5

AGID | Agenzia per l'Italia Digitale

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Sommario

CAPITOLO 1 Introduzione, strumenti di lettura e disposizioni comuni 6

1.1. Scopo del documento 6

1.2. Ambito soggettivo di applicazione 6

1.3. Ambito oggettivo di applicazione 7

1.4. Abrogazioni e norme transitorie 7

1.5. Principali riferimenti normativi 8

1.6. Linee guida AGID richiamate 9

1.7. Gruppo di lavoro 9

1.8. Allegati 10

1.9. Premessa metodologica 10

1.10. Natura vincolante delle Linee Guida 11

1.11. Principi generali della gestione documentale 11

CAPITOLO 2 Formazione dei documenti informatici 13

2.1. Documento informatico 13

2.1.1. Formazione del documento informatico 13

2.2. Copie per immagine su supporto informatico di documenti analogici 15

2.3. Duplicati, copie ed estratti informatici di documenti informatici 16

2.4. Il documento amministrativo informatico 17

2.4.1. Formazione del documento amministrativo informatico 17

2.5. Copie su supporto informatico di documenti amministrativi analogici 18

CAPITOLO 3 Gestione documentale 19

3.1. Registrazione informatica dei documenti 19

3.1.1. Ambito di applicazione 19

3.1.2. Adeguamento organizzativo e funzionale 19

3.1.3. Registrazione di protocollo e altre forme di registrazione 20

3.1.4. Formato della registrazione e della segnatura di protocollo 21
3.1.5. Annullamento delle informazioni registrate in forma immodificabile 22
3.1.6. Requisiti minimi di sicurezza dei sistemi di protocollo informatico 22
3.2. Classificazione dei documenti informatici 23
3.3. Aggregazioni documentali informatiche e archivio informatico 23
3.3.1. Fascicoli informatici 23
3.3.2. Altre aggregazioni documentali informatiche 24
3.3.3. Registri e repertori informatici 25
3.3.4. Archivio informatico 25
3.4. Compiti del responsabile della gestione documentale 25
3.5. Manuale di gestione documentale 26
3.6. Formati di file 29
3.7. Riversamento 29
3.8. Trasferimento al sistema di conservazione 29
3.9. Misure di sicurezza 30
CAPITOLO 4 Conservazione 32
4.1. Sistema di conservazione 32
4.2. Pacchetti informativi 33
4.3. Modelli organizzativi della conservazione 33
4.4. Ruoli e responsabilità 34
4.5. Responsabile della conservazione 34
4.6. Manuale di conservazione 36
4.7. Processo di conservazione 37
4.8. Infrastrutture 38
4.9. Modalità di esibizione 39
4.10. Misure di sicurezza 39

4.11. Selezione e scarto dei documenti informatici 40

Questo documento raccoglie il testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici.*

CAPITOLO 1 Introduzione, strumenti di lettura e disposizioni comuni

1.1. Scopo del documento

Lo scopo delle presenti linee guida è duplice:

a) aggiornare le attuali regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale[1] (da ora in avanti CAD), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;

b) incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

1.2. Ambito soggettivo di applicazione

Le presenti Linee Guida sono applicabili ai soggetti indicati nell'art. 2 commi 2 e 3 del CAD[2], fatti salvi gli specifici riferimenti alla Pubblica Amministrazione.

[1] L'art. 71, comma 1, del CAD prevede che "L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice".

[2] L'art. 2, comma 2, del CAD prevede che le disposizioni del 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)".
Il successivo comma 3 prevede che le disposizioni del 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".

