Ministero della Giustizia

Dipartimento dell'Organizzazione Giudiziaria, del Personale e dei Servizi

Direzione Generale per i Sistemi Informativi Automatizzati

MANUALE PER LA GESTIONE DEI FLUSSI DOCUMENTALI DEL MINISTERO DELLA GIUSTIZIA

Revisione al 04.01.2021

Il presente "Manuale di Ente" **descrive** il sistema di gestione e di conservazione dei documenti, **fornisce** le istruzioni uniche e vincolanti per le articolazioni del Ministero della Giustizia per il corretto funzionamento del servizio di tenuta del protocollo informatico e di gestione dei flussi documentali, **mira** a realizzare le condizioni operative per gestire il flusso informativo e documentale anche ai fini di una più rapida semplificazione ed una maggiore trasparenza amministrativa.

INDICE

PREMESSA

Il Manuale di Gestione (di seguito "Manuale") è redatto ai sensi del par. 3.5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate sul sito web istituzionale dell'AGID in data 11.09.2020.

Queste sono articolate in un documento principale e in sei Allegati che ne costituiscono parte integrante. Gli allegati sono i seguenti:

Allegato 1 - Glossario dei termini e degli acronimi
Allegato 2 - Formati di file e riversamento
Allegato 3 - Certificazione di processo
Allegato 4 - Standard e specifiche tecniche
Allegato 5 - Metadati
Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati.

A partire dalla data di applicazione delle Linee Guida AGID, 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".
- il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico" fatti salvi i seguenti articoli:
    - 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.
- 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" sostituita dal sopra richiamato allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati".

Una volta adottato, il Manuale viene aggiornato periodicamente, in virtù del costante censimento e della progressiva razionalizzazione delle attività e delle prassi in essere, dell'individuazione e della definizione di nuovi aspetti organizzativi e gestionali, anche nel rispetto della normativa eventualmente sopraggiunta.

INTRODUZIONE

Il Manuale indica le politiche di gestione dell'intero ciclo di vita di un documento e le caratteristiche del sistema di protocollo, come individuate dalla cangiante normativa.
La normativa inerente alla gestione del patrimonio documentale e del suo ciclo di vita è riportata in **ALLEGATO 1** ed è da intendersi aggiornata ed integrata anche dagli interventi del Legislatore successivi alla data di adozione del presente atto.
In **ALLEGATO 2** è riportato l'elenco delle definizioni e degli acronimi utilizzati in questo documento.
In **ALLEGATO 3** è riportato l'elenco dei formati dei documenti informatici ammessi – in ricezione – dal MINISTERO DELLA GIUSTIZIA.
In **ALLEGATO 4** è riportato il documento sulle politiche di sicurezza.
In **ALLEGATO 5** è riportato un estratto del "Codice Aurora" di cui alle c.d. "Pillole di Aurora".
In **ALLEGATO 6** è riportato l'elenco delle Aree Organizzative Omogenee (AOO) del Ministero della Giustizia.
In **ALLEGATO 7** è riportata la nomina del Coordinatore ministeriale della Gestione documentale e suo vicario.

1 STRUMENTI DI GESTIONE DOCUMENTALE.

1.1 IL MANUALE DI GESTIONE DI ENTE.

Il presente Manuale di Gestione di Ente definisce criteri, regole e prassi vincolanti per ciascuna AOO ministeriale, in materia di formazione, protocollazione, gestione e conservazione del documento.
Obiettivo generale del documento è presentare una visione d'insieme che aggreghi in un "corpo unico" le materie che nella prassi sono regolate separatamente da ciascun ufficio o in maniera assai differente, da ufficio ad ufficio. Considerata la velocità dell'innovazione sia tecnologica che normativa, questo Manuale fissa un nucleo minimo di politiche vincolanti per tutte le articolazioni ministeriali riconoscendo a queste ultime, l'opportunità di adattare alle proprie prassi quei punti in cui è espresso il rinvio al Manuale di AOO.
Quindi, ciascuna AOO potrà redigere il proprio Manuale di Gestione al fine di rendere le prassi qui definite, coerenti con il proprio contesto organizzativo.
Al fine di garantire un adattamento costante ai cambiamenti pretesi dalla trasformazione delle prescrizioni normative in operatività digitale, il Manuale consta di un testo "statico" che contiene le politiche di riferimento e di una serie di "allegati" i cui contenuti saranno aggiornabili agevolmente

senza che ciò comporti una riadozione dell'intero Manuale [versione ß (*beta) permanente*[1]]. La Direzione Generale per i Sistemi Informativi Automatizzati – di seguito DGSIA - nella qualità di Responsabile per la transizione al digitale[2], ha individuato le AOO del Ministero di Giustizia, ha redatto il presente Manuale, supporterà l'eventuale adozione dei Manuali da parte di ciascuna AOO e definirà tempi, modalità, misure organizzative e tecniche per la eliminazione dei protocolli settoriali e dei relativi registri, specie se ancora cartacei[3].

Nel Ministero della Giustizia, di seguito MdG, i compiti previsti in capo al Responsabile della gestione documentale sono assolti dal Coordinatore della Gestione documentale dell'Ente, nominato con il provvedimento di cui all'ALLEGATO 7.

Il Coordinatore definisce criteri uniformi di trattamento dei documenti informatici, regole per la classificazione ed archiviazione, modalità della comunicazione tra le Aree Organizzative Omogenee *interne*, ai sensi dell'art. 50, comma 4, del Testo Unico; stabilisce regole uniformi per la gestione dei servizi di protocollo di Ente ed ha il compito di redigere e pubblicare il Manuale di Gestione di Ente.

1.1.1 MODALITÀ DI ADOZIONE, PUBBLICAZIONE ED AGGIORNAMENTO DEL MANUALE.

L'Amministrazione adotta il presente Manuale su proposta del Coordinatore per la gestione documentale di Ente, con determinazione della DGSIA ex art. 4, co. 1 lett. b) del DPCM 19 giugno 2019 n. 99 recante il "Regolamento concernente l'organizzazione del Ministero della Giustizia di cui al decreto del Presidente del Consiglio dei ministri 15 giugno 2015, n. 84." e provvede alla pubblicazione sul proprio sito WEB. Le esigenze di aggiornamento derivanti da specifiche richieste delle AOO dovranno essere rappresentate al Responsabile per la Transizione al Digitale nella persona del Direttore Generale Sistemi Informativo Automatizzati oppure al Coordinatore per la gestione documentale dell'Ente.

1.2 AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO DEL SERVIZIO DI GESTIONE DOCUMENTALE.

Una AOO[4] è un insieme di unità organizzative dell'Amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali.

---

[1] La versione ß di un documento è una versione definita ma non definitiva, già validata dagli esperti, messa a disposizione di un gran numero di utenti esterni o fruitori chiamati dalla quotidiana prassi lavorativa ad un frequente uso del documento e che per questo potranno portare alla luce esigenze di nuove integrazioni, adattamenti, emendamenti e revisioni dello stesso, senza sottoporre ogni volta il documento in parola all'intero work flow approvativo.

[2] Art. 17 CAD e DPCM 99/2019 art.4; da ultimo, D.M 23.04.2020, recante "Misure necessarie al coordinamento informativo ed operativo tra la Direzione Generale per i sistemi informativi automatizzati del Ministero della Giustizia, nonché concernente l'individuazione degli uffici di livello dirigenziale non generale e la definizione dei relativi compiti ai sensi dell'articolo 16, commi 1 e 2, del decreto del Presidente del Consiglio dei Ministri 15 giugno 2015, n. 84 e dell'articolo 8, comma 2, del decreto del Presidente del Consiglio dei Ministri 19 giugno 2019, n. 99.

[3] Art. 50 comma 2 del Testo Unico per la Documentazione Amministrativa.

[4] cfr.art. 50, comma 4, DPR n. 445/2000

Per ciascuna AOO, il sistema di protocollazione è unico.
Il modello organizzativo, definito per tipologie standard di ufficio e validato dal Coordinatore della Gestione documentale di Ente e da DGSIA, è descritto, insieme ai flussi interni correlati, nel Manuale di gestione di AOO. L'elenco delle AOO del MdG è riportato in ALLEGATO 6. Tale documento, in versione *ß permanente,* è automaticamente aggiornato nei casi di sopravvenuta pubblicazione di norme e regolamenti o provvedimento istitutivi o di revoca delle AOO.

1.3 POSTA ELETTRONICA CERTIFICATA (PEC), DOMICILIO DIGITALE E INDICE IPA.

La comunicazione istituzionale avente valore legale è gestita a mezzo PEC e sempre tramite protocollo informatico, fatti salvi i canali di comunicazione collegati ai sistemi informatizzati dei registri giudiziari e degli applicativi ufficiali distribuiti dalla DGSIA, e tutti i canali gestiti in cooperazione applicativa con le piattaforme di altre Pubbliche Amministrazioni.
Ogni AOO è, pertanto, dotata di almeno una casella istituzionale di PEC, integrata nel sistema di protocollo informatico e fornita dal MdG. Tale casella costituisce il domicilio digitale della AOO ex art. 6 c.1 del Codice dell'Amministrazione Digitale - CAD. [5]
Le AOO del MdG di cui all'ALLEGATO 6, con il relativo indirizzo PEC integrato nel sistema di protocollo, sono iscritte nell'Indice dei Domicili Digitali della Pubblica Amministrazione e dei gestori di pubblici servizi – IPA[6].
In capo ad ogni AOO è la verifica almeno semestrale dei dati pubblicati in IPA, come da art. 6-ter del CAD e secondo le dedicate linee guida AGID.
Le richieste di modifica dei dati pubblicati su IPA devono essere trasmesse tramite protocollo al Referente nazionale IPA.
Termini e modalità di verifica e comunicazione sono definibili dal singolo ufficio, con separato atto o nello specifico manuale di AOO.
In definitiva, la PEC è idonea a gestire le comunicazioni esterne istituzionali aventi valore legale, mentre è inidonea per gestire comunicazioni interne o riservate.

[5] "Il domicilio digitale è un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato valido ai fini delle comunicazioni elettroniche aventi valore legale [art.1 comma 1 lettera n-ter del CAD].
L'IPA (Indice dei domicili digitali) è l'elenco pubblico di fiducia contenente i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti validi a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.
I domicili digitali devono essere associati ad un registro di protocollo che, nell'IPA, è rappresentato da una ed una sola Area Organizzativa Omogenea (AOO)." Font: stralcio dalla pagina https://www.indicepa.gov.it/documentale/n-domicili-digitali.php
[6] Art. 6 ter del CAD.

