MODULO ONLINE

Concorso
ISTRUTTORE AMMINISTRATIVO ENTI LOCALI CAT.C
QUIZ COMMENTATI

MOD. I - Privacy e Amministrazione Digitale

Tutte le materie richieste nei concorsi più recenti:
Diritto Costituzionale • Diritto Amministrativo • Ordinamento degli Enti Locali • Pubblico Impiego e Responsabilità Contabilità Pubblica • Contratti Pubblici (D.Lgs. 36/2023 e correttivi 2024–25) • Trasparenza, Anticorruzione e PIAO Privacy e Amministrazione Digitale • Logica e Ragionamento Inglese Base • Reati contro la Pubblica Amministrazione • Glossario e Modulistica Comunale

TUTTA **LA TEORIA SPIEGATA** IN MODO **SEMPLICE** E **CONCRETO**

iltuo concorso

01. Secondo il Regolamento UE 2016/679 (GDPR) e il D.Lgs. 10/2023, quale dei seguenti principi richiede che i dati personali siano trattati in modo da garantire un'adeguata sicurezza?

A) Principio di liceità

B) Principio di integrità e riservatezza

C) Principio di trasparenza

Risposta corretta: B

Commento: La risposta corretta è la B. Il principio di integrità e riservatezza, sancito dall'art. 5, par. 1, lett. f) del GDPR, richiede che i dati personali siano "trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali". Questo principio è stato ulteriormente rafforzato dal D.Lgs. 10/2023, che ha armonizzato la normativa italiana sulla protezione dei dati personali con il GDPR, abrogando il precedente D.Lgs. 101/2018. In particolare, il D.Lgs. 10/2023 ha introdotto misure più stringenti per garantire la sicurezza dei dati trattati dalle PA, anche in relazione alla crescente digitalizzazione. Il principio di liceità (risposta A) riguarda invece la necessità che il trattamento abbia una base giuridica legittima, mentre il principio di trasparenza (risposta C) attiene all'informazione chiara e completa all'interessato sul trattamento dei suoi dati.

02. Quale figura, secondo la normativa vigente, è designata dal titolare del trattamento per assicurare che il trattamento dei dati personali avvenga conformemente al GDPR all'interno di un'organizzazione?

A) Il Responsabile della Protezione dei Dati (RPD/DPO)

B) Il Responsabile del Trattamento

C) L'Amministratore di Sistema

Risposta corretta: A

Commento: La risposta corretta è la A. Il Responsabile della Protezione dei Dati (RPD), o Data Protection Officer (DPO) in inglese, è la figura prevista dagli artt. 37-39 del GDPR che deve essere designata dal titolare del trattamento per assicurare che il trattamento dei dati personali avvenga conformemente al Regolamento. La sua nomina è obbligatoria per tutte le autorità pubbliche, inclusi gli enti locali, indipendentemente dalla loro dimensione. Il D.Lgs. 10/2023 ha ulteriormente precisato i requisiti per questa figura, sottolineando la necessità di competenze specifiche in materia

di protezione dei dati e indipendenza nello svolgimento dei compiti. Il Responsabile del Trattamento (risposta B) è invece un soggetto esterno che tratta dati personali per conto del titolare (ad esempio un fornitore di servizi cloud), mentre l'Amministratore di Sistema (risposta C) è una figura tecnica con compiti operativi sui sistemi informatici, che non ha necessariamente responsabilità specifiche in materia di protezione dei dati personali nel senso inteso dal GDPR.

03. Quale principio del GDPR impone di raccogliere solo i dati personali necessari alle finalità per le quali sono trattati?

A) Limitazione della conservazione

B) Minimizzazione dei dati

C) Esattezza

Risposta corretta: B

Commento: La risposta corretta è la B. Il principio di minimizzazione dei dati, stabilito dall'art. 5, par. 1, lett. c) del GDPR, prevede che i dati personali siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". Questo principio richiede ai titolari del trattamento di raccogliere e trattare solo i dati strettamente necessari al raggiungimento delle finalità dichiarate, evitando trattamenti eccessivi o non pertinenti. Il D.Lgs. 10/2023 ha rafforzato questo principio, prevedendo specifiche sanzioni per i trattamenti eccessivi, soprattutto nell'ambito delle pubbliche amministrazioni. Il principio di limitazione della conservazione (risposta A) riguarda invece la durata della conservazione dei dati, che non deve eccedere il tempo necessario al raggiungimento delle finalità. Il principio di esattezza (risposta C) attiene invece alla necessità che i dati siano aggiornati e corretti.