1.3. Ambito oggettivo di applicazione

Le presenti Linee Guida contengono le regole tecniche sugli ambiti disciplinati dalle seguenti disposizioni del CAD:

- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 21, *Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale*
- Art. 22, commi 2 e 3, *Copie informatiche di documenti analogici*
- Art. 23, *Copie analogiche di documenti informatici*
- Art. 23-bis, *Duplicati e copie informatiche di documenti informatici*
- Art. 23-ter, *Documenti amministrativi informatici*
- Art. 23-quater, *Riproduzioni informatiche*
- Art. 34, *Norme particolari per le Pubbliche Amministrazioni*
- Art. 40, *Formazione di documenti informatici*
- Art. 40-bis, *Protocollo informatico*
- Art. 41, *Procedimento e fascicolo informatico*
- Art. 42, *Dematerializzazione dei documenti delle Pubbliche Amministrazioni*
- Art. 43, *Conservazione ed esibizione dei documenti*
- Art. 44, *Requisiti per la conservazione dei documenti informatici*
- Art. 45, *Valore giuridico della trasmissione*
- Art. 46, *Dati particolari contenuti nei documenti trasmessi*
- Art. 47, *Trasmissione dei documenti tra le Pubbliche Amministrazioni*
- Art. 49, *Segretezza della corrispondenza trasmessa per via telematica*
- Art. 50, *Disponibilità dei dati delle Pubbliche Amministrazioni*
- Art. 51, *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni*
- Art. 64-bis, *Accesso telematico ai servizi della Pubblica Amministrazione*
- Art. 65, *Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica*

1.4. Abrogazioni e norme transitorie

Le presenti Linee Guida entrano in vigore il giorno successivo a quello della loro pubblicazione sul sito istituzionale di AGID, di cui si darà notizia sulla Gazzetta Ufficiale.

Esse si applicano a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore.

A partire da questo termine i soggetti di cui all' art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle presenti Linee Guida.

A partire dalla data di applicazione delle presenti Linee Guida, sono abrogati:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".

Per quanto concerne il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*;
- art. 9, *Formato della segnatura di protocollo*;
- art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
- art. 20, *Segnatura di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatura*.

Sempre a far data dalla data di applicazione delle presenti Linee guida, la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni" è abrogata e sostituita dall'allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati" del presente documento.

1.5. Principali riferimenti normativi

I principali riferimenti normativi presi in considerazione ai fini della redazione delle presenti Linee Guida sono i seguenti:

a) RD 1163/1911, *Regolamento per gli archivi di Stato*;
b) DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;
c) DPR 854/1975, *Attribuzioni del Ministero dell'interno in materia di documenti archivistici non ammessi alla libera consultabilità*;
d) Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
e) DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
f) DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
g) D.lgs 196/2003 *recante il Codice in materia di protezione dei dati personali*;
h) D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
i) Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;*
j) D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
k) D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
l) DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*;
m) DPCM 21 marzo 2013, *Individuazione di 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, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

n) Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;*

o) Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;*

p) Reg. UE 679/2016 (GDPR), *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;*

q) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;*

r) Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA;*

s) Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;*

t) Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;*

u) DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.*

1.6. Linee guida AGID richiamate

a) Linee guida del 15 aprile 2019 *dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;*

b) Linee guida del 6 giugno 2019 *contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.*

c) Linee guida del 09/01/2020 *sull'Accessibilità degli strumenti informatici.*

1.7. Gruppo di lavoro

Il presente documento è stato redatto dal Tavolo di lavoro dell'Agenzia per l'Italia Digitale, istituito con determinazione del Direttore Generale n. 137 del 2 maggio 2018. Al Tavolo di lavoro, coordinato da Patrizia Gentili, hanno partecipato Alessandra Antolini, Gaetano Bruno, Matteo Carabellese, Antonio Florio, Enrica Massella Ducci Teri, Guido Pera, Vincenzo Travascio, Cristina Valiante. A titolo di esperti hanno partecipato inoltre Walter Arrighetti, Pietro Falletta Giacomo Massi e Luigi Avena, sentito anche il MIBACT come da art. 23 ter comma 4 del CAD[3].

[3] L'art. 23 ter comma 4 del CAD prevede che "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".