1.4 POSTA ELETTRONICA ORDINARIA (PEO) E SISTEMA DI PROTOCOLLO INFORMATICO

I sistemi di protocollo possono essere integrati anche con una casella istituzionale di posta elettronica ordinaria, destinata ad essere utilizzata per trasmissioni interne oppure per scambi con interlocutori non dotati di casella di posta elettronica certificata e per comunicazioni non aventi valore legale bensì ordinario e corrente (interlocutorio o informativo).
In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, tutti i dipendenti sono dotati dall'Amministrazione di una casella istituzionale di posta elettronica ordinaria avente dominio giustizia.it. Essa è idonea a gestire le comunicazioni interne all'"ecosistema Giustizia", mentre è inidonea per le comunicazioni esterne istituzionali o aventi valore legale.

1.5 FIRME ELETTRONICHE

Il Ministero ha dotato le proprie risorse di CNS per la sottoscrizione digitale di documenti e atti inerenti all'espletamento delle attività istituzionali, ai processi, nonché alle attività connesse alla normativa relativa alla gestione dei documenti informatici. I formati relativi alle firme elettroniche avanzate utilizzate per la firma sono i seguenti:

- **CADES** (CMS Advanced Electronic Signatures) è una firma digitale che può essere apposta su qualsiasi tipo di file. Tale modalità di firma genera una "busta crittografica" contenente il documento informatico originale e si caratterizza per il suffisso P7M che si aggiunge all'estensione del file;
- **PADES** (PDF Advanced Electronic Signatures), invece, è una firma che può essere apposta solo su file PDF e in tal caso, l'apposizione della firma lascia immutata l'estensione del documento.

La prima è da utilizzarsi prevalentemente nel caricamento di dati su piattaforme gestite da altre PP.AA..
La seconda è da utilizzarsi in tutte le comunicazioni ordinarie aventi rilevanza esterna o interna.

Le firme digitali di cui trattasi servono pertanto a:

- fissare la paternità dell'atto;
- autenticare la firma autografa di terzi;
- attestare la conformità di una copia all'originale.

2 FIGURE DI SISTEMA

Stando alla normativa di settore vigente, si distinguono almeno quattro figure chiamate a interfacciarsi tra loro:

- il Coordinatore ministeriale della gestione documentale;

- il Responsabile di AOO del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi[7] (RSP) di cui al successivo par. 2.2;
- il Responsabile della Transizione al digitale ex art. 17 del CAD;
- il Responsabile del trattamento dei dati personali;
- il Responsabile del sistema di conservazione.

Oltre queste figure deputate alla definizione delle strategie di gestione documentale che considerino le esigenze di standardizzazione delle prassi e procedure documentali, di coerenza alla norma, di minimizzazione degl'impatti organizzativi, di efficienza ed efficacia dell'azione amministrativa, occorre che ciascuna AOO individui le figure di cui ai successivi paragrafi, deputati al presidio dell'operatività quotidiana, a garanzia della disponibilità dei servizi di cui trattasi.

2.1 INDIVIDUAZIONE E DESIGNAZIONE DELLE FIGURE

Ogni AOO individua, con dedicato atto di nomina del Capo dell'Ufficio, successivamente trasmesso al Direttore Generale per il Sistemi Informativi Automatizzati, le figure i cui compiti sono specificati nei paragrafi successivi e che possono, eventualmente, essere ulteriormente dettagliati nel Manuale di ciascuna AOO:

- Amministratore di AOO ed un suo vicario;
- Referente per la gestione delle PEC e PEO e un suo vicario.

Gli Amministratori di AOO, al fine di assicurare un approccio operativo standard alla gestione degli SdP, sono coordinati da un Amministratore di Ente o un suo Vicario.

2.2 RESPONSABILE DELLA GESTIONE DOCUMENTALE (RSP)

Trattasi di un dirigente o 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. È compito del RSP:

- presidiare la puntuale attuazione del presente Manuale;
- predisporre lo schema di Manuale di gestione di AOO, contenente regole integrative e/o attuative del presente Manuale;
- provvedere alla pubblicazione del Manuale sul sito istituzionale della propria AOO, se esistente;
- profilare i necessari utenti da inserire nel Servizio di Protocollo – di seguito SdP, inserendo per ciascuno di essi, le funzioni più appropriate tra quelle disponibili;
- curare l'aggiornamento sul SdP dell'organigramma e affidare all'amministratore di AOO l'esecuzione operativa della modifica;

[7] Art. 61 co. 1 del Testo Unico per la Documentazione Amministrativa

- presidiare il rispetto delle disposizioni normative inerenti alle operazioni di protocollo;
- organizzare la tenuta la copia del registro giornaliero di protocollo;
- autorizzare le operazioni di annullamento della registrazione di protocollo così come indicato dal manuale di AOO;
- disporre l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza secondo quanto previsto nel paragrafo 10.1
- indicare tempi, modalità, misure organizzative e tecniche per la eliminazione dei protocolli settoriali e dei relativi registri, specie se ancora cartacei.

2.3 AMMINISTRATORE DI AOO

Trattasi di una figura operativa di supporto al responsabile della Gestione documentale (RSP).

È compito dell'Amministratore di AOO:

- manutenere ed aggiornare gli elementi costitutivi di ciascuna AOO: registri, titolario di archivio, liste di competenza, uffici e utenti dell'AOO, rubriche ecc.;
- assicurare l'inserimento nel SdP degli utenti individuati dal RSP secondo il profilo e le funzioni e secondo quanto stabilito nel manuale di AOO;
- verificare, in caso di cessazione dal servizio o trasferimento ad altro ufficio di un utente del sistema di protocollo, che lo stesso abbia classificato tutti i documenti a suo carico o assegnare gli stessi ad altro utente e poi provvedere alla chiusura dell'utenza.
- formalizzare all'RSP la richiesta di abilitazione al servizio qualora formulata dai singoli utenti;
- monitorare il rispetto delle disposizioni inerenti al protocollo;
- garantire operativamente la conservazione della copia del registro giornaliero di protocollo secondo termini e modalità specificati nel manuale di AOO;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza in attuazione delle disposizioni dichiarative dell'emergenza da parte del Direttore Generale SIA, del Coordinatore della Gestione Documentale o del RSP;
- monitorare l'iPA per l'aggiornamento semestrale dei dati;
- supportare la redazione del manuale di AOO;
- supportare il RSP nella adozione delle misure organizzative e tecniche per la eliminazione dei protocolli settoriali e dei relativi registri, specie se ancora cartacei.

2.4 REFERENTE PER LA PEC E LA PEO ISTITUZIONALI

Trattasi di figura operativa di supporto. È compito del referente:

- monitorare la gestione dei "punti unici di accesso documentale" gestiti a mezzo posta elettronica certificata e ordinaria, se esistenti;
- stimolare l'attuazione delle disposizioni normative e regolamentari vigenti in materia;

- disporre tempi, termini e modalità di gestione delle password di accesso alle caselle di posta non integrate negli applicativi ministeriali e non personali, oggetto di presidio e monitoraggio da parte dell'AOO, se non da altri gestiti (es. referenti GSI).

3 IL DOCUMENTO

I documenti sono distinguibili in:

- analogici o informatici
- aventi rilevanza esterna o interna
- trasmesso o ricevuto (in entrata/in uscita)
- amministrativo o meno

In Allegato 2 le relative definizioni.

Di seguito, i termini e le modalità di redazione e gestione.

3.1 DOCUMENTO ANALOGICO E DOCUMENTO INFORMATICO

In osservanza della normativa di settore vigente, con particolare riguardo all'art. 40 del CAD, i documenti del MdG sono redatti con strumenti informatici dovendo essere, ex lege, nativi digitali.
Pertanto, le produzioni documentali analogiche (esempio: lettera scritta a mano) sono da considerarsi casi straordinari di oggettiva impossibilità, di generare un documento elettronico.
I documenti informatici, in particolare se destinati al protocollo, indipendentemente dal software utilizzato per la loro redazione e prima della loro eventuale sottoscrizione con firma digitale, devono essere convertiti in uno dei formati standard di cui all'ALLEGATO 3, al fine di garantire la non alterabilità durante le fasi di accesso e conservazione, e l'immutabilità nel tempo del contenuto e della struttura.
Per la sottoscrizione dei documenti si rinvia alle disposizioni contenute nel Codice dell'Amministrazione Digitale.

3.1 RILEVANZA ESTERNA O INTERNA DI UN DOCUMENTO

La gestione dei documenti di rilevanza esterna è regolamentata dal CAD e dal TUDA, mentre la gestione di quelli di rilevanza interna è disciplinata dai Manuali di Gestione di Ente e di AOO.
Le comunicazioni di rilevanza interna, scambiate tra uffici via PEO, possono essere assunte a protocollo su richiesta del mittente o del responsabile della AOO/UO, qualora ritenute rilevanti per la gestione di un procedimento amministrativo e meritevoli di conservazione.

3.2 IL CICLO DI VITA DI UN DOCUMENTO INFORMATICO

Il documento amministrativo si forma ed è gestito secondo i seguenti processi:

1. Redazione
   È la produzione tramite l'utilizzo di appositi strumenti software. Le caratteristiche di immodificabilità e integrità sono garantite da una delle seguenti operazioni: dalla sottoscrizione con firma digitale, dall'apposizione di una validazione temporale, dal trasferimento a soggetti terzi tramite posta elettronica certificata, dalla registrazione nel sistema di protocollo informatico o tramite versamento in un sistema di conservazione.
   Ogni documento tratta uno specifico argomento, indicato dall'autore in maniera sintetica ma esaustiva nello spazio riservato all'oggetto;
2. Acquisizione
   È la presa in carico di documenti in ingresso o in uscita, che avviene di norma per via telematica, o con acquisizione di file su supporto informatico, di file prodotti mediante copia per immagine (scansione o copia informatica di documento analogico) oppure con presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente.
3. Registrazione informatica.
   È l'inserimento delle informazioni relative al documento acquisito nel SdP o nei sistemi di workflow management di cui l'Amministrazione è dotata. Ogni documento sarà identificato univocamente da una registrazione di protocollo;
4. Gestione informatica
   È la definizione di chi, cosa e quando può trattare il documento acquisito secondo le prescrizioni in materia di accessibilità, di responsabilità amministrativa in materia di opportuna ed intelligente trattazione del contenuto nel rispetto delle competenze relative alla definizione dei procedimenti attivati.
   Ogni documento può attenere a più fascicoli elettronici.
5. Conservazione a norma
   È il processo che consente la corretta tenuta ed archiviazione di un documento informatico.

