.

Per quanto concerne **il processo di conservazione**, il trasferimento del documento oggetto di conservazione all'interno del sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsto dal manuale di cui si è appena detto.

In particolare: in primo luogo, il sistema di conservazione acquisisce il PdV, il quale ultimo e gli oggetti digitali ivi contenuti vengono verificati per riscontrarne la coerenza con le modalità previste dal manuale di conservazione; in secondo luogo, viene generato un rapporto di versamento che viene identificato in maniera univoca dal sistema di conservazione e con un riferimento temporale e una o più impronte; infine, viene sottoscritto con la firma digitale o elettronica da parte del responsabile della conservazione o dal responsabile del servizio di conservazione il rapporto di versamento e del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente.

Le linee guida dettano anche alcune regole per quanto concerne **le infrastrutture utilizzate per il servizio di conservazione**.

A tal proposito, viene stabilito l'obbligo per il soggetto che fornisce il servizio di conservazione, di conservare e rendere disponibili nel territorio italiano le descrizioni del sistema di conservazione. Inoltre, viene stabilito che i conservatori debbono garantire alle amministrazioni di poter accedere in via elettronica in maniera effettiva e tempestiva a tutti i dati conservati, indipendentemente dal territorio dello Stato membro dell'Ue dove i medesimi sono conservati.

Viene, inoltre, previsto che tutte le componenti tecnologiche che vengono usate nei sistemi di conservazioni, siano esse componenti hardware o software, debbono essere segregate logicamente.

Diritto & Diritti ISSN 1127-8579

Infine, è previsto che i sistemi di conservazione siano realizzati nel rispetto dei principi di integrità e riservatezza dei dati nonché dei principi di privacy by design e privacy by default stabiliti dal GDPR.

Per quanto concerne **le modalità di esibizione dei documenti conservati**, le linee guida stabiliscono che il sistema di conservazione debba permettere ai soggetti autorizzati di poter accedere direttamente, anche da remoto, ai documenti che sono conservati all'interno del sistema e che debbano essere previste delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato rispetto al rischio e alle modalità di accesso in base alla tipologia di dati personali trattati e alle operazioni di trattamento che sono consentite al soggetto autorizzato all'accesso.

Per quanto concerne, infine, **le misure di sicurezza da applicare al sistema di conservazione**, le linee guida prevedono un richiamo alle misure minime di sicurezza ICT emanate dalla stessa AGID con la circolare del 18 aprile 2017 e stabiliscono che – a tal fine – il responsabile della conservazione debba predisporre il piano della sicurezza del sistema di gestione informatica dei documenti, individuando delle misure tecniche e organizzative che siano idonee a garantire un livello di sicurezza adeguato rispetto al rischio in materia di protezione dei dati personali nel rispetto di quanto previsto dal GDPR, anche tenendo conto delle tipologie di dati personali trattati.

La effettiva adozione delle misure di sicurezza individuate come idonee spetta al Titolare del trattamento o, in caso di trattamento effettuato per suo conto dal Responsabile del trattamento, spetta a quest'ultimo. Una volta adottate, le misure di sicurezza devono essere descritte all'interno del manuale di conservazione di cui si è sopra detto.

Il piano di sicurezza, infine, deve contenere anche la descrizione della procedura che deve essere adottata in caso in cui si verifichi un data breach ai sensi del GDPR.

Le linee guida si chiudono con una breve disciplina dello **scarto dei documenti informatici dap arte della Pubblica amministrazione**.

A tal proposito, viene previsto che, qualora la disciplina applicabile prevede che i documenti possono non essere più conservati, il Titolare del documento conservato individua e scarta i relativi pacchetti di archiviazione. In particolare, il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione che contiene i documenti che sono destinati allo scarto e lo comunica al responsabile della gestione documentale. Le proposte di scarto di pacchetti di archiviazione devono essere autorizzate del Ministero dell'interno e, dopo detta autorizzazione, il titolare procede alla distruzione dei pacchetti medesimi. Tale operazione di scarto deve essere tracciata sul sistema attraverso la creazione di metadati che descrivono le informazioni relative allo scarto e infine il Titolare comunica l'avvenuta distruzione agli organi preposti e al Ministero dell'interno.

Volume consigliato

Diritto & Diritti ISSN 1127-8579

Diritto & Diritti ISSN 1127-8579