1.8. Allegati

Costituiscono parte integrante delle presenti Linee Guida i seguenti allegati:

1. Glossario dei termini e degli acronimi
2. Formati di file e riversamento
3. Certificazione di processo
4. Standard e specifiche tecniche
5. Metadati
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

1.9. Premessa metodologica

Le presenti linee guida costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nei DPCM del 2013 e 2014. Obiettivo generale del documento è che la gestione complessiva del documento informatico risulti semplificata attraverso una visione d'insieme che aggrega in un "corpo unico" materie prima disciplinate separatamente.

L'approccio utilizzato è di tipo olistico, ossia diretto a mettere in evidenza e a rappresentare le interdipendenze funzionali tra le varie fasi della gestione documentale dal momento della formazione fino alla selezione per lo scarto o la conservazione permanente.

La tecnica redazionale – stante la natura prescrittiva del testo - ha privilegiato uno stile chiaro e fruibile per il lettore, indipendentemente dalla natura pubblica o privata di quest'ultimo e dalle sue competenze in materia.

Considerata la velocità dell'innovazione, le linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di prevedere un testo "statico" che contenga la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli "allegati" è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione. Relativamente ai temi della trasmissione di contenuti digitali tra e con le pubbliche amministrazioni si assicura la conformità al Modello di interoperabilità definito da AgID e alle tecnologie introdotte dallo stesso.

1.10. Natura vincolante delle Linee Guida

Come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*.

Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD[4].

1.11. Principi generali della gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.

Dal punto di vista archivistico, si distinguono tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti

[4] L'art. 17 comma 1-quater del CAD prevede che "È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni".

informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano. Al tal fine, risulta decisivo avvalersi di un valido e completo manuale di gestione documentale, di workflow documentali e sistemi di Document & Content Management e di applicativi informatici, per la PA ai sensi degli articoli 68[5] e 69[6] del CAD, che si basino su elevati livelli di automazione ed interoperabilità in grado di operare nel web. In un contesto in continua trasformazione, il manuale di gestione documentale deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati. Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici devono essere sottoposti ad un costante lavoro di valutazione, monitoraggio, ri-progettazione e reingegnerizzazione. L'adozione del manuale di gestione documentale e del manuale di conservazione non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo come specificato ai paragrafi 3.5 e 4.7, al quale per la PA fa seguito l'ulteriore obbligo della loro pubblicazione sul sito istituzionale dell'ente.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione da realizzarsi in ottemperanza a quanto disposto dal CAD e dalle presenti Linee guida.

La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione.

Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati.

Nell'ambito della gestione documentale possono essere necessarie attività di riversamento dei documenti in altro formato diverso da quello originale, come specificato al paragrafo 3.7. Tale riversamento può avvenire più volte nella gestione del documento informatico e in diversi momenti per finalità gestionali o conservative.

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale o comunque derivanti dalla normativa in materia di trasparenza devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere i predetti obblighi è necessario che esso garantisca la conformità di quanto pubblicato all'originale, l'autorevolezza dell'ente emanatore e del sito web, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

---

[5] L'art. 68 del CAD prevede che "Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) software sviluppato per conto della pubblica amministrazione;
b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
c) software libero o a codice sorgente aperto;
d) software fruibile in modalità cloud computing;
e) software di tipo proprietario mediante ricorso a licenza d'uso;
f) software combinazione delle precedenti soluzioni".

[6] L'art. 69 del CAD prevede che "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali".

CAPITOLO 2 Formazione dei documenti informatici

2.1. Documento informatico

2.1.1. Formazione del documento informatico

Il contenuto del presente capitolo si applica, salvo ove diversamente specificato, ai soggetti di cui all'art. 2 commi 2 e 3 del CAD.

Il documento informatico è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione[7], l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

[7]Si fa riferimento ai soggetti di cui all'art. 2 comma 2, lettera a) del CAD.

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- il trasferimento a soggetti terzi attraverso 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 (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto al documento stesso.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" alle presenti linee guida. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali. Nel caso della Pubblica Amministrazione, tali politiche e procedure sono contenute nel manuale di gestione documentale di cui al paragrafo 3.5. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 2 "Formati di file e riversamento" alle presenti linee guida ove sono specificate, anche, le caratteristiche e i criteri di scelta del formato stesso.