I processi di cui sopra, devono garantire:

- l'identificabilità del soggetto che ha formato il documento e l'AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche e con gli strumenti tecnologici ivi prescritti;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- la possibilità di accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- le possibilità di circolazione dei documenti all'interno della stessa AOO e tra AOO diverse.

4 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

4.1 REGISTRAZIONE INFORMATICA E SEGNATURA DI PROTOCOLLO

L'art. 53 co. 5 del TUDA dispone che "sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici" ed elenca i dati minimi obbligatori e le regole per la registrazione inseriti come da ALLEGATO 5.

Il registro di protocollo è un atto pubblico originario che fa fede dell'effettivo ricevimento o spedizione di un documento in una data certa. È unico, con numerazione progressiva per anno solare. Il numero di protocollo individua un unico documento e ogni documento reca un solo numero di protocollo. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo già attribuiti ad altri atti, pur se strettamente correlati tra loro. Di conseguenza, non è ammessa la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in entrata e per il documento in uscita né tantomeno è consentita l'assegnazione di un solo numero di protocollo alla ricezione di una gran mole di documenti simili in risposta, ad esempio, ad un avviso o bando pubblico[8]. In caso di necessità di inviare più documenti è possibile procedere o con protocollazione singola di ciascuna istanza, o con protocollazione di una sola nota di trasmissione corredata delle istanze di cui trattasi.

La segnatura di protocollo è un'operazione effettuata contestualmente a quella di registrazione. Consiste nell'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni essenziali ed obbligatorie, riguardanti il documento stesso, consentendo di individuarlo in modo inequivocabile. A tal fine, il sistema di protocollo informatico produce il file di segnatura, i cui dati saranno utilizzati a completamento automatico delle informazioni afferenti alla registrazione di protocollo. Tali dati non saranno modificabili dall'addetto al protocollo successivamente alla registrazione o in caso di registrazione automatica, fatto salvo il campo "oggetto" il cui contenuto può essere integrato per inserire ulteriori informazioni necessarie alla AOO ricevente.

Sui documenti in uscita, l'etichetta di segnatura di protocollo viene impressa almeno sul primo foglio del documento informatico. Al fine di garantire la validità del documento informatico così prodotto, la segnatura apposta sul documento viene firmata in modalità automatica. Il file di segnatura viene allegato a tutti i documenti in uscita per posta elettronica. Il formato della segnatura di protocollo dell'AOO viene prodotto coerentemente con le specifiche tecniche dedicate.

Per migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare, integrare o eliminare elementi facoltativi del protocollo: la modifica di dati facoltativi

[8] All'interno del DPCM del 3 dicembre 2013, articoli 40-bis, 41, 47, 57-bis e 71, nonché del CAD sono stabilite le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni:
- di registrazione e segnatura di protocollo, di cui agli articoli 53, 55 e 66 del D.P.R. 28 dicembre 2000, n. 445 (TUDA);
- di registrazione di protocollo agli articoli 40-bis, 41 e 47 del Codice dell'amministrazione digitale (CAD).

non comporta necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

4.2 DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

L'art. 53, co. 5 del TUDA esclude dalla registrazione le seguenti tipologie documentali:

- gazzette ufficiali;
- bollettini ufficiali della PA;
- notiziari della PA;
- note di ricezione delle circolari e altre disposizioni;
- documenti statistici;
- atti e corrispondenza interna di natura informativa scambiata tra uffici come ad esempio, richieste di materiale di cancelleria, richieste di interventi di manutenzione hardware;
- materiale editoriale o pubblicitario;
- inviti a manifestazioni;
- documenti erroneamente indirizzati;
- tutti i documenti già soggetti a protocollazione particolare dell'amministrazione;

Sono parimenti esclusi dalla registrazione di protocollo:

- i certificati medici dei dipendenti
- le richieste di ferie di singoli;
- le richieste di permessi retribuiti;
- le comunicazioni da parte di enti diversi di bandi di concorso;
- Le fatture elettroniche che vengono gestite attraverso il sistema di interscambio messo a disposizione della P.A. (Sicoge);
- I documenti unici di regolarità contributiva (DURC) dei fornitori di beni, servizi e lavori.

Un sistema di protocollo informatico non è in grado di riconoscere l'eventuale appartenenza di un documento ad uno dei punti sopra elencati, pertanto, la valutazione deve essere eseguita manualmente.

Alcune delle voci in elenco hanno perso rilevanza perché i corrispondenti documenti sono stati inglobati in diversi flussi informatici e in nuove modalità di comunicazione.[9]

Eventuali deroghe a quanto sopra, da motivare adeguatamente, possono essere contemplate nel manuale di AOO.

Atti preparatori e corrispondenza interna possono trovare utile registrazione mediante la funzione di protocollo interno, non specificamente prevista dalla norma, ma implementata per evidente opportunità e di cui al par. 5.3.

[9] Es.: Gazzetta Ufficiale e Bollettino Ufficiale, oggi pubblicate e non più assoggettate a spedizione periodica

4.3 ANNULLAMENTO DELLE REGISTRAZIONI DI PROTOCOLLO.

I dati obbligatori della registrazione di protocollo sono inseriti in campi non modificabili e quindi, eventuali errori di immissione ad essi riferiti, non possono essere corretti ma comportano la necessità di annullare l'intera registrazione di protocollo. Anche le registrazioni a protocollo di documenti erroneamente introdotti nel patrimonio documentale dell'AOO devono essere annullate.
La richiesta di annullamento, da chiunque provenga, va trasmessa al RSP o all'Amministratore di AOO, o a terzi secondo termini e modalità individuate nel Manuale di AOO.
In assenza di quest'ultimo, il RSP riceve la richiesta via PEO, completa di indicazioni sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Quindi, nessun operatore può annullare in autonomia protocolli se non è intervenuta l'autorizzazione del preposto individuato dal Manuale di Ente o di AOO.

4.4 PROTOCOLLAZIONE DIFFERITA

Nel caso in cui non sia possibile procedere alla registrazione di protocollo nel giorno di ricevimento (ad esempio per un eccezionale e imprevisto carico di lavoro, per un problema tecnico o per una ricezione avvenuta in chiusura dell'ufficio) e qualora dalla mancata registrazione di un documento nel medesimo giorno di ricezione possa venire meno un diritto di terzi, è possibile effettuare la registrazione differita di protocollo.
Il protocollo differito consente la normale registrazione a protocollo con l'evidenza della data effettiva di ricevimento. La registrazione differita è possibile esclusivamente per i documenti in arrivo a cui si possa inequivocabilmente associare la data di ricevimento e non si applica per i documenti informatici pervenuti via PEC essendo questi corredati delle ricevute e delle notifiche di accettazione e consegna che attestano la data certa di ricevimento dell'atto.
La richiesta di differimento, da chiunque provenga, va trasmessa al RSP o all'Amministratore di AOO, o a terzi secondo termini e modalità individuate nel Manuale di AOO.
In assenza di quest'ultimo, il RSP riceve la richiesta via PEO, completa di indicazioni sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Quindi, nessun operatore può differire in autonomia protocolli se non è intervenuta l'autorizzazione del preposto individuato dal Manuale di Ente o di AOO.

4.5 LIVELLO DI RISERVATEZZA

La riservatezza di alcuni documenti atta a tutelare il trattamento di dati sensibili è affare organizzativo a cui concorre, per la corretta definizione del processo di gestione, la tecnologia e la disponibilità di idonei applicativi tra cui il SdP.
Il SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati: ciascuno vede i documenti assegnatigli nella qualità di redattore, sottoscrittore o competente dell'evasione dell'affare.

Il trattamento di documenti che richiedono o prevedono livelli maggiori di sicurezza è disciplinato dalla vigente normativa in materia di protezione dei dati personali e pertanto si rinvia all'allegato 4.
Per ogni documento da trasmettere, le AOO del Ministero sono tenute a garantire la riservatezza di cui sopra omettendo l'inserimento di informazioni sensibili nei campi oggetto e/o note del SdP e individuando altresì, opportune regole da indicare nel manuale di AOO.
È sempre possibile intervenire in modifica dell'oggetto nei documenti ricevuti per evitare l'esposizione di dati riservati. Della eventuale modifica il SdP tiene la traccia dovuta ex lege.

4.6 DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

I documenti già destinati a registri informatici dell'Amministrazione (es. atti destinati ai registri penali o civili) non devono essere registrati al protocollo.
L'istituzione sul SdP di specifici registri particolari può essere proposta dalle AOO e disposta dal Responsabile per la Transizione al Digitale o dal Coordinatore ministeriale per la gestione documentale.

4.7 PROTOCOLLI URGENTI

La protocollazione di atti avviene, di norma, secondo l'ordine cronologico di arrivo nella disponibilità delle risorse deputate al servizio.
La richiesta di protocollare urgentemente un documento, da chiunque provenga, va trasmessa al RSP o all'Amministratore di AOO, o a terzi secondo termini e modalità individuate nel Manuale di AOO.
In assenza di quest'ultimo, il RSP riceve la richiesta via PEO, completa di indicazioni sulla nota in questione e sulla motivazione per la quale l'operazione sarebbe opportuna.
Quindi, nessun operatore può procedere in autonomia se non è intervenuta l'autorizzazione del preposto individuato dal Manuale di Ente o di AOO.
L'urgenza di cui trattasi, è motivata esclusivamente da una necessità indifferibile e straordinaria. Tale procedura, osservata sia per i documenti in ingresso che per quelli in uscita, può essere regolamentata nel Manuale di ciascuna AOO.

4.8 DOCUMENTI NON FIRMATI - ANONIMI

Nel caso di ricevimento di documenti non firmati o anonimi, l'addetto al protocollo, conformandosi alle regole stabilite in ciascun manuale di AOO, attesta la data, la forma e la provenienza per ciascuno di essi. Le lettere anonime devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e identificate come tali con la dicitura "documento non sottoscritto".
Al di là della forma documentale, il merito posto va sempre verificato per eventuali seguiti di competenza, secondo termini e modalità di cui a ciascun manuale di AOO.

4.9 REGISTRO GIORNALIERO DI PROTOCOLLO

Le regole sulla formazione e conservazione dei registri e repertori informatici sono contenute nelle Linee guida AGID di cui in premessa.
Il SdP genera automaticamente un file contenente le registrazioni di protocollo del giorno.

