Allegato 12

Elenco delle principali tipologie di documenti della Pubblica Amministrazione soggetti alle norme sulla privacy (GDPR)

Manuale di gestione documentale dell'archivio e del protocollo

Le Pubbliche Amministrazioni (PA) raccolgono, archiviano e trattano quotidianamente una vasta gamma di documenti contenenti dati personali, spesso di natura sensibile o giudiziaria. Questi dati riguardano cittadini, dipendenti pubblici e soggetti che interagiscono con gli enti per accedere a servizi essenziali come sanità, istruzione, assistenza sociale, fiscalità e sicurezza pubblica.

La gestione di queste informazioni è disciplinata dal Regolamento Generale sulla Protezione dei Dati (GDPR - Regolamento UE 2016/679) e dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018). Le PA hanno l'obbligo di garantire che il trattamento dei dati sia conforme ai principi di liceità, correttezza, trasparenza, minimizzazione e sicurezza, assicurando il rispetto dei diritti degli interessati, come il diritto di accesso, rettifica e cancellazione dei propri dati.

L'accesso ai documenti amministrativi deve sempre bilanciare il principio di trasparenza con la tutela della privacy. In alcuni casi, la diffusione di determinate informazioni può essere limitata o soggetta a misure di anonimizzazione per proteggere le persone coinvolte.

Di seguito è riportato un elenco delle principali tipologie di documenti gestiti dalle Pubbliche Amministrazioni che contengono dati personali e sono quindi soggetti alle normative sulla protezione della privacy.

1. **Documenti Anagrafici e di Stato Civile**
   - Certificati di nascita, matrimonio, morte
   - Documenti di residenza e cittadinanza
   - Codice fiscale e documenti identificativi
2. **Documenti Sanitari**
   - Cartelle cliniche
   - Referti medici e diagnosi
   - Certificati di invalidità
   - Dati relativi a vaccinazioni
3. **Documenti del Personale Dipendente e Collaboratori**
   - Contratti di lavoro e atti di nomina
   - Buste paga e dati previdenziali
   - Valutazioni di performance e disciplinari
   - Permessi e certificati medici
4. **Documenti Fiscali e Tributari**
   - Dichiarazioni dei redditi
   - Atti di riscossione e cartelle esattoriali
   - Agevolazioni fiscali e contributi pubblici
5. **Documenti Scolastici ed Educativi**
   - Registri scolastici con dati su studenti e famiglie
   - Atti di esami e valutazioni
   - Documenti relativi a BES (Bisogni Educativi Speciali) e disabilità
6. **Documenti Giudiziari e di Sicurezza**
   - Atti di polizia e indagini
   - Ordinanze di protezione
   - Atti relativi a misure cautelari
7. **Documenti di Assistenza Sociale**
   - Pratiche per contributi economici (es. reddito di cittadinanza)
   - Dati su minori in affido o adozione
   - Interventi di assistenza per persone fragili
8. **Documenti di Accesso e Partecipazione ai Servizi Pubblici**
   - Richieste di accesso agli atti
   - Istanza di partecipazione a concorsi pubblici
   - Domande per alloggi popolari

I documenti gestiti contengono diversi livelli di dati personali, alcuni dei quali particolarmente sensibili e soggetti a rigorose misure di protezione previste dal GDPR. A seconda della loro natura, questi dati possono essere comuni, sensibili (categorie particolari di dati, come quelli sanitari) o giudiziari (legati a procedimenti legali).

Di seguito è riportato un elenco delle principali tipologie di documenti amministrativi con l'indicazione del livello di sensibilità dei dati trattati, per evidenziare la necessità di adeguate misure di sicurezza e tutela della privacy.

1) **Documenti Anagrafici e di Stato Civile**
    a) **Dati personali comuni** (nome, cognome, data e luogo di nascita, codice fiscale, residenza, cittadinanza)
    b) **Dati sensibili (categorie particolari di dati)** solo in casi specifici (es. atti di riconoscimento di figli naturali o cambi di genere)

2) **Documenti Sanitari**
    a) **Dati sensibili (categorie particolari di dati)** (cartelle cliniche, referti medici, disabilità, vaccinazioni, dati genetici e biometrici)
    b) **Dati giudiziari**, se relativi a certificazioni di inabilità derivanti da procedimenti legali

3) **Documenti del Personale Dipendente e Collaboratori**
    a) **Dati personali comuni** (contratti di lavoro, dati anagrafici, retribuzioni)
    b) **Dati sensibili (categorie particolari di dati)** (certificati medici, assenze per malattia, permessi per disabilità)
    c) **Dati giudiziari**, se presenti procedimenti disciplinari o condanne

4) **Documenti Fiscali e Tributari**
    a) **Dati personali comuni** (dichiarazioni dei redditi, cartelle esattoriali, dati patrimoniali)
    b) **Dati sensibili**, se connessi a esenzioni per motivi di salute o altre condizioni particolari
    c) **Dati giudiziari**, in caso di pignoramenti o contenziosi fiscali

5) **Documenti Scolastici e Educativi**

a) **Dati personali comuni** (registri scolastici, esiti di valutazioni)

b) **Dati sensibili**, se relativi a studenti con BES (Bisogni Educativi Speciali), DSA o disabilità

c) **Dati giudiziari**, se riguardano provvedimenti disciplinari con impatto legale

6) **Documenti Giudiziari e di Sicurezza**

a) **Dati giudiziari** (indagini di polizia, misure cautelari, ordinanze di protezione)

b) **Dati sensibili**, se connessi a situazioni di salute o fragilità (es. vittime di violenza, minori a rischio)

7) **Documenti di Assistenza Sociale**

a) **Dati personali comuni** (domande di contributi, assegni di sostegno)

b) **Dati sensibili**, se connessi a condizioni di salute, disabilità o situazioni di disagio sociale

c) **Dati giudiziari**, in caso di affidi, tutela minori o provvedimenti giudiziari per situazioni familiari critiche

8) **Documenti di Accesso e Partecipazione ai Servizi Pubblici**

a) **Dati personali comuni** (istanze di accesso agli atti, richieste per concorsi pubblici)

b) **Dati sensibili**, se contenenti informazioni su condizioni di salute (es. richieste di esoneri o agevolazioni)

c) **Dati giudiziari**, in caso di verifiche su requisiti di onorabilità nei concorsi pubblici

Questi livelli di sensibilità richiedono misure di protezione adeguate, come crittografia, accessi limitati e procedure di anonimizzazione quando necessario.