2.2. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, 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.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD[8] nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD[9].

---

[8] L'art. 22 comma 4 del CAD prevede "Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta."

[9] L'art. 22 commi 4 e 5 del CAD prevedono "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 assolve-re gli obblighi

2.3. Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD[10] nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

---

di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.
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."

[10] Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, 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.

2.4. Il documento amministrativo informatico

2.4.1. Formazione del documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis[11], 40 -bis[12] e 65[13] del CAD.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici. Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA[14], nonché i metadati relativi alla

---

[11] L'art. 5-bis, comma 1, del CAD prevede che "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese".

[12] L'art. 40-bis del CAD prevede che "Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71".

[13] L'art. 65 del CAD disciplina "Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici".

[14] L'art. 53, comma 1, del TUDA prevede che "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile; b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile; c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

classificazione, ai sensi dell'articolo 56 del TUDA[15], e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle presenti Linee guida.

Sarà cura dell'Amministrazione individuare ulteriori metadati (ad es. metadati relativi al Registro giornaliero di protocollo ecc.) da associare a particolari tipologie di documenti amministrativi informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel manuale di gestione documentale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter comma 5-bis del CAD[16], i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

2.5. Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 2.2.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

[15] L'art. 56 del TUDA prevede che "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

[16] L'art. 23-ter comma 5-bis prevede che "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".

CAPITOLO 3 Gestione documentale

3.1. Registrazione informatica dei documenti

3.1.1. Ambito di applicazione

Il presente capitolo individua le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, di cui agli articoli da 50 a 57 e da 61 a 66 del TUDA[17].

Il presente capitolo stabilisce inoltre le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo di cui agli articoli 40-bis, 41 e 47 del CAD[18].

3.1.2. Adeguamento organizzativo e funzionale

Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a:

A. individuare le aree organizzative omogenee (di seguito AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del TUDA[19];

B. nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

[17] Gli articoli da 50 a 57 e da 61 a 66 del TUDA sono compresi nel Capo IV "Sistemi di gestione informatica del documento".

[18] Gli articoli 40-bis, 41 e 47 del CAD disciplinano, rispettivamente, in materia di protocollo informatico, procedimento e fascicolo informatico, trasmissione dei documenti tra le pubbliche amministrazioni.

[19] L'art. 50, comma 4, del TUDA prevede che "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

C. per le amministrazioni con più AOO, nominare il coordinatore della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

D. adottare per ogni AOO il manuale di gestione documentale, su proposta del responsabile della gestione documentale oppure, ove nominato, dal coordinatore della gestione documentale.

Secondo quanto previsto dal CAD e dalle Linee guida AGID del 15 aprile 2019[20], l'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi, di seguito indicato con l'acronimo IPA, include, tra gli indirizzi telematici degli Enti ivi iscritti, il domicilio digitale da cui provengono, o sono inviate, comunicazioni, istanze, dichiarazioni e notifiche che formano oggetto di registrazione di protocollo.

3.1.3. Registrazione di protocollo e altre forme di registrazione

La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53 comma 5 del TUDA[21].

Al termine della registrazione, il documento è identificato da un insieme di dati in forma elettronica che può includere sin da questa fase la classificazione e si integra con il piano di organizzazione delle aggregazioni documentali, definito dal Responsabile della gestione documentale di cui al paragrafo 3.4, nell'ambito del manuale di gestione.

La Pubblica Amministrazione, al fine di dare attuazione alle disposizioni introdotte dal CAD stesso in materia di sistema di gestione informatica dei documenti realizza le funzionalità di gestione dell'archivio corrente, dell'archivio di deposito, dei flussi documentali, automatizzazione dei procedimenti amministrativi sulla base dei propri obiettivi di miglioramento dei servizi e di incremento dell'efficienza operativa, tenuto conto del rapporto costi e benefici, nel rispetto degli articoli 53 e 55 del TUDA[22] e dei requisiti del sistema di gestione informatica dei documenti e dei flussi documentali" definiti negli articoli 52, 65 e 67 del TUDA[23], applicando ove possibile i requisiti fissati per la registrazione di protocollo anche alle altre forme di registrazione informatica dei documenti, fatto salvo quanto disposto per esse da eventuali norme vigenti".