04. Secondo il CAD (D.Lgs. 82/2005) aggiornato al 2025, quale dei seguenti documenti NON può essere oggetto di istanza digitale da parte del cittadino?

A) Certificato di residenza

B) Documento con firma olografa soggetto a specifiche disposizioni di legge

C) Certificato di attribuzione del codice fiscale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 65 del Codice dell'Amministrazione Digitale (CAD), come modificato dalle riforme fino al 2025, le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica sono valide se sottoscritte mediante firma digitale o qualificata, SPID, CIE o altre modalità previste. Tuttavia, alcuni documenti che richiedono una

firma olografa in base a specifiche disposizioni normative non possono essere oggetto di istanza puramente digitale, richiedendo ancora procedure ibride o fisiche. Gli aggiornamenti normativi del 2024-2025 hanno ulteriormente ridotto queste eccezioni, ma alcune permangono per specifici atti notarili, testamenti, procure speciali e altri documenti che la legge richiede espressamente in forma scritta con firma autografa. Il certificato di residenza (risposta A) e il certificato di attribuzione del codice fiscale (risposta C) possono invece essere richiesti completamente in modalità digitale attraverso i portali delle amministrazioni o tramite l'App IO, come previsto dalle più recenti disposizioni sul completamento della transizione digitale.

05. In base al CAD aggiornato al 2025, quali caratteristiche deve avere il domicilio digitale del cittadino?

A) Deve essere necessariamente un indirizzo PEC o un servizio elettronico di recapito certificato qualificato

B) Può essere un qualsiasi indirizzo email ordinario comunicato alla PA

C) Deve essere esclusivamente un indirizzo PEC fornito gratuitamente dalla PA

Risposta corretta: A

Commento: La risposta corretta è la A. Secondo l'art. 6-quater del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, il domicilio digitale del cittadino deve essere un indirizzo di Posta Elettronica Certificata (PEC) o un servizio elettronico di recapito certificato qualificato (SERCQ), conforme agli standard europei. La scelta di questi strumenti è legata alla necessità di garantire l'opponibilità a terzi, la certezza della consegna e del contenuto delle comunicazioni. Le riforme del 2023-2025 hanno ampliato le possibilità, includendo anche i SERCQ conformi al Regolamento eIDAS, ma hanno mantenuto il requisito della certificazione legale della consegna. La risposta B è errata perché un indirizzo email ordinario non garantisce le caratteristiche legali richieste per il domicilio digitale. La risposta C è errata perché, sebbene esistano iniziative per fornire domicili digitali gratuiti ai cittadini, il CAD non prevede che il domicilio digitale debba essere esclusivamente un indirizzo PEC fornito gratuitamente dalla PA.

06. Secondo la normativa vigente, come devono essere gestiti i documenti informatici da parte di un Comune?

A) È sufficiente conservarli in qualsiasi formato digitale per il periodo previsto dalla legge

B) Devono essere formati, gestiti e conservati secondo le Linee Guida AgID, garantendo autenticità, integrità e leggibilità nel tempo

C) Devono essere tutti stampati e conservati anche in formato cartaceo

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo gli artt. 40-44 del CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate al 2024, i documenti informatici devono essere formati, gestiti e conservati in modo da garantirne nel tempo l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità. Questo implica l'utilizzo di formati idonei alla conservazione a lungo termine (come PDF/A), metadati adeguati, sistemi di classificazione e fascicolazione conformi al piano di classificazione (titolario), e un sistema di conservazione a norma. Le riforme 2024-2025 hanno ulteriormente rafforzato questi requisiti, prevedendo anche l'interoperabilità tra i sistemi documentali delle diverse PA. La risposta A è errata perché non è sufficiente conservare i documenti in qualsiasi formato digitale, ma occorre rispettare standard specifici. La risposta C è errata perché, secondo il principio del "digital first" sancito dal CAD, le amministrazioni formano e conservano i propri documenti come originali informatici, senza necessità di stampa e conservazione cartacea (salvo eccezioni specifiche).