4.10 TENUTA DEI DOCUMENTI REGISTRATI

I documenti registrati sono tenuti sul SdP in modalità non modificabile per almeno dieci anni. Sono resi disponibili alle UO competenti dopo l'operazione di assegnazione ed in base ai diritti di visibilità.
Il SdP rappresenta pertanto, il cosiddetto *archivio corrente*.

5 PROTOCOLLAZIONE ATTI IN ENTRATA, IN USCITA ED INTERNI

Il canale applicativo privilegiato per lo scambio di documenti tra PP.AA. è quello interoperabile.
Dall'01.01.2022 il canale applicativo interoperabile sarà il mezzo esclusivo per lo scambio di documenti tra le AOO di Giustizia.
La registrazione di protocollo prevede una numerazione sequenziale annuale per gli atti in entrata ed in uscita, contraddistinti, rispettivamente, dal simbolo .E (entrata) oppure .U (uscita).
Il SdP del MdG dedica un registro con numerazione indipendente, da 1 a n per anno, per il flusso di gestione degli atti interni, contraddistinti dal simbolo .ID (interno), e per le registrazioni di emergenza (.EM).

5.1 DOCUMENTI IN ENTRATA

I documenti in entrata attivano un workflow diverso dipendente dalla natura dello stesso: analogico, digitale o "misto".

5.1.1 DOCUMENTI DIGITALI E MISTI.

Nelle more della scadenza di cui sopra, al fine di promuovere buone prassi di gestione documentale, ciascun RSP può, in caso di corrispondenza pervenuta per canali diversi da quelli interoperabili, inviare via mail al mittente una comunicazione di invito all'uso dei canali di trasmissione PEC disponibili sul protocollo.
La ricezione dei documenti informatici può avvenire via posta elettronica certificata o ordinaria. Per questo, il personale della UOP è tenuto a monitorate le caselle istituzionali di PEO e presidiare quelle di PEC, salvo diversa indicazione da esplicitare nel Manuale di ciascuna AOO.
Si distinguono i seguenti casi:

a. messaggio ricevuto su una casella istituzionale di posta elettronica di servizio integrata nel sistema di protocollo: questo verrà automaticamente protocollato;

b. messaggio ricevuto su una casella istituzionale di posta elettronica di servizio non integrata nel sistema di protocollo: solo qualora esso abbia una rilevanza amministrativa, nei modi e termini indicati nel Manuale di AOO, va inoltrato all'UOP che provvederà alla protocollazione, inserendo correttamente il mittente d'origine nel sistema di protocollo;
c. messaggio avente in allegato un documento scansionato e sottoscritto in maniera autografa: va verificata la provenienza certa del documento secondo le previsioni della normativa di settore vigente. Termini e modalità di verifica nonché di valutazione dei casi in cui i mittenti non sono verificabili, sono descritti nel manuale di AOO. In mancanza, varranno le puntuali determinazioni del RSP comunicate a mezzo PEO istituzionale;
d. messaggio firmato digitalmente o avente in allegato, un documento sottoscritto digitalmente: si provvederà a protocollarlo registrando come mittente il soggetto firmatario nel rispetto delle regole descritte nel manuale di AOO, se adottato;
e. messaggio contenente un testo non sottoscritto: vale quanto al punto c);
f. documento sottoscritto digitalmente consegnato in sede: va protocollato segnando come mittente il firmatario e annotando in campo "note" data, ora e autore della consegna;
g. documento sottoscritto digitalmente con allegati analogici: va protocollato e nel campo "note" va segnato che gli allegati cartacei sono tenuti presso la stanza X e vanno ritirati dall'assegnatario per competenza della nota, contattando Y;
h. documento sottoscritto in maniera autografa con allegati digitali: la nota analogica va scansionata e protocollata insieme agli allegati digitali consegnati, compatibilmente al "peso" degli stessi. Qualora tale peso eccedesse la misura fissata dalle specifiche tecniche proprie del SdP, nel campo "note" va segnato che gli allegati digitali, organizzati su un dedicato supporto, sono tenuti presso la stanza X e vanno ritirati dall'assegnatario per competenza della nota, contattando Y.

Per i documenti informatici ricevuti per via telematica, il SdP, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di almeno uno dei seguenti messaggi:

- notifica alla AOO mittente di avvenuta protocollazione;
- notifica di eccezione: documenta la rilevazione di una anomalia in un messaggio ricevuto;
- notifica di annullamento di protocollazione: comunica l'annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza.

5.1.2 DOCUMENTI ANALOGICI O CARTACEI

Il documento pervenuto in formato cartaceo è acquisito in formato immagine (copia per immagine di documento analogico) attraverso un processo di scansione, secondo le fasi di seguito indicate:

- acquisizione delle immagini in unico file anche se il documento cartaceo sia composto da più pagine;
- verifica della leggibilità e della qualità delle immagini acquisite;

- registrazione di protocollo e rilascio del numero progressivo.

I documenti pervenuti tramite servizio postale sono consegnati direttamente alla UOP per le verifiche del caso (integrità, riservatezza, sicurezza, pertinenza e correttezza del recapito).

Ciascuna AOO individua, nel proprio Manuale, le tipologie di missive che, correttamente recapitate, non sono subito aperte ed avviate all'UOP. A titolo di esempio, si citano i casi relativi agli atti di gara – se espressamente previsto dei relativi documenti regolatori o alle buste recanti la dicitura "personale" o "riservata".

In mancanza del Manuale di AOO, le missive relative alla gestione di gare e contratti e quelle riportanti la dicitura "riservata" o simili, vanno consegnate al RSP per il seguito di competenza.
Quelle riportanti la dicitura "personale" o simili, vanno consegnate alla risorsa indicata in indirizzo. In assenza, anch'esse vanno consegnate al RSP.

Tra PPAA la trasmissione via fax dei documenti è esclusa ai sensi art. 47 del CAD.

Ogni AOO provvederà ad eliminare dai propri siti web, modelli e carta intestata i riferimenti al FAX. Tuttavia, il documento comunque ricevuto via FAX va gestito come se fosse un documento cartaceo. Qualora l'AOO sia dotata di apparecchi di fax management, il documento ricevuto è un documento digitale da trattare come tale.
Qualora pervenga in un momento successivo l'originale del documento già trasmesso via FAX, quest'ultimo NON va protocollato.

5.1.3 INTEGRAZIONI DOCUMENTARIE

Il protocollatore non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento e gli eventuali allegati. Tale verifica spetta all'UO assegnataria: qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta la sospensione del procedimento. I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOP con esplicito riferimento alla registrazione di protocollo "PRECEDENTE", al fine della corretta gestione del fascicolo.
Termini e modalità differenti saranno definibili dalle AOO nel proprio Manuale.

5.1.4 ASSEGNI E ALTRI VALORI DI DEBITO O CREDITO

Nel caso di ricezione di assegni o valori di debito o credito, va protocollata la lettera di trasmissione e indicato nel campo "note" il luogo di custodia dell'originale ricevuto.

5.1.5 PROTOCOLLAZIONE DI DOCUMENTI DI GARE CONFEZIONATE SU SUPPORTI CARTACEI

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" et similia, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP. Quest'ultima provvede a timbrare il plico, a riportare sul medesimo la data, l'ora di arrivo, a protocollarla ed a consegnarla alla UO competente in materia, secondo le eventuali istruzioni da questa fornite. In assenza, il plico così protocollato viene consegnato alla UO competente che provvede alla custodia per il seguito. Successivamente all'apertura delle buste, l'UO che gestisce la gara riporta su tutti i documenti in essa contenuti gli estremi di protocollo indicati sul plico.

5.1.6 ATTI PERVENUTI PER ERRORE

Un documento perviene per errore quando reca una errata definizione del destinatario o viene recapitato per errata esecuzione dei servizi di consegna.

Fatte salve le disposizioni di legge sull'accesso agli atti e all'accesso civico generalizzato, relativamente alla circolazione delle istanze e ai relativi obblighi in carico alle pubbliche amministrazioni, nonché quanto riportato al paragrafo "Accesso esterno al patrimonio documentale", si propongono i seguenti casi, vincolanti solo in assenza di manuale di AOO:

1) Atto pervenuto per errore su caselle di PEC o PEO integrate nel SdP: il protocollo si rifiuta motivando che trattasi di errato recapito ma indicando altresì, quello ritenuto corretto, al fine di non appesantire il procedimento amministrativo, come da art. 2 della L. n. 241/1990.
2) Atto pervenuto per errore su caselle di PEC o PEO non integrate nel SdP: o si comunica al mittente l'incompetenza, indicando l'indirizzo corretto a cui trasmettere la documentazione, oppure si procede al c.d. "inoltro informato", vale a dire che il destinatario del documento mal recapitato inoltra il messaggio di posta al destinatario corretto, mettendo in copia al messaggio l'indirizzo del mittente che ha confezionato erroneamente la spedizione telematica degli atti, perché i seguiti possano essere correttamente recapitati e gestiti.
3) Atto pervenuto per errore in modalità cartacea: qualora non sia possibile evincere dalle indicazioni sulla busta quale sia l'articolazione o ufficio competente si procede preliminarmente all'apertura della busta, si individua l'ufficio competente e si consegna la documentazione agli incaricati della consegna o all'ufficio di smistamento di posta cartacea centralizzato, con indicazione dell'ufficio ritenuto competente. Se dalle indicazioni della busta ancora chiusa è possibile risalire al corretto destinatario si procede analogamente senza aprire la busta.

5.2 DOCUMENTI IN USCITA

I documenti in uscita sono il risultato di un workflow proprio di ciascuna AOO che può essere dettagliato nel proprio manuale. Il flusso documentale in uscita da una AOO non può mai essere cartaceo o analogico e quindi, solo digitale o "misto", come da art. 40 del CAD.

I documenti amministrativi aventi rilevanza esterna contengono almeno le seguenti informazioni:

- In intestazione: denominazione e logo dell'AOO mittente;
- a piè di pagina: indirizzo completo dell'amministrazione sia nella versione civica (via, numero, CAP, città, provincia) che elettronica (indirizzo di posta elettronica certificata e ordinaria dell'AOO);
- i- l'oggetto, recante le informazioni essenziali sul contenuto della nota espresse in modo sintetico;

Costituiscono ulteriori elementi opzionali, i riferimenti/codici dell'estensore o Responsabile del Procedimento; da inserire in intestazione o a piè di pagina il codice fiscale, il codice IPA o il Codice univoco per la fatturazione elettronica. Altre regole per la determinazione dei contenuti e per la definizione della struttura dei documenti informatici possono essere fissate dalla singola AOO nel proprio Manuale di Gestione.