---

[20] Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

[21] L'art. 53, comma 5, del TUDA prevede che "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

[22] Gli articoli 53 e 55 del TUDA disciplinano, rispettivamente, in materia di registrazioni di protocollo e segnatura di protocollo.

[23] Gli articoli 52, 65 e 67 del TUDA disciplinano, rispettivamente, in materia di sistema di gestione informatica dei documenti, requisiti del sistema per la gestione dei flussi documentali e trasferimento dei documenti all'archivio di deposito.

3.1.4. Formato della registrazione e della segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA[24] e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa. In merito, l'articolo 53, comma 1, del TUDA indica le informazioni che caratterizzano il registro di protocollo[25], a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.

In merito l'articolo 55, comma 1, del TUDA individua le informazioni che caratterizzano la segnatura di protocollo[26].

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.

Gli "standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati" sono definiti nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati".

---

[24] L'art. 53, comma 5 del TUSA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

[25] L'art. 53, comma 1, del TUDA prevede che: "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:
a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) oggetto del documento, registrato in forma non modificabile;
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

[26] L'art. 55, comma 1, del TUDA prevede che: "La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:
a) il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4".

3.1.5. Annullamento delle informazioni registrate in forma immodificabile

Il protocollo informatico deve assicurare il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA[27];
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsti dall'art. 54, comma 2 del TUDA.

3.1.6. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID di cui al paragrafo 3.9 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

[27] L'art. 54, comma 2, del TUDA prevede che: "La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione".

3.2. Classificazione dei documenti informatici

La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi informatici prodotti o ricevuti da un ente nell'esercizio delle sue funzioni. L'attività di classificazione si avvale del piano di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente.

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo, ai sensi degli articoli 56[28] e 64, comma 4[29], del TUDA. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

Il Responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento.

Nel sistema di gestione informatica dei documenti dell'AOO l'attività di classificazione guida la formazione dell'archivio mediante il piano di organizzazione delle aggregazioni documentali.

3.3. Aggregazioni documentali informatiche e archivio informatico

La Pubblica Amministrazione documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati, così come definiti nell'allegato 5 "Metadati" alle presenti Linee guida.

3.3.1. Fascicoli informatici

Nelle Pubbliche Amministrazioni l'AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.

---

[28] L'articolo 56 del TUDA prevede che: "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

[29] L'articolo 64, comma 4, del TUDA prevede che: "Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo".

La produzione, il mantenimento e l'uso dei fascicoli informatici sono conformi a quanto stabilito dall'art. 65[30] del TUDA e dell'art 41[31] del CAD.

3.3.2. Altre aggregazioni documentali informatiche

All'interno del sistema di gestione informatica dei documenti la Pubblica Amministrazione forma, gestisce e utilizza tipologie di aggregazioni documentali informatiche diverse dai fascicoli: serie che aggregano documenti e serie che aggregano fascicoli.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

I fascicoli appartenenti a serie diverse possono essere collegati tra loro.

---

[30] L'articolo 65 del TUDA prevede che: "Oltre a possedere i requisiti indicati all'articolo 52, il sistema per la gestione dei flussi documentali deve:

a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
c) fornire informazioni statistiche sull'attività dell'ufficio;
d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi".

[31] L'art. 41, comma 2-ter, del CAD prevede che: "Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
   2. delle altre amministrazioni partecipanti;
   3. del responsabile del procedimento;
   4. dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
e-bis) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida".

Il successivo comma 2-quater prevede che: "Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. AgID detta, ai sensi dell'articolo 71, Linee guida idonee a garantire l'interoperabilità tra i sistemi di gestione dei fascicoli dei procedimenti e i servizi di cui agli articoli 40-ter e 64-bis".