07. Nel contesto dell'amministrazione digitale, cosa si intende per "once only"?

A) Il principio secondo cui il cittadino deve interfacciarsi con una sola amministrazione per ogni procedimento

B) Il principio secondo cui il cittadino deve comunicare una sola volta i propri dati alla PA, che li riutilizzerà nei diversi procedimenti

C) L'obbligo di conservare i documenti informatici in un'unica copia

Risposta corretta: B

Commento: La risposta corretta è la B. Il principio "once only" (una volta sola) è un principio fondamentale dell'amministrazione digitale, sancito a livello europeo dal Regolamento UE 2018/1724 e recepito nel CAD all'art. 50, che prevede che il cittadino debba comunicare una sola volta i propri dati alla pubblica amministrazione, la quale li riutilizzerà nei diversi procedimenti attraverso l'interoperabilità delle banche dati. L'obiettivo è ridurre gli oneri amministrativi a carico dei cittadini e delle imprese, evitando richieste multiple degli stessi dati. Gli aggiornamenti normativi

2024-2025 hanno rafforzato l'applicazione di questo principio, imponendo alle amministrazioni di acquisire d'ufficio le informazioni già in possesso di altre PA, attraverso il sistema di interoperabilità PDND (Piattaforma Digitale Nazionale Dati). La risposta A è errata perché il principio non riguarda l'interfacciarsi con una sola amministrazione, ma il fornire i dati una sola volta. La risposta C è errata perché non si riferisce alla conservazione dei documenti.

08. In base alla normativa sulla privacy aggiornata al 2025, quando un Comune deve effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA)?

A) Solo quando tratta dati biometrici o genetici

B) Sempre prima di ogni trattamento di dati personali

C) Quando un trattamento presenta rischi elevati per i diritti e le libertà delle persone fisiche, in particolare con l'uso di nuove tecnologie

Risposta corretta: C

Commento: La risposta corretta è la C. Secondo l'art. 35 del GDPR, confermato e ulteriormente specificato dal D.Lgs. 10/2023, la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è obbligatoria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, in particolare se utilizza nuove tecnologie. Esempi specifici includono: valutazioni sistematiche e automatizzate di aspetti personali, trattamento su larga scala di categorie particolari di dati, sorveglianza sistematica di zone accessibili al pubblico. Le Linee Guida del Garante Privacy, aggiornate nel 2024, hanno fornito un elenco di trattamenti per i quali la DPIA è obbligatoria, con particolare riferimento agli enti locali (ad esempio, videosorveglianza estesa, geolocalizzazione dei dipendenti, sistemi di welfare con profilazione). La risposta A è errata perché la DPIA non è limitata ai soli dati biometrici o genetici, sebbene questi richiedano spesso una DPIA. La risposta B è errata perché la DPIA non è necessaria per ogni trattamento, ma solo per quelli a rischio elevato.

09. Secondo la normativa vigente, cosa si intende per "identità digitale"?

A) Esclusivamente le credenziali SPID rilasciate dai gestori accreditati

B) La rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale

C) Solo la Carta d'Identità Elettronica (CIE) rilasciata dal Ministero dell'Interno

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 1, comma 1, lett. u-quater) del CAD, come aggiornato dalle riforme fino al 2025, l'identità digitale è "la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale". Questo concetto è più ampio rispetto ai singoli strumenti che la implementano. Le modifiche normative del 2024 hanno ulteriormente ampliato questa definizione, includendo anche gli attributi derivati e verificati che caratterizzano l'utente all'interno del sistema. La risposta A è errata perché SPID (Sistema Pubblico di Identità Digitale) è solo uno degli strumenti di identità digitale, insieme alla CIE, alla CNS (Carta Nazionale dei Servizi) e, dal 2024, all'European Digital Identity Wallet previsto dal nuovo Regolamento eIDAS 2.0. La risposta C è errata perché la CIE è solo uno degli strumenti che implementano l'identità digitale, non l'identità digitale in sé.

10. In base al CAD aggiornato al 2025, quali caratteristiche deve avere un documento informatico per avere l'efficacia della scrittura privata prevista dall'art. 2702 del codice civile?

A) Deve essere redatto su carta e poi scansionato

B) Deve essere formato nel rispetto delle Linee guida AgID e sottoscritto con firma digitale, qualificata o avanzata, o con altro tipo di firma elettronica riconducibile all'autore

C) È sufficiente che sia creato con un normale programma di videoscrittura e salvato in formato PDF

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 20, comma 1-bis, del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile quando è formato nel rispetto delle Linee guida AgID, e vi è apposta una firma digitale, qualificata o avanzata, o un altro tipo di firma elettronica purché sia possibile accertare la provenienza e l'integrità del documento. Le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate nel

2024, specificano i requisiti tecnici per garantire validità e efficacia probatoria ai documenti informatici. La risposta A è errata perché un documento scansionato (copia per immagine) non ha automaticamente l'efficacia della scrittura privata, a meno che non sia sottoscritto con firma digitale. La risposta C è errata perché non è sufficiente il semplice formato PDF senza una firma elettronica valida per garantire l'efficacia di scrittura privata.