Per i documenti in uscita la UO protocollante:

a) esegue le verifiche di conformità allo standard di cui sopra;
b) verifica la corretta indicazione del mittente e del destinatario, l'avvenuta sottoscrizione e la presenza degli eventuali allegati dichiarati;
c) registra il documento nel protocollo generale generando la segnatura;
d) in caso riscontri irregolarità negli elementi di cui alle precedenti lett. a, b, c) restituisce la nota alla UO proponente con le osservazioni del caso e provvede alla trasmissione a mezzo PEC/interoperabilità, una volta risolte le problematiche;
e) trasmette il documento primario e suoi eventuali allegati. Se le loro dimensioni superano quella massima consentita o dal SdP in uso o dalle specifiche tecniche degli strumenti di posta elettronica, il SdP segnala con un messaggio l'impossibilità di invio. In questo caso il documento informatico viene copiato su idoneo supporto digitale e trasmesso al destinatario secondo modalità condivise con l'UO proponente;
f) Collega gli eventuali documenti correlati e richiamati nel testo, già presenti nel protocollo della AOO. L'operazione evidenzia con immediatezza la concatenazione tra più atti di uno stesso affare (per es. riscontro a note in entrata). Nel caso di collegamento, le regole di visibilità sono le stesse dell'accesso stabilito in origine sui singoli documenti.

Qualora fosse necessaria la spedizione di documenti per raccomandata, la UOP specificherà sempre sulla cartolina di ritorno il numero di protocollo cui ci si riferisce e l'articolazione o l'UO proponente a cui la cartolina dovrà essere restituita, ponendo la massima cura nell'operazione per evitarne lo smarrimento.

5.3 DOCUMENTI INTERNI

Sono atti interni quelli nei quali mittente e destinatario appartengono entrambi all'AOO.

Possono essere:

- di natura prevalentemente informativa;
- di natura prevalentemente giuridico-probatoria.

I documenti interni di natura informativa quali mere comunicazioni interne scambiate tra uffici, richieste di materiale di cancelleria, richieste di interventi di manutenzione PC, non vanno protocollati. Di regola, lo scambio di tali documenti avviene per mezzo della posta elettronica. I documenti interni di natura prevalentemente giuridico-probatoria, ossia gli atti redatti dal personale di Giustizia nell'esercizio delle proprie funzioni, volti a documentare le attività istruttorie di competenza, possono essere protocollati.
Il registro per i documenti interni può contenere pertanto, circolari e disposizioni generali in quanto documenti fondamentali per la gestione dei procedimenti amministrativi.
Nel Manuale di AOO sono definite eventuali, ulteriori specificazioni di quanto sopra, visto che la registrazione a protocollo di tali atti non è obbligatoria per legge, ma utile ai fini procedimentali, o sotto il profilo organizzativo.

6 CRITERI DI ASSEGNAZIONE

A seconda del tipo, della materia e della rilevanza, i documenti, dopo la registrazione, devono essere portati all'attenzione di risorse opportunamente profilate sul SdP e quindi nell'organigramma almeno di una AOO/UO in cui sono configurabili diversi livelli gerarchici, per i seguiti di competenza. Ogni documento, in entrata, in uscita o interno, può essere assegnato per competenza oppure per conoscenza ad una o più unità organizzative e/o a singole risorse. L'assegnazione per competenza individua il soggetto responsabile della trattazione della pratica e ne determina la presa in carico.
Una assegnazione può determinare l'attribuzione a diversi soggetti (UO oppure singole risorse) sia della competenza che della conoscenza di un determinato atto. È sempre necessario che per ogni affare documentale, ci sia almeno un soggetto competente della conseguenziale trattazione.
Per questo motivo ogni risorsa di Giustizia è tenuta alla consultazione quotidiana del protocollo.
Il sistema di protocollo informatico consente in qualunque momento di verificare chi è assegnatario di un documento. Ogni AOO può definire specifici criteri e modalità operative per assegnare i documenti a chi deve prenderli in carico, nel proprio Manuale.

6.1 LIVELLI DI ASSEGNAZIONE

L'ufficio, unità o incaricato di protocollo della AOO può rendere disponibili gli atti protocollati in entrata secondo uno dei seguenti modelli di cui si dà conto in questo Manuale o in quello di AOO:

MODELLO 1

Assegnazione di I livello: i documenti in ingresso sono assegnati al vertice della AOO (titolare, sua Segreteria o UOP).

Assegnazione di II livello: questo provvede ad assegnarli ai Responsabili di UO, ai Coordinatori di Gruppi di Lavoro o a Referente di Servizi.
Assegnazione di III livello: questi provvederanno poi al loro smistamento finale assegnando la competenza e la conoscenza del documento alle risorse ritenute competenti della trattazione o della evasione dell'affare.

MODELLO 2

Assegnazione di I livello: i documenti in ingresso sono assegnati da incaricati dal vertice della AOO ai Responsabili di UO, ai Coordinatori di Gruppi di Lavoro o a Referente di Servizi.
Assegnazione di II livello: questi provvederanno poi al loro smistamento finale assegnando la competenza e la conoscenza del documento alle risorse ritenute competenti della trattazione o della evasione dell'affare.

MODELLO 3

Assegnazione di I livello: i documenti in ingresso sono assegnati da incaricati dal vertice della AOO ai Responsabili di UO, ai Coordinatori di Gruppi di Lavoro o a Referente di Servizi, sulla base di una dettagliata matrice di attribuzione di compiti e funzioni costantemente aggiornata, direttamente alle risorse ritenute competenti della trattazione o della evasione dell'affare.

In assenza di determinazioni a riguardo, opportunamente riportate nel Manuale di AOO, è da applicarsi il **MODELLO 1**.

7 CLASSIFICAZIONE E FASCICOLAZIONE

Registrazione, segnatura di protocollo e classificazione sono individuate dalla normativa vigente come operazioni necessarie per la corretta tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni[10].
Di seguito è illustrato il sistema di classificazione dei documenti, di formazione del fascicolo e consultazione dell'archivio.

7.1 CARATTERISTICHE GENERALI

La classificazione dei documenti amministrativi è un'operazione prevista dall'articolo 56 del TUDA, che consente al singolo Ufficio di organizzare gli atti amministrativi secondo un ordine logico in relazione alle funzioni ed alle competenze dell'AOO nonché di renderne agevole l'identificazione e la tracciabilità all'interno dell'archivio documentale. Le operazioni di classificazione si svolgono utilizzando il piano di classificazione, o titolario, all'interno del quale è possibile creare fascicoli

[10] Cfr. artt. 56, 64 c.4, 68 c.1 TU documentazione amministrativa – Dpr 445/2000

elettronici. Il documento può essere associato alla voce corrispondente (operazione di classificazione) ed inserito in un fascicolo o sotto fascicolo elettronico (operazione di fascicolazione). Si possono associare allo stesso documento più voci di classifica, in funzione delle attività nell'ambito delle quali il documento protocollato viene trattato.
La classificazione non è legata necessariamente al momento della registrazione di protocollo: in ogni momento della lavorazione è possibile effettuare, modificare o integrare la classificazione associata al documento protocollato.

7.2 PIANO DI CLASSIFICAZIONE O TITOLARIO

Il piano di classificazione o titolario per ciascuna AOO il cui elenco è in **ALLEGATO 6**, è il "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'AOO, al quale viene ricondotta la molteplicità dei documenti prodotti"[11]
Si suddivide in Funzioni, Macroattività, Attività, più comunemente dette "voci di I, II e III livello".
Per ciascuna tipologia di AOO, il titolario già caricato nel SdP è definito, revisionato ed aggiornato centralmente. Nel caso in cui vengano apportate modifiche, l'onere di informare, nelle modalità ritenute adeguate, tutti i soggetti abilitati alla classificazione dei documenti e di impartire istruzioni per il corretto uso è in capo al RSP della singola AOO.

7.3 FASCICOLAZIONE

La fascicolazione è l'operazione, conseguente alla classificazione, mediante la quale ogni documento registrato nel protocollo viene inserito, all'interno del titolario d'archivio, nel fascicolo di riferimento o all'occorrenza in sotto fascicoli. La creazione e alimentazione dei fascicoli elettronici ha la funzione di garantire l'ordinata sequenza degli atti procedimentali, in quanto il sistema provvede all'ordinamento cronologico dei documenti.
La creazione di fascicoli è demandata, di regola, ai soggetti che ricevono gli atti per competenza, individuati nel manuale di gestione di AOO, secondo le scelte organizzative interne e, per quanto possibile, nel rispetto di quanto stabilito nel modello di titolario. Si evidenzia l'importanza della corretta individuazione di tali figure all'interno dell'AOO, per evitare ridondanze nella creazione dei fascicoli ed ottenere un patrimonio documentale ordinato.
Qualora un documento dia luogo all'avvio di più procedimenti amministrativi o pratiche, potrà essere assegnato a più fascicoli.
I fascicoli esprimono una relazione amministrativa tra i documenti che sono destinati ad esservi contenuti. I criteri di formazione sono indicati nel modello di titolario e possono essere diversi, ad esempio:

[11] Paola Carucci, *Le fonti archivistiche: ordinamento e conservazione*, Roma, NIS, 1983 (Beni culturali, 10) p.229

- per persona fisica/giuridica. Il ciclo di vita del fascicolo (apertura e chiusura) segue quello del rapporto giuridico che lega la persona fisica o giuridica all'Amministrazione;
- per serie documentale, quando trattasi di documenti della stessa tipologia es. contratti, verbali e circolari, ordini di servizio etc.;
- per procedimento amministrativo. In questo caso il contenuto del fascicolo segue il flusso del procedimento, incamerando via via tutti gli atti procedimentali prodotti.

All'interno dei fascicoli possono essere creati sotto fascicoli destinati a contenere atti relativi a particolari aspetti dell'affare trattato nel fascicolo principale. In questo caso, di regola, nessun atto dovrà essere inserito nel fascicolo padre, ma tutti gli atti saranno sistemati nei sotto fascicoli appropriati.
Criteri più dettagliati di organizzazione del patrimonio documentale in fascicoli e sotto fascicoli rispetto al modello di titolario della AOO, possono essere esplicitati nel manuale di AOO.