Il sistema di gestione informatica dei documenti dell'AOO, individuata ai sensi dell'art. 50, comma 4, del TUDA[32], permette la gestione, formazione, utilizzo di serie secondo il piano di classificazione o di fascicolatura, sulla base delle indicazioni contenute nel manuale di gestione.

3.3.3. Registri e repertori informatici

Il registro di protocollo e i registri dei documenti soggetti a registrazione particolare, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati attraverso la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti che operano fra loro, secondo una struttura logica predeterminata e memorizzata in forma statica.

3.3.4. Archivio informatico

Ai fini di una corretta organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche, nella Pubblica Amministrazione il manuale di gestione documentale definisce la struttura dell'archivio all'interno del sistema di gestione informatica dei documenti.

L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa.

3.4. Compiti del responsabile della gestione documentale

Le Pubbliche Amministrazioni definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale.

Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA[33] e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui

---

[32] L'art. 50, comma 4, del TUDA, prevede che: "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

[33] L'articolo 61 del TUDA prevede che "1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.

all'art.17 del CAD[34] e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 "Designazione del responsabile della protezione dei dati" e 39 "Compiti del responsabile della protezione dei dati" del Regolamento UE 679/2016, predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

Per l'Amministrazione con più AOO il coordinatore della gestione, sentiti i responsabili della gestione documentale, assicura l'adozione di criteri uniformi per la gestione informatica dei documenti.

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

3.5. Manuale di gestione documentale

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

---

2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente. 3. Il servizio svolge i seguenti compiti:
a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni del presente testo unico;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
g) autorizza le operazioni di annullamento di cui all'articolo 54;
h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

[34] L'art. 17 del CAD prevede che:" ...ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale".

Nel manuale di gestione documentale sono riportati, in particolare:

1. relativamente agli aspetti organizzativi:
   a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
   b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
   c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
   d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

2. relativamente ai formati dei documenti:
   a) l'individuazione dei formati utilizzati per la formazione del documento informatico, come introdotti nel paragrafo 3.6, tra quelli indicati nell'Allegato 2 "Formati di file e riversamento";
   b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 "Formati di file e riversamento";
   c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 e nell'Allegato 2 "Formati di file e riversamento";

3. relativamente al protocollo informatico e alle registrazioni particolari:
   a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
   b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;
   c) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA[35], inclusa la funzione di recupero dei dati protocollati manualmente;
   d) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA[36];

---

[35] L'art. 63 del TUDA prevede che: "1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".

[36] L'art. 53, comma 5, del TUDA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle presenti Linee Guida;
f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;

4. relativamente alle azioni di classificazione e selezione:
   a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

5. relativamente alla formazione delle aggregazioni documentali
   a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6. relativamente ai flussi di lavorazione dei documenti in uso:
   a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;

7. relativamente alle misure di sicurezza e protezione dei dati personali adottate:
   a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;

8. relativamente alla conservazione:
   a) per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
   b) per i soggetti diversi dalle Pubbliche Amministrazioni che sono sprovvisti di piano di conservazione, qualora si renda necessario redigere un Manuale di gestione per la complessità della struttura organizzativa e della documentazione prodotta, dovrebbero essere definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti, ivi compresi i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013[37].

[37] L'art. 9, comma 1, del d.lgs. 33/2013, prevede che: "Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

3.6. Formati di file

I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti dall'Allegato 2 "Formati di file e riversamento". Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

Le pubbliche amministrazioni garantiscono sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), le pubbliche amministrazioni, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento", effettuando una valutazione di interoperabilità.

La valutazione di interoperabilità è effettuata in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento". La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.

3.7. Riversamento

A seguito della valutazione di interoperabilità, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD valutano l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento".

3.8. Trasferimento al sistema di conservazione

I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.

Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento a un sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi

pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali[38] di comunicazione agli organi competenti in materia di tutela dei beni archivistici o, nel caso di affidamento esterno, alla loro autorizzazione.