11. Quale dei seguenti NON è un diritto dell'interessato previsto dal GDPR e dal D.Lgs. 10/2023?

A) Diritto alla portabilità dei dati

B) Diritto di accesso ai dati personali

C) Diritto al risarcimento automatico in caso di qualsiasi violazione

Risposta corretta: C

Commento: La risposta corretta è la C. Il "diritto al risarcimento automatico in caso di qualsiasi violazione" non è un diritto previsto dal GDPR. L'art. 82 del GDPR prevede sì un diritto al risarcimento per danni materiali o immateriali causati da una violazione del Regolamento, ma questo non è automatico: richiede la dimostrazione del danno subito e del nesso causale con la violazione, secondo i normali principi della responsabilità civile. Il D.Lgs. 10/2023 ha confermato questo approccio, specificando ulteriormente le modalità di esercizio di tale diritto nell'ordinamento italiano. Il diritto alla portabilità dei dati (risposta A) è invece un diritto effettivamente previsto dall'art. 20 del GDPR, che consente all'interessato di ricevere i dati personali che lo riguardano in un formato strutturato e di trasmetterli ad un altro titolare. Analogamente, il diritto di accesso ai dati personali (risposta B) è garantito dall'art. 15 del GDPR, che permette all'interessato di ottenere conferma del trattamento e copia dei dati personali oggetto di trattamento.

12. Secondo il CAD aggiornato al 2025, cosa si intende per "riuso del software"?

A) L'utilizzo di software piratati per risparmiare sui costi

B) La possibilità per le PA di utilizzare e modificare senza oneri software sviluppati per conto e a spese di altre amministrazioni

C) La pratica di riutilizzare i vecchi computer dell'amministrazione

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 69 del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, il "riuso del software" consiste nella possibilità per le pubbliche amministrazioni di utilizzare e modificare senza oneri programmi informatici o parti di

essi sviluppati per conto e a spese di altre amministrazioni, adattandoli alle proprie esigenze. Le Linee Guida AgID sul riuso del software, aggiornate nel 2024, hanno ulteriormente specificato le modalità operative, prevedendo l'obbligo di rilasciare il software con licenza aperta e di pubblicarlo nel catalogo nazionale del riuso gestito da AgID. La riforma 2024 ha introdotto anche sanzioni per le amministrazioni che sviluppano software senza renderli disponibili per il riuso. La risposta A è errata perché il riuso non ha nulla a che fare con software piratati o illegali. La risposta C è errata perché il riuso riguarda il software, non l'hardware.

13. In base al GDPR e al D.Lgs. 10/2023, quando un Comune può trattare dati personali per l'esecuzione di un compito di interesse pubblico senza richiedere il consenso dell'interessato?

A) Mai, il consenso è sempre necessario

B) Quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

C) Solo quando tratta dati di pubblici dipendenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 6, par. 1, lett. e) del GDPR, il trattamento è lecito, senza necessità di consenso, quando "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Questa base giuridica è particolarmente rilevante per gli enti locali, che trattano dati personali principalmente nell'esercizio delle loro funzioni istituzionali. Il D.Lgs. 10/2023 ha confermato questa impostazione, specificando all'art. 2-ter che la base giuridica deve essere costituita da una norma di legge o, nei casi previsti dalla legge, di regolamento. Le Linee Guida del Garante Privacy per gli enti locali, aggiornate nel 2024, hanno fornito esempi concreti di trattamenti basati su questa condizione di liceità (ad esempio, anagrafe, stato civile, tributi locali). La risposta A è errata perché il consenso non è sempre necessario, esistendo altre basi giuridiche come quella descritta. La risposta C è errata perché questa base giuridica si applica a tutti i dati personali necessari all'esecuzione dei compiti istituzionali, non solo a quelli dei dipendenti.

14. Secondo il GDPR, quale delle seguenti informazioni NON deve essere necessariamente inclusa nell'informativa privacy fornita agli interessati?

A) L'identità e i dati di contatto del titolare del trattamento

B) Il curriculum vitae dettagliato del Responsabile della Protezione dei Dati

C) Il periodo di conservazione dei dati personali o i criteri utilizzati per determinarlo

Risposta corretta: B

Commento: La risposta corretta è la B. Il curriculum vitae dettagliato del Responsabile della Protezione dei Dati (RPD/DPO) non è un elemento che deve essere necessariamente incluso nell'informativa privacy secondo gli artt. 13 e 14 del GDPR. L'informativa deve includere i dati di contatto del RPD/DPO, ma non il suo curriculum vitae dettagliato. Il D.Lgs. 10/2023 e le Linee Guida del Garante Privacy sulle informative, aggiornate nel 2024, hanno confermato questi requisiti, introducendo anche modelli semplificati di informativa per alcune tipologie di trattamento. La risposta A è errata perché l'identità e i dati di contatto del titolare del trattamento sono informazioni obbligatorie ai sensi dell'art. 13, par. 1, lett. a) del GDPR. La risposta C è errata perché il periodo di conservazione dei dati o i criteri utilizzati per determinarlo sono informazioni obbligatorie ai sensi dell'art. 13, par. 2, lett. a) del GDPR.