7.4 CICLO DI VITA DEL FASCICOLO

L'apertura del fascicolo è l'operazione compiuta dalle persone abilitate alla sua creazione. Di regola avviene quando un documento dia luogo all'avvio di una nuova pratica, un nuovo flusso di lavoro o un nuovo procedimento amministrativo, in base all'organizzazione e al modello di titolario previsto per la AOO. Il fascicolo viene creato agganciandolo all'ultimo livello della struttura gerarchica del titolario ed inserendo nel sistema le seguenti informazioni:

- oggetto del fascicolo, seguendo gli standard elaborati dall'AOO
- eventuale riferimento alla collocazione fisica dei documenti originali cartacei
- livello di riservatezza, se differente da quello ordinario del sistema

Il sistema fornisce automaticamente la segnatura del fascicolo, comprendente funzione, macroattività, attività, numero progressivo e data di apertura del fascicolo.
I soggetti abilitati alla fascicolazione, ricevuto un documento protocollato, devono verificare se risulta già esistente un fascicolo di pertinenza ed in tal caso procedere al semplice inserimento in esso. In alternativa procederanno all'apertura di un nuovo fascicolo.
Al termine del procedimento amministrativo o all'esaurimento dell'affare è buona norma procedere all'operazione di chiusura del fascicolo.

7.5 PROCESSO DI ASSEGNAZIONE DEI FASCICOLI

L'assegnatario in competenza di un documento protocollato o eventuale incaricato, verifica se il documento attiene ad un affare o procedimento in corso per il quale esiste già un fascicolo ed in tal caso lo inserisce.
Se non è ancora stato creato il fascicolo riferito al procedimento o affare, si procede alla creazione ed alla adeguata denominazione del nuovo fascicolo. Il titolario di AOO costituisce guida rispetto alla

creazione del fascicolo ed ulteriori indicazioni potranno essere formulate nel Manuale di gestione di AOO.
La gestione ottimale di un procedimento amministravo o di una pratica comporta la creazione di un fascicolo unico con permessi di accesso a tutti gli incaricati dello stesso affare. Nel manuale di AOO devono essere formulate le regole di visibilità dei fascicoli.
Il responsabile del fascicolo procede, ove necessario, alla trasmissione, all'assegnazione ed all'eventuale rettifica di assegnazione del fascicolo.

8 ACCESSO AL PATRIMONIO DOCUMENTALE

8.1 LIVELLI DI ACCESSO INTERNO AL PATRIMONIO DOCUMENTALE

Gli utenti interni possono accedere alla documentazione di protocollo in funzione del proprio ruolo all'interno dell'AOO, del conseguente profilo assegnato nel sistema e delle abilitazioni concesse.
I documenti non fascicolati sono visibili agli assegnatari, a coloro che li hanno ricevuti in conoscenza o trasmissione ed ai superiori gerarchici
Le regole di accesso ai documenti si conformano ai differenti livelli di accesso che gli utenti hanno in relazione agli affari trattati nel rispetto della riservatezza prevista dalle norme vigenti.
L'accesso per la ricerca all'intero archivio documentale corrente è prerogativa del responsabile di AOO e del RSP, che possono servirsi della UOP per l'esecuzione materiale della ricerca. Ogni UO/risorsa può procedere alle ricerche sulla porzione di archivio documentale assegnato.

8.2 ACCESSO ESTERNO AL PATRIMONIO DOCUMENTALE

Secondo il principio di trasparenza, la normativa prevede che i soggetti esterni possano accedere alla documentazione dell'AOO; in particolare si fa riferimento alle prerogative previste nella legge 241/90 s.m.i., nonché all'istituto dell'accesso civico generalizzato D.Lgs. 33/2013 come modificato dal D.Lgs. 97/2016.
Il soggetto esterno può avviare un procedimento che inizia con l'atto di richiesta e si conclude, in via ordinaria, con l'esibizione, cioè l'operazione che consente di visualizzare il documento conservato o di estrarne copia. Talvolta si tratta di ottenere un estratto per riassunto ovvero un documento nel quale si attestano, in maniera sintetica ma esaustiva, fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici. In particolare, la normativa prevede prerogative e diritti per il cittadino che intenda accedere alla documentazione della P.A. L'UOP è il primo interlocutore sia per chi intenda esercitare il diritto di accesso ai sensi della L. 241/90 e successive modifiche sia per la ricezione di istanze di accesso civico generalizzato ai sensi del D.Lgs. 33/2013, come modificata dal D.Lgs. 97/2016. Le istanze dovranno essere prese in carico dal servizio di protocollo, che le tratterà secondo le disposizioni degli uffici deputati a gestire queste tipologie di richiesta.

9 IL REGISTRO DI EMERGENZA

9.1 IL REGISTRO DI EMERGENZA

Laddove per cause tecniche si determini l'impossibilità di utilizzare il SdP per oltre ventiquattro ore, va attivato il registro di emergenza secondo i termini e le modalità di seguito specificati.

1) Per eventi di rilevanza nazionale l'attivazione del registro di emergenza e la comunicazione formale dell'avvenuto ripristino, sono disposte dal Direttore Generale per i Sistemi Informativi Automatizzati o, in subordine, dal Coordinatore della Gestione Documentale o dal Dirigente dell'ufficio DGSIA presso cui è incardinata la gestione applicativa del servizio di protocollo.
2) Per eventi di rilevanza locale lo stato di emergenza e la comunicazione formale dell'avvenuto ripristino, sono disposte dal titolare della AOO o dal RSP. Di ciò va data pronta comunicazione al Coordinatore ministeriale della gestione documentale di Ente ed al Direttore Generale SIA.

In conseguenza della dichiarazione dello stato di emergenza, l'Amministratore di AOO attiva il registro di emergenza, fino alla comunicazione formale dell'avvenuto ripristino funzionale del sistema di protocollo informatico.

Al ripristino delle funzionalità del sistema, le informazioni relative ai documenti protocollati in emergenza sono inserite senza ritardo nel sistema informatico, utilizzando l'apposita funzione di recupero dei dati. Nelle more resta disabilitata la protocollazione agli operatori dei registri che non siano di emergenza.

Durante la fase di ripristino, a ciascun documento protocollato nel registro di emergenza viene attribuito un numero di protocollo del sistema informatico ordinario; il sistema provvede a mantenerne stabilmente la correlazione con il numero utilizzato in emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo ordinario.

Per la decorrenza dei termini del procedimento amministrativo si fa riferimento alla data in cui è stata effettuata la protocollazione sul registro di emergenza, assicurando in tal modo la corretta sequenza dei documenti che ne fanno parte.

Terminato l'import, si potrà riprendere la protocollazione di routine.

La numerazione del registro di emergenza si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre.

9.2 MODALITÀ DI APERTURA DEL REGISTRO DI EMERGENZA

Per le finalità di cui sopra, prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, è necessario che l'Amministratore di AOO ed il RSP verifichino ed abbiano contezza della correttezza della data e dell'ora evidenziata dal client di registro di emergenza su cui occorre operare, e che ne curino il reset laddove necessario.

Il registro di emergenza si attiva invocando un client installato su alcune macchine, formalmente individuate (almeno due e non più di quattro per ogni AOO) di cui una individuata come MASTER.
La prima registrazione di emergenza DEVE riferirsi al provvedimento di autorizzazione di apertura del registro di emergenza, di cui sopra.
L'ultima registrazione di emergenza DEVE riferirsi alla ripristinata disponibilità del SdP.
Entrambe devono essere protocollate SOLO sulla postazione MASTER.
Ad import chiuso, il RSP formalizza la chiusura dell'emergenza, ed il relativo atto va inserito nel protocollo ordinario, come primo atto indicativo della ripresa ordinaria del servizio di gestione documentale.

9.3 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.
Il formato delle registrazioni di protocollo è lo stesso previsto per il protocollo generale, rispettandone l'obbligatorietà dei campi di registrazione.
I documenti protocollati in emergenza, dopo il trasferimento al SdP, risulteranno in carico alla UO protocollante, che ne ha effettuato il trasferimento. Sarà necessario, quindi, assegnarli all'Ufficio competente e procedere alla loro classificazione e fascicolazione.

10 MISURE DI SICUREZZA

Idonee misure tecniche e organizzative funzionali a garantire la sicurezza applicativa ed infrastrutturale del protocollo informatico e del sistema di gestione documentale nel suo complesso, sono stabilite e presidiate dall'Ufficio della DGSIA titolare dell'esecuzione dei contratti di sviluppo e manutenzione del SdP.
I fornitori dei servizi di cui trattasi sono resi edotti delle strategie ministeriali in materia di sicurezza informatica per il tramite delle figure deputate al presidio dell'esecuzione contrattuale [Responsabile Unico del Procedimento (RUP) e Direttore dell'Esecuzione (DEC)].
Lo sviluppo e la manutenzione del SdP sono adeguati alla normativa di settore vigente e quindi assicurano la corretta gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici.
Quanto sopra è finalizzato a garantire che:

- i documenti e le informazioni trattati dall'Ente/AOO siano disponibili ed integri.
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme

alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

L'amministrazione titolare dei dati, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati eventuali limiti e condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente, anche mediante la stipula di apposite convenzioni di servizio.

Coerentemente con le disposizioni del Codice disciplinare del personale non dirigente di cui CCNL 2016 -2018 Funzioni Centrali, artt. 60- 66, tutti gli utenti del sistema di protocollo sono tenuti a non divulgare, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica. Costituiscono eccezione le informazioni che, per loro natura o per espressa indicazione del mittente, siano destinate ad essere rese pubbliche.

In particolare, gli addetti alla UOP o a qualunque UO con facoltà di protocollo, osservano al riguardo la massima cautela e sono tenuti ad utilizzare le informazioni alle quali accedono esclusivamente per la compilazione dei campi di registrazione e per le funzioni agli stessi affidati. Fuori da questo ambito non devono duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica.

In ALLEGATO 4 si riportano ulteriori politiche di sicurezza.

11 DISPOSIZIONI TRANSITORIE

Le regole del presente Manuale non si applicano ai documenti gestiti con registri applicativi diversi da quelli previsti dal SdP.

Dalla data di efficacia del presente Manuale, decadono le disposizioni interne ed i regolamenti interni delle AOO con esso contrastanti.

Laddove i sistemi attualmente in uso non dispongano della tecnologia per attuare quanto indicato dalle norme, le AOO hanno facoltà di adottare soluzioni alternative sul piano organizzativo, dandone riscontro nel proprio Manuale.

Il Manuale utente per l'uso del client del protocollo emergenziale sarà comunicato da DGSIA, con separata nota, entro il 31.04.2021.