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di gestione informatica dei documenti nel rispetto della normativa sui beni culturali.

3.9. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)[39], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

---

[38] L'art. 21, comma 1, del Codice dei beni culturali prevede che: "Sono subordinati ad autorizzazione del Ministero: a) la rimozione o la demolizione, anche con successiva ricostituzione, dei beni culturali; b) lo spostamento, anche temporaneo, dei beni culturali mobili, salvo quanto previsto ai commi 2 e 3; c) lo smembramento di collezioni, serie e raccolte; d) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13, nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'articolo 10, comma 2, lettera c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'articolo 13; e) il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13".
Il successivo comma 3 prevede che: "Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione, ma comporta l'obbligo di comunicazione al Ministero per le finalità di cui all'articolo 18".

[39] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[40], e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.

In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento Reg. UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

[40] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

CAPITOLO 4 Conservazione

4.1. Sistema di conservazione

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD[41],:

a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000[42] e art. 44, comma 1-bis, CAD;
c) gli archivi informatici con i metadati associati.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il

[41] L'art. 44, comma 1-bis, del CAD prevede che: "Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi".

[42] L'art. 67, comma 2, del TUDA prevede che: "Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente".

sistema di conservazione sono riportati negli allegati 2 "Formati di file e riversamento" e 4 "Standard e specifiche tecniche".

4.2. Pacchetti informativi

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;

b) pacchetti di archiviazione;

c) pacchetti di distribuzione.

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati individuati nel manuale di gestione e nel manuale di conservazione in conformità con le presenti Linee Guida.

4.3. Modelli organizzativi della conservazione

Le Pubbliche Amministrazioni realizzano il processo di conservazione ai sensi dall'art. 34, comma 1-bis, del CAD[43], fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del Titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

---

[43] L'art. 34, comma 1-bis, del CAD prevede che: "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".

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems - Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (*Open Archival Information System - Sistema informativo aperto per l'archiviazione*), e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.*

4.4. Ruoli e responsabilità

I ruoli individuati nel processo di conservazione sono:

a) titolare dell'oggetto della conservazione;
b) produttore dei PdV;
c) utente abilitato;
d) responsabile della conservazione
e) conservatore.

Nelle Pubbliche Amministrazioni, il ruolo di produttore del PdV è svolto da persona interna alla struttura organizzativa.

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

Nelle Pubbliche Amministrazioni il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PdV e assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Nel caso di affidamento a terzi, il produttore di PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

4.5. Responsabile della conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD[44].

[44] L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad

Nella Pubblica Amministrazione, il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti

---

altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali[45];

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.

Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

4.6. Manuale di conservazione

Il manuale di conservazione è un documento informatico che deve illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il manuale di conservazione, inoltre, deve riportare:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione

[45] L'art. 41, comma 1, del Codice dei beni culturali prevede che: "Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio".

e di evoluzione delle medesime;

h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione.

La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

In caso di affidamento del servizio di conservazione ad un conservatore esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al manuale del conservatore esterno.

Resta fermo l'obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici.

Resta ferma inoltre la competenza del Ministero dei beni e delle attività culturali e del Turismo in materia di tutela dei sistemi di conservazione sugli archivi pubblici e privati che rivestono interesse storico particolarmente importante, così come disciplinato dalla normativa sui beni culturali.

4.7. Processo di conservazione

Il trasferimento dell'oggetto di conservazione nel sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsti dal manuale di conservazione di cui al paragrafo 4.7.

Il processo di conservazione prevede:

a) l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico;
b) la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell' allegato 2 "Formati di file e riversamento" relativo ai formati;
c) il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione;
d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
e) la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica

qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o dal responsabile del servizio di conservazione con il sigillo elettronico qualificato o avanzato del titolare dell'oggetto di conservazione o del conservatore e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386:2010 e secondo le modalità riportate nel manuale di conservazione;
g) la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;
h) ai fini della interoperabilità tra sistemi di conservazione, i pacchetti di distribuzione possono contenere parte, uno o più i pacchetti di archiviazione;
i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;
j) la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 "Formati di file e riversamento";
k) l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nel successivo paragrafo 4.12;
l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIBACT rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e al successivo paragrafo 4.12.