15. Quale strumento, tra quelli elencati, è utilizzato per consentire ai cittadini di effettuare pagamenti elettronici verso le pubbliche amministrazioni?

A) SPID (Sistema Pubblico di Identità Digitale)

B) PagoPA

C) ANPR (Anagrafe Nazionale della Popolazione Residente)

Risposta corretta: B

Commento: La risposta corretta è la B. PagoPA è la piattaforma nazionale dei pagamenti elettronici verso le pubbliche amministrazioni, istituita dall'art. 5 del CAD e gestita dalla società PagoPA S.p.A. Consente ai cittadini e alle imprese di effettuare pagamenti elettronici verso le PA in modo standardizzato, attraverso molteplici canali e strumenti di pagamento (bonifico, carta di credito, ecc.). Gli aggiornamenti normativi 2024-2025 hanno ulteriormente potenziato la piattaforma, prevedendo l'integrazione con l'App IO e nuove funzionalità come la possibilità di rateizzare i pagamenti e di ricevere notifiche digitali relative agli avvisi di pagamento. La risposta A è errata perché SPID è il Sistema Pubblico di Identità Digitale, che consente l'accesso ai servizi online della PA ma non è uno strumento di pagamento. La risposta C è errata perché ANPR è l'Anagrafe

Nazionale della Popolazione Residente, la banca dati nazionale che ha sostituito le anagrafi comunali, ma non è uno strumento di pagamento.

16. In base alla normativa sulla privacy aggiornata al 2025, quale misura NON è obbligatoria in caso di data breach (violazione dei dati personali)?

A) Notifica al Garante Privacy entro 72 ore, se la violazione presenta rischi per i diritti e le libertà delle persone

B) Comunicazione agli interessati, se la violazione presenta un rischio elevato per i loro diritti e libertà

C) Pubblicazione obbligatoria di un comunicato stampa sui quotidiani nazionali

Risposta corretta: C

Commento: La risposta corretta è la C. La pubblicazione obbligatoria di un comunicato stampa sui quotidiani nazionali non è una misura prevista dalla normativa in caso di data breach. Secondo gli artt. 33 e 34 del GDPR, confermati e specificati dal D.Lgs. 10/2023, in caso di violazione dei dati personali il titolare del trattamento deve: 1) notificare la violazione all'autorità di controllo (Garante Privacy) entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti rischi per i diritti e le libertà delle persone; 2) comunicare la violazione all'interessato senza ingiustificato ritardo, quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Le Linee Guida del Garante Privacy sulla gestione dei data breach, aggiornate nel 2024, hanno ulteriormente dettagliato queste procedure, introducendo anche una piattaforma telematica per la notifica semplificata. La comunicazione può avvenire attraverso vari canali efficaci, ma non esiste un obbligo generalizzato di pubblicare comunicati stampa sui quotidiani nazionali.

17. Secondo il CAD aggiornato al 2025, qual è la differenza principale tra CIE (Carta d'Identità Elettronica) e CNS (Carta Nazionale dei Servizi)?

A) La CIE è un documento di riconoscimento con funzionalità di identificazione fisica e digitale, mentre la CNS è solo uno strumento di identificazione digitale

B) La CIE può essere rilasciata solo ai maggiorenni, mentre la CNS è disponibile per tutti

C) La CIE è valida solo in Italia, mentre la CNS è riconosciuta in tutta l'Unione Europea

Risposta corretta: A

Commento: La risposta corretta è la A. Secondo gli artt. 66 e 66-bis del CAD, come aggiornati

dalle riforme fino al 2025, la principale differenza tra CIE e CNS è che la Carta d'Identità Elettronica (CIE) è un documento di riconoscimento fisico con funzionalità di identificazione sia fisica che digitale, rilasciato dal Ministero dell'Interno tramite i Comuni, mentre la Carta Nazionale dei Servizi (CNS) è esclusivamente uno strumento di autenticazione digitale che contiene un certificato di autenticazione per l'accesso ai servizi online, ma non costituisce un documento di riconoscimento fisico. La CIE 3.0, introdotta nel 2016 e ulteriormente potenziata con gli aggiornamenti 2024, integra un microchip che consente sia l'identificazione a vista tramite i dati e la foto stampati sul supporto, sia l'autenticazione digitale. La risposta B è errata perché anche la CIE può essere rilasciata ai minori (con validità differenziata in base all'età). La risposta C è errata perché la CIE è valida come documento di viaggio in tutti i paesi dell'Unione Europea e in quelli con cui esistono specifici accordi.