12 EFFICACIA DEL MANUALE DI ENTE

Le disposizioni presente Manuale saranno efficaci a far data dall'01.07.2021.

ALLEGATO 1 – RIFERIMENTI NORMATIVI

- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate sul sito web istituzionale dell'AGID in data 11.09.2020.
- Decreto del Presidente del Consiglio dei ministri 31 ottobre 2000 – "*Regole tecniche per il Protocollo Informatico di cui al DPR 428/98*"
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 "*Disposizioni legislative in materia di documentazione amministrativa*" (TUDA)
- Decreto del Presidente del Consiglio dei ministri 13 gennaio 2004 – "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*"
- Decreto Legislativo 7 marzo 2005, n. 82. – "*Codice dell'Amministrazione digitale*" (CAD)
- Decreto del Presidente del Consiglio dei ministri 22 luglio 2011 – "*Comunicazioni con strumenti informatici tra imprese e Amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*"
- Decreto del Presidente del Consiglio dei ministri 3 dicembre 2013: "*Regole tecniche per il protocollo informatico*"
- Circolare AgID n. 62 del 30 aprile 2013: "*Documento informatico - Linee guida per il contrassegno generato elettronicamente"*
- Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 "*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 –bis, 23 –ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*" contenente, tra l'altro, regole tecniche per la conservazione
- Regolamento AgID per l'adozione di *Linee Guida per l'attuazione del Codice dell'Amministrazione Digitale*.

Posta elettronica certificata

- Circolare AIPA 7/5/2001 n. 28 - "*Regole tecniche per l'interoperabilità dei sistemi di protocollo informatico*"
- Decreto del Presidente della Repubblica 11 febbraio 2005, n.68. – "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata*"
- Circolare n. 1/2010/DDI – "*Uso della Posta Elettronica Certificata nelle amministrazioni pubbliche*"
- Regolamento UE 679/2016.
- Regolamento eIDAS n. 910/2014

Firma elettronica

- Decreto legislativo 23 gennaio 2002, n. 10 – "*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*"
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137 – "*Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002*"
- Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 – "*Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici*"
- Linee guida AgID 20/06/2019 contenenti le "*Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*".

Sicurezza

- Decreto legislativo n.196 del 30 giugno 2003 – "*Codice in materia di protezione dei dati personali*": norme per l'attuazione nelle Pubbliche Amministrazioni delle disposizioni relative alla gestione delle risorse umane, con particolare riguardo ai soggetti che effettuano il trattamento
- "GDPR" Regolamento Europeo 2016/679 – normativa in materia di protezione dati personali.

Amministrazione giudiziaria

- Decreto 23 aprile 2020 recante *Misure necessarie al coordinamento informativo ed operativo tra la Direzione generale per i sistemi informativi automatizzati del Dipartimento dell'Organizzazione giudiziaria, del personale e dei servizi e altre articolazioni del Ministero della Giustizia, nonché concernente l'individuazione degli uffici di livello dirigenziale non generale e la definizione dei relativi compiti ai sensi dell'art. 16 c1 e c2 del D.P.C.M. n. 84/2015 e dell'art.6, co. 2, del D.P.C.M. n. 99/2019*
- Decreto del Presidente del Consiglio dei ministri 15 giugno 2015, n. 84 "*Regolamento di riorganizzazione del MdG e riduzione degli uffici dirigenziali e delle dotazioni organiche*"
- Circolare Capo di Gabinetto 2018 sul tema dell'accesso civico generalizzato
- Decreto 10 maggio 2018 – "*Modificazioni ai decreti del Ministro della giustizia 14 dicembre 2015 e 19 gennaio 2016 in tema di ridefinizione dei compiti della Direzione generale per i sistemi informativi automatizzati del Dipartimento dell'Organizzazione giudiziaria, del personale e dei servizi per i sistemi di multivideoconferenza*".

ALLEGATO 2 - DEFINIZIONI E ACRONIMI

DEFINIZIONI

Amministrazione	MdG
Archivio	Complesso organico di documenti, fascicoli e aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici, aggregazioni documentali informatiche, gestiti e conservati in ambiente informatico
Classificazione	Organizzazione logica di documenti secondo uno schema articolato in voci rappresentative di aggregazioni logiche/funzioni individuate attraverso specifici metadati
Coordinatore della Gestione Documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Documento	È una rappresentazione di atti, fatti o dati giuridicamente rilevanti.
Documento amministrativo	Si intende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale. Vedasi l'articolo 22, comma 1, lettera d) della Legge n. 241/1990
Documento analogico	Si intende un documento formato utilizzando supporti fisici (carta, film, nastri magnetici etc).

Documento informatico	Si intende "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Documento ordinario e corrente	Si intendono atti che non afferiscono all'esercizio di un potere autoritativo, di spesa (documenti contabili) o di rappresentanza (documenti legali o atti di visibilità istituzionale come Protocolli d'Intesa, Accordi Quadro, Convenzioni) o di gestione delle risorse umane e strumentali.
Documenti in entrata/ricevuto	Documenti acquisiti dalla AOO con diversi mezzi e modalità in base sia alla modalità di trasmissione scelta dal mittente sia alla natura del documento.
Documenti in uscita/trasmesso	Documenti redatti dalle UO delle AOO e trasmessi a terzi, aventi rilevanza esterna
Documento di rilevanza esterna	Qualunque documento ricevuto/trasmesso da/a altro Ente/AOO, altra persona fisica o giuridica.
Documenti di rilevanza interna	I documenti che a qualunque titolo sono scambiati tra uffici e/o gruppi di lavoro, commissioni della stessa AOO
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività, di uno specifico procedimento e raccolti per procedimento, per serie, per affare. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice
Manuale di conservazione	Atto che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
Manuale di gestione	Manuale di descrizione del sistema di gestione documentale. Esso descrive le funzionalità disponibili e le prassi in essere, agli addetti al servizio e ai soggetti esterni che a diverso titolo, interagiscono con l'amministrazione

Massimario di scarto	Strumento che descrive le informazioni relative ai tempi, ai criteri e alle regole per la conservazione, selezione e scarto della documentazione archiviata
Originale di un documento	di un documento amministrativo analogico: la versione definitiva corredata di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa. di un documento amministrativo informatico:
Sistema di protocollo informatico	L'applicativo in uso all'Amministrazione per implementare il servizio di protocollo informatico
Registro di protocollo	Registro informatico degli atti e dei documenti ricevuti ed inviati dall'Amministrazione, consentendone l'identificazione univoca all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Registro particolare	Registro informatico degli atti e dei documenti ricevuti ed inviati dall'Amministrazione, afferenti a particolari tipologie documentali, previsto dall'articolo 53, comma 5, del D.P.R. 28 dicembre 2000, n. 445 come deputato alla registrazione di atti non di competenza del protocollo informatico. L'istituzione dei registri particolari è autorizzata dall'Amministrazione. Il ruolo generale civile e il ruolo generale penale sono esempi di registri particolari nel sistema giudiziario.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1, del D.p.c.m. 3 dicembre 2013 recante le "Regole tecniche in materia di sistema di conservazione"

Responsabile della protezione dei dati	Dipendente del titolare del trattamento o del responsabile del trattamento o altro soggetto che in base a un contratto di servizi, vigila sull'osservanza del Regolamento UE 679/2016
Responsabile del procedimento amministrativo	Incaricato che ha la responsabilità amministrativa dell'esecuzione degli adempimenti relativi ad un provvedimento amministrativo,
Responsabile del trattamento dei dati	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 4 n. 8 del Regolamento UE 679/2016
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Titolario di classificazione	Strumento che descrive l'organizzazione della documentazione prodotta o ricevuta in settori e categorie, schematizzando in maniera logica le sue competenze e funzioni

ACRONIMI

AOO	Area organizzativa omogenea definita come un insieme di unità organizzative dell'Amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali.
CAD	Codice dell'amministrazione digitale Decreto legislativo 7 marzo 2005, n. 82 e ss.mm.ii.
UO	Unità organizzativa - Ufficio componente di una AOO che, per tipologia di mandato istituzionale e competenza, di funzione amministrativa perseguita, di obiettivi e attività svolta, presenta esigenze di gestione unitaria e coordinata della documentazione
UOP	Unità Organizzative di registrazione di Protocollo – ovvero ufficio che svolge attività di registrazione di protocollo
MdG	MdG
DGSIA	Direzione generale dei sistemi Informativi Automatizzati del MdG

IPA	Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi
PI	Protocollo Informatico
PA	Pubblica Amministrazione
PP.AA.	Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
SdP	Servizio di protocollo informatico
RSP	Responsabile del Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali di una AOO
RPA	Responsabile del Procedimento Amministrativo
GDPR	General Data Protection Regulation Regolamento europeo generale sulla protezione dei dati n. 2016/679
AgID	Agenzia per l'Italia Digitale
TUDA	Testo Unico per la Documentazione Amministrativa D.P.R. 28 dicembre 2000, n. 445 e ss.mm.ii.
DPCM	Decreto del Presidente del Consiglio dei Ministri
CIRC	Circolare
DPR	Decreto del Presidente della Repubblica
PDG	Provvedimento del Direttore Generale

ALLEGATO 3 - FORMATI DEI DOCUMENTI INFORMATICI AMMESSI

Salvo i casi in cui, in relazione a specifici flussi documentali, vi siano particolari previsioni normative, provvedimenti del Coordinatore di Ente o istruzioni operative per la fruizione di servizi telematici che dispongano diversamente, il MdG assicura l'accettazione dei documenti elettronici inviati ai suoi uffici tramite posta elettronica, posta elettronica certificata e altri canali telematici oppure consegnati direttamente su supporti informatici quando sono prodotti in uno dei seguenti formati:

- .pdf (compreso il formato PDF/A);
- .gif, .jpg, .tif;
- OOOXML - Office Open XML (principali estensioni: .docx, .xlsx, .pptx);
- Open Document Format;
- .txt (codifica Unicode UTF 8);
- .zip (a condizione che i file contenuti all'interno del file compresso siano prodotti in uno dei formati previsti nel presente elenco);
- .p7m (documenti firmati digitalmente con sottoscrizione di tipo CADES e a condizione che i file originali oggetto di sottoscrizione digitale siano prodotti in uno dei formati previsti nel presente elenco).

In ogni caso i documenti elettronici inviati o consegnati agli uffici del MdG dovranno essere privi di elementi attivi, tra cui macro e campi variabili.