Nel caso di affidamento a terzi del servizio di conservazione le modalità sono indicate nei manuali del Titolare dell'oggetto di conservazione e del conservatore e concordate tra le parti.

4.8. Infrastrutture

Fatto salvo quanto previsto dal Codice dei beni culturali, nel rispetto del principio di libera circolazione dei dati all'interno dell'Unione europea[46], si sottolinea l'obbligo, in capo al fornitore del servizio di conservazione, di conservare e rendere disponibili le descrizioni del sistema di conservazione all'interno del territorio nazionale. I conservatori devono altresì garantire alle amministrazioni l'accesso elettronico effettivo e tempestivo ai dati conservati, indipendentemente dallo Stato membro nel cui territorio i dati sono conservati.

Le componenti tecnologiche hardware e software utilizzate dai sistemi di conservazione delle Pubbliche Amministrazioni e dei conservatori sono segregate logicamente. Qualora i servizi di conservazione siano erogati in modalità cloud, il servizio deve essere qualificato come previsto dalla Circolare Agid n. 3 del 9 aprile 2018 e, conseguentemente, essere presente nel "Catalogo dei servizi Cloud per la PA qualificati" pubblicato sul sito di Agid.

[46] Reg. (UE) 2018/1807 all'articolo 4, paragrafo 1 recita:" Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità."

I sistemi di conservazione devono essere realizzati nel rispetto del principio di integrità e riservatezza, nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita, e dei conseguenti adempimenti previsti dagli artt. 25[47] e 32 del citato Regolamento UE 679/2016.

4.9. Modalità di esibizione

Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione secondo le modalità descritte nel manuale di conservazione, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e modalità di accesso diverse, in funzione delle tipologie di dati personali trattati, nonché delle operazioni di trattamento consentite.

Nel caso di affidamento esterno del servizio di conservazione tali modalità sono concordate tra le parti e indicate nei rispettivi manuali.

4.10. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016[48], anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

---

[47] L'art. 25 del Regolamento "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"

[48] L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art.28 del Regolamento.

Il piano conterrà altresì la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016[49], e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.
Le misure di sicurezza sono descritte nel manuale di conservazione di cui al par. 4.7.

Nel caso di affidamento esterno del servizio di conservazione le misure di sicurezza sono concordate tra le parti e indicate nei rispettivi manuali. In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è delegata la tenuta del sistema di conservazione sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici adeguano il sistema di conservazione a tali regole. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

4.11. Selezione e scarto dei documenti informatici

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Titolare dell'oggetto di conservazione e, nel caso delle Pubbliche Amministrazioni, secondo quanto indicato dal piano di conservazione. Nel caso di affidamento esterno del servizio di conservazione le modalità operative sono concordate dal Titolare dell'oggetto di conservazione e dal Conservatore.

Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o del coordinatore della gestione documentale, ove nominato. In caso di affidamento esterno del servizio di conservazione l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

[49] Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

Nel caso degli archivi pubblici e degli archivi privati con il solo riferimento a quelli dichiarati di interesse storico particolarmente importante l'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.

Le proposte di scarto di pacchetti di archiviazione contenenti documenti e/o dati sottratti alla libera consultabilità devono essere autorizzate dal Ministero dell'interno.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, procede alla distruzione dei pacchetti di archiviazione.

Nel caso di affidamento esterno del servizio di conservazione, il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

L'operazione di scarto viene tracciata sul sistema mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione notifica l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza. Analoga comunicazione è inviata al Ministero dell'interno in caso di eliminazione di pacchetti di archiviazione contenenti documenti e/o dati di carattere riservato.

Tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.

I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Titolare dell'oggetto di conservazione.