18. In un Comune, quale delle seguenti operazioni richiede necessariamente l'utilizzo della firma digitale secondo il CAD aggiornato al 2025?

A) La semplice protocollazione di un documento in entrata

B) L'invio di una email ordinaria a un cittadino

C) L'adozione di un atto amministrativo in formato digitale che produce effetti verso terzi

Risposta corretta: C

Commento: La risposta corretta è la C. Secondo l'art. 24 del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, l'utilizzo della firma digitale è necessario per gli atti amministrativi in formato digitale che producono effetti verso terzi, in quanto sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere a ogni fine previsto dalla normativa vigente. Le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate nel 2024, hanno ulteriormente specificato che tutti gli atti amministrativi adottati dalle PA devono essere prodotti come documenti informatici nativi e firmati digitalmente. La risposta A è errata perché la semplice protocollazione di un documento in entrata non richiede necessariamente l'apposizione di firma digitale da parte dell'operatore che effettua la protocollazione (sebbene il sistema di protocollo utilizzi meccanismi di validazione). La risposta B è errata perché l'invio di una semplice email ordinaria non richiede firma digitale, a meno che non contenga documenti che necessitano di firma.

19. Secondo il GDPR e il D.Lgs. 10/2023, chi è il "titolare del trattamento" in un Comune?

A) Il Sindaco, in quanto rappresentante legale dell'ente

B) Il Responsabile della Protezione dei Dati (RPD/DPO)

C) L'ente Comune nel suo complesso, come persona giuridica

Risposta corretta: C

Commento: La risposta corretta è la C. Secondo l'art. 4, par. 1, punto 7 del GDPR, il titolare del trattamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". Nel caso di un Comune, il titolare del trattamento è l'ente nel suo complesso, come persona giuridica, e non le persone fisiche che operano al suo interno. Il D.Lgs. 10/2023 ha confermato questa interpretazione, specificando ulteriormente le responsabilità del titolare nelle PA. Il Garante Privacy, nelle sue Linee Guida per gli enti locali aggiornate nel 2024, ha chiarito che, sebbene le decisioni siano prese dagli organi dell'ente o dai funzionari delegati, la titolarità del trattamento rimane in capo all'ente come soggetto unitario. La risposta A è errata perché, sebbene il Sindaco sia il rappresentante legale dell'ente, non è personalmente il titolare del trattamento. La risposta B è errata perché il RPD/DPO è una figura di controllo e consulenza, non il titolare del trattamento.

20. Quale delle seguenti affermazioni sui registri delle attività di trattamento è corretta secondo il GDPR e il D.Lgs. 10/2023?

A) I registri devono essere tenuti solo dalle aziende private, non dagli enti pubblici

B) Il registro deve contenere elementi come le finalità del trattamento, le categorie di dati e di interessati, i destinatari, le misure di sicurezza adottate

C) Il registro è facoltativo per tutti gli enti con meno di 250 dipendenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 30 del GDPR, confermato dal D.Lgs. 10/2023, il registro delle attività di trattamento deve contenere: il nome e i dati di contatto del titolare, le finalità del trattamento, le categorie di interessati e di dati personali, le categorie di destinatari, gli eventuali trasferimenti verso paesi terzi, i termini previsti per la cancellazione delle diverse categorie di dati e una descrizione generale delle misure di sicurezza tecniche e organizzative adottate. Le Linee Guida del Garante Privacy, aggiornate nel 2024, hanno fornito modelli standard di registro e chiarito che questo strumento è fondamentale per dimostrare l'accountability del titolare. La risposta A è errata perché i registri devono essere tenuti sia dalle aziende private che dagli enti pubblici. La risposta C è errata perché, sebbene l'art. 30, par. 5 del GDPR preveda

un'esenzione per le organizzazioni con meno di 250 dipendenti, questa non si applica se il trattamento può presentare un rischio per i diritti e le libertà degli interessati, se riguarda dati particolari o relativi a condanne penali, o se non è occasionale. Gli enti pubblici, inclusi i Comuni, sono quindi sempre tenuti a mantenere il registro, indipendentemente dal numero di dipendenti.

21. Quale delle seguenti è una corretta definizione di "firma elettronica qualificata" secondo il CAD aggiornato al 2025?