Il MdG si riserva comunque la facoltà di non accettare documenti informatici prodotti in formati che consentano la modifica dei contenuti (.doc, .txt et alia)

ALLEGATO 4 - ULTERIORI POLITICHE DI SICUREZZA

Il Piano della Sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio e archiviazione elettronica dei documenti è parte del più ampio Piano Strategico per la Sicurezza Informatica del Ministero della Giustizia che viene periodicamente aggiornato annualmente da DGSIA.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Protocollo

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'applicativo utile a informatizzare il servizio di protocollo, sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al SdP o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati presenti sul SdP;
- perdita dei documenti e dei dati contenuti nel SdP;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, DGSIA adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Requisiti minimi di sicurezza applicativa

Con nota avente prot. n. 6281.I dell'01.06.2020, l'Amministrazione nell'ambito dell'esecuzione dei contratti di sviluppo in essere, ha assicurato la compliance del SdP alle seguenti misure:

1. Il sistema di protocollo deve essere conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).
2. Il sistema di protocollo deve assicurare l'accesso sia dalla propria postazione di lavoro connessa in rete locale che da remoto, secondo stringenti condizioni di sicurezza
3. Il sistema di protocollo deve assicurare l'accesso per il tramite di credenziali già disponibili alla risorsa ministeriale (c.d. "di ADN")
4. Il sistema di protocollo deve assicurare la protezione della sessione di lavoro dell'utente. In particolare, devono essere attivati meccanismi non più deboli dei seguenti:
    a) la comunicazione tra la stazione di lavoro e i sistemi di elaborazione che realizzano il Servizio di Protocollo è crittografata tramite il protocollo SSL a 128 bit;
    b) è configurato un time-out per la disconnessone automatica delle utenze dal servizio dopo 30 minuti di inattività;
    c) non sono consentite le sessioni multiple con la stessa user-id.
5. Il sistema di protocollo deve assicurare soddisfare i seguenti requisiti:
    a) garanzia della disponibilità, riservatezza e integrità dei documenti e del registro di protocollo;
    b) garanzia della corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
    c) possibilità di reperimento delle informazioni riguardanti i documenti registrati;

d) accesso in sicurezza alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
e) garanzia della corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato.

6. Il sistema di protocollo deve assicurare che Titolare e Responsabile del Trattamento dei dati personali possano trattare tutti i dati personali raccolti e trattati perché contenuti nei documenti elettronici oggetto del servizio di Protocollo e/o di Scrivania digitale siano trattati solo per le finalità proprie dell'applicativo e della gestione e manutenzione sua e dell'infrastruttura ospitante.
7. Il servizio di protocollo assicurare la disponibilità delle registrazioni di sicurezza rappresentate da:
   a) dai log di sistema generati dal sistema operativo;
   b) dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall), se disponibili;
   c) dalle registrazioni del sistema di Protocollo.
8. Il sistema di protocollo deve assicurare la disponibilità di almeno i seguenti livelli di autorizzazione per l'accesso alle funzioni del sistema di Protocollo:
   a) abilitazione alla consultazione;
   b) abilitazione all'inserimento;
   c) abilitazione alla cancellazione;
   d) abilitazione alla modifica delle informazioni;
   e) abilitazione all'annullamento delle registrazioni;
   f) abilitazioni alla classificazione dei documenti.

Sicurezza della rete di accesso al servizio

La Rete Unitaria di Giustizia è protetta da una rete di circa 600 firewall.
Questa robusta protezione perimetrale assicura la messa in sicurezza delle comunicazioni Untrusted che avvengono tra l'esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura.
I server su cui alloggia il SdP è in una zona filtro, denominata "DMZ".
Le contromisure necessarie per proteggere le comunicazioni che avvengono all'interno dell'organizzazione sono attuate tramite l'adozione di un dominio di Active Directory e a un sistema centralizzato di Antivirus.
Da un punto di vista generale, qualsiasi accesso esterno alla rete ministeriale ed in particolare al protocollo, può costituire una minaccia per l'organizzazione.
Tuttavia, la necessità di avere costantemente a disposizione i dati e documenti ministeriali, anche quando non è possibile fisicamente accedere al SdP dall'interno della RUG, impone l'utilizzo di tecnologie in grado di fornire un accesso diretto al SdP con connessioni da qualsiasi punto del mondo ed indipendentemente dall'orario locale. Per far fronte a tale necessità si è strutturato un sistema che prevede l'inserimento all'interno della DMZ di un reverse proxi come ulteriore protezione dal WEB per permettere l'accesso remoto al portale di protocollazione.
Il SdP è alloggiato su storage e server ad alta affidabilità costantemente aggiornato e manutenuto.

Accesso non autorizzato a computer e reti informatiche

L'accesso a computer e reti informatiche è normalmente autorizzato solo per i soggetti che superano un processo di autenticazione dell'utente, inteso come il riconoscimento dell'identità dichiarata, via ADN.

Accesso al SdP da parte di utenti interni all'AOO

L'accesso di cui trattasi avviene attraverso l'utilizzo di credenziali di autenticazione c.d. di ADN;
i profili di abilitazione alle funzionalità del SdP sono attribuiti a ciascun utente sulla base di quanto stabilito dal titolare della AOO e dal RSP. Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione/autenticazione (ADN), il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente. Alle risorse incaricate a vario titolo per l'accesso al SdP è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno otto caratteri, tra cui almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare. La Password deve essere modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza semestrale. L'User-Id non è assegnato a nessun altro incaricato per nessuna motivazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità (intesa come efficacia sulla sicurezza) che consente all'incaricato l'accesso ai dati personali. Qualora l'utente medesimo dimenticasse la propria Password si procederà all'assegnazione di una nuova chiave di accesso. Gli incaricati a vario titolo al SdP non devono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento dei documenti ministeriali.
Le credenziali di accesso al SdP di ciascun operatore devono essere consegnate in busta chiusa e sigillata al RSP. In caso di prolungata assenza o impedimento del **soggetto incaricato del trattamento di specifici documenti di una certa rilevanza** e qualora **si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema**, il RSP è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere al trattamento, comunicandolo al titolare.
Di ciò va depositata a protocollo una relazione a firma del RSP che dettagli quanto sopra in grassetto.
Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della Password, provvedendo all'inserimento della stessa in altra busta sigillata da riconsegnare al suddetto RSP.

Formazione e sottoscrizione dei documenti

I documenti dell'AOO sono prodotti utilizzando i formati previsti dalle Linee Guida di cui in premessa e dall'ALLEGATO 3 del presente Manuale. L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il formato PDF); l'acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche. L'apposizione delle varie tipologie di sottoscrizioni elettroniche, l'apposizione della firma digitale, nonché la validazione temporale del documento sottoscritto digitalmente deve avvenire in conformità a quanto sancito dalle richiamate Linee guida emanate

ai sensi dell'art. 71 del D. Lgs. 82/05. La sottoscrizione del documento con firma digitale deve avvenire prima dell'effettuazione della registrazione di protocollo.

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato alla protocollazione. L'accesso in consultazione al registro di protocollo è consentito sulla base dell'organizzazione dell'AOO: di norma, ciascun operatore è abilitato ad accedere esclusivamente ai documenti e ai dati di protocollo dei documenti che ha prodotto, che gli sono stati assegnati o, comunque, di competenza del proprio ufficio di riferimento. Ogni registrazione di protocollo viene memorizzata dal SdP unitamente all'identificativo univoco dell'autore che l'ha eseguita insieme alla data e l'ora della stessa. Eventuali modifiche, autorizzate nei termini e nelle modalità fissate dal presente manuale, vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il SdP mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione. Il SdP non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il SdP manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnato da autorizzazione scritta del RSP e il SdP deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione o la motivazione dell'annullamento. L'impronta digitale del documento informatico, associata alla registrazione di protocollo del medesimo è generata utilizzando una funzione di hash, conforme a quanto previsto dalla normativa vigente. Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il SdP permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale. Il SdP consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il SdP consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate. Il Sistema e tutti i documenti e/o dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici dannosi in quanto è impegno costante di DGSIA, attraverso l'attività del Centro Gestione Firewall, del Tavolo per la Governance della Sicurezza Informatica di Giustizia e l'attuazione del Piano Strategico per la sicurezza informatica ministeriale, il rendere ragionevolmente sicuri gli accessi al SdP ed alla RUG e quindi a tutti i documenti e dati in esso contenuti. Ciò anche in virtù del presidio del processo di apertura delle porte in uscita (LAN to WAN) del firewall che avviene esclusivamente verso indirizzi preventivamente individuati da personale interno qualificato.

Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dal SdP e dagli applicativi ministeriali, vengono costantemente tenuti aggiornati per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Il Backup dei dati contenuti nel SdP su supporti mobili rizzati i dati sensibili o giudiziari, quando presenti, devono essere custoditi, sotto chiave, a cura del RSP al fine di evitare accessi non autorizzati e trattamenti non

consentiti. Cessato lo scopo per cui sono stati memorizzati, se non riscrivibili devono essere necessariamente distrutti, se riscrivibili possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.
Il backup full dei dati del SdP deve consentire, attuando best practise vigenti, il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, entro 24/36 ore lavorative in caso di generico malfunzionamento, entro 72 ore lavorative in caso di disastro (si ricorda che va redatto il Piano di Continuità Operativa e Disaster Recovery del SdP).

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno di AOO o tra AOO del Ministero, deve avvenire esclusivamente per mezzo del SdP; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati. La trasmissione di documenti informatici al di fuori del MdG avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo.

Piani formativi del personale

In conformità a quanto disposto dall'art. 13 del D.lgs. 82/2005, ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione, DGSIA rappresenterà alle articolazioni competenti in materia la necessità di predispone apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del SdP;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali.

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

L'amministratore di Ente del SdP controlla mensilmente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.
Il Coordinatore Ministeriale della gestione documentale effettua periodiche verifiche sul corretto funzionamento del SdP.

Misure di tutela e garanzia

Qualora DGSIA o il MdG adotti misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione, riceverà dall'installatore una descrizione scritta dell'intervento che ne attesti la conformità alle disposizioni di cui alla normativa di settore vigente.

ALLEGATO 5 - ESTRATTO DEL CODICE AURORA

VEDASI SEPARATO FILE

ALLEGATO 6 - ELENCO DELLE AOO DEL MINISTERO DELLA GUSTIZIA

VEDASI SEPARATO FILE

ALLEGATO 7 – NOMINA DEL COORDINATORE MINISTERIALE

VEDASI SEPARATO FILE