A) Una firma elettronica avanzata che sia stata apposta utilizzando un certificato rilasciato da una qualsiasi azienda informatica

B) Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

C) Una firma autografa scannerizzata e inserita in un documento PDF

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 1, comma 1, lett. r-bis) del CAD, come aggiornato dalle riforme fino al 2025 in conformità con il Regolamento eIDAS (UE) 910/2014, la firma elettronica qualificata è "un particolare tipo di firma elettronica avanzata che è basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma". Questa definizione evidenzia i tre elementi caratteristici della firma elettronica qualificata: 1) deve essere una firma elettronica avanzata, quindi connessa in modo univoco al firmatario e in grado di identificarlo; 2) deve basarsi su un certificato qualificato, rilasciato da un prestatore di servizi fiduciari qualificato; 3) deve essere creata mediante un dispositivo sicuro per la creazione della firma (QSCD). Le Linee Guida AgID sulle firme elettroniche, aggiornate nel 2024, hanno ulteriormente dettagliato questi requisiti. La risposta A è errata perché il certificato deve essere qualificato e rilasciato da un prestatore di servizi fiduciari qualificato, non da una qualsiasi azienda informatica. La risposta C è errata perché una firma autografa scannerizzata non costituisce una firma elettronica qualificata, non garantendo né l'identificazione univoca del firmatario né l'integrità del documento.

22. Un istruttore amministrativo comunale deve inviare una comunicazione ufficiale a un cittadino. Secondo il CAD aggiornato al 2025, quale modalità è corretta?

A) Inviare sempre una raccomandata cartacea con ricevuta di ritorno

B) Utilizzare prioritariamente il domicilio digitale del cittadino e, solo in sua assenza, i mezzi tradizionali

C) Inviare una email ordinaria, indipendentemente dalla presenza di un domicilio digitale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 3-bis del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, le pubbliche amministrazioni, i gestori di servizi pubblici e le società a controllo pubblico devono utilizzare prioritariamente il domicilio digitale per le comunicazioni ai cittadini che lo hanno dichiarato. L'art. 6 del CAD stabilisce inoltre che le comunicazioni tramite domicilio digitale (PEC o servizio elettronico di recapito certificato qualificato) producono, quanto al momento della spedizione e di ricezione, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno. Solo in assenza di un domicilio digitale, le amministrazioni possono predisporre le comunicazioni ai cittadini in forma cartacea. La risposta A è errata perché il CAD impone la priorità della comunicazione digitale su quella cartacea. La risposta C è errata perché una email ordinaria non garantisce valore legale alla comunicazione e può essere utilizzata solo per comunicazioni informali, non per comunicazioni ufficiali che richiedono certezza di consegna.

23. Quale delle seguenti operazioni, relative alla gestione documentale di un Comune, è corretta secondo la normativa vigente?

A) La fascicolazione dei documenti è facoltativa e può essere effettuata solo per i procedimenti più complessi

B) Tutti i documenti informatici devono essere classificati e fascicolati secondo il piano di classificazione (titolario) dell'ente

C) La classificazione si applica solo ai documenti cartacei, non a quelli informatici

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate al 2024 in attuazione degli artt. 40-44 bis del CAD, tutti i documenti informatici devono essere classificati e fascicolati secondo il piano di classificazione (titolario) dell'ente. La classificazione e la fascicolazione sono attività obbligatorie e

fondamentali per la corretta gestione documentale, in quanto permettono di organizzare i documenti in modo sistematico, di collegarli ai relativi procedimenti e di garantirne la reperibilità nel tempo. Il manuale di gestione documentale, che ogni amministrazione deve adottare secondo l'art. 5 delle Linee Guida AgID, deve descrivere le regole per la classificazione e fascicolazione dei documenti. La risposta A è errata perché la fascicolazione non è facoltativa ma obbligatoria per tutti i documenti. La risposta C è errata perché la classificazione si applica a tutti i documenti, sia cartacei che informatici.

24. Secondo il GDPR e il D.Lgs. 10/2023, quale affermazione è corretta riguardo al trattamento di dati relativi a condanne penali da parte di un Comune?

A) È sempre vietato, senza eccezioni

B) È consentito solo se autorizzato da una norma di legge o regolamento che preveda garanzie appropriate

C) È sempre consentito, essendo il Comune una pubblica amministrazione

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 10 del GDPR e l'art. 2-octies del D.Lgs. 196/2003 (Codice Privacy), come modificato dal D.Lgs. 10/2023, il trattamento di dati relativi a condanne penali e reati o a connesse misure di sicurezza da parte di un soggetto pubblico è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati. Le Linee Guida del Garante Privacy per gli enti locali, aggiornate nel 2024, hanno fornito esempi concreti di trattamenti leciti in questo ambito (ad esempio: controlli antimafia, gestione del contenzioso, accesso agli atti amministrativi). La risposta A è errata perché questo tipo di trattamento non è assolutamente vietato, ma sottoposto a condizioni specifiche. La risposta C è errata perché l'essere una pubblica amministrazione non è sufficiente per trattare qualsiasi tipo di dato penale; è necessaria una specifica base giuridica che autorizzi il trattamento.

25. Un cittadino richiede a un Comune l'accesso ai propri dati personali ai sensi dell'art. 15 del GDPR. Entro quanto tempo l'ente deve rispondere secondo la normativa aggiornata al 2025?

A) 180 giorni dalla richiesta

B) 30 giorni dalla richiesta, prorogabili di ulteriori 60 giorni in casi di particolare complessità

C) 15 giorni non prorogabili

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 12, par. 3 del GDPR, confermato dal D.Lgs. 10/2023, il titolare del trattamento deve fornire all'interessato le informazioni relative all'esercizio dei suoi diritti (incluso l'accesso ai dati ai sensi dell'art. 15) senza ingiustificato ritardo e, comunque, al più tardi entro un mese (30 giorni) dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi (60 giorni), se necessario, tenuto conto della complessità e del numero delle richieste. In questo caso, il titolare deve informare l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta. Le Linee Guida del Garante Privacy sui diritti degli interessati, aggiornate nel 2024, hanno ribadito questi termini e fornito ulteriori indicazioni operative per le PA. La risposta A è errata perché indica un termine troppo lungo (180 giorni). La risposta C è errata perché indica un termine troppo breve (15 giorni) e non considera la possibilità di proroga prevista dal Regolamento.

26. In base al CAD aggiornato al 2025, quale delle seguenti affermazioni sul fascicolo informatico è corretta?

A) Il fascicolo informatico può contenere solo documenti informatici nativi, non copie informatiche di documenti cartacei

B) Il fascicolo informatico deve garantire la corretta collocazione, la facile reperibilità e la collegabilità dei documenti in relazione al procedimento, e può essere consultato ed alimentato da diverse amministrazioni

C) Il fascicolo informatico deve essere creato esclusivamente dal responsabile del procedimento e non può essere alimentato da altri soggetti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 41 del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, il fascicolo informatico riunisce gli atti, i documenti e i dati del procedimento da chiunque formati ed è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le

caratteristiche del fascicolo informatico sono ulteriormente specificate nelle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate nel 2024, che richiedono funzionalità che assicurino: l'identificazione univoca del fascicolo, la corretta collocazione nell'ambito del piano di classificazione, la facile reperibilità, la possibilità di collegare i documenti che ne fanno parte. La risposta A è errata perché il fascicolo informatico può contenere sia documenti informatici nativi sia copie informatiche di documenti analogici. La risposta C è errata perché, sebbene il fascicolo sia creato dal responsabile del procedimento, può essere alimentato anche da altri soggetti autorizzati, incluse altre amministrazioni coinvolte nel procedimento.

27. Secondo il Regolamento eIDAS e il CAD aggiornati al 2025, qual è la differenza principale tra firma elettronica e firma elettronica avanzata?

A) La firma elettronica è utilizzabile solo in Italia, mentre la firma elettronica avanzata è valida in tutta l'UE

B) La firma elettronica è gratuita, mentre la firma elettronica avanzata è a pagamento

C) La firma elettronica è una forma generica di identificazione, mentre la firma elettronica avanzata garantisce l'identificazione univoca del firmatario e l'integrità del documento

Risposta corretta: C

Commento: La risposta corretta è la C. Secondo il Regolamento eIDAS (UE) 910/2014 e l'art. 1, comma 1, lett. q) e lett. r) del CAD, come aggiornati fino al 2025, la firma elettronica è definita in modo generico come "dati in formato elettronico, allegati oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare", mentre la firma elettronica avanzata deve soddisfare requisiti specifici: essere connessa in modo univoco al firmatario, consentire l'identificazione del firmatario, essere creata con dati che il firmatario può utilizzare sotto il proprio controllo esclusivo, ed essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica. Le Linee Guida AgID sulle firme elettroniche, aggiornate nel 2024, hanno ulteriormente dettagliato questi requisiti e le differenze tra i vari tipi di firma. La risposta A è errata perché entrambe le tipologie di firma sono disciplinate dal Regolamento eIDAS e quindi riconosciute in tutta l'UE. La risposta B è errata perché il costo non è un elemento distintivo tra le due tipologie di firma.

28. Quale delle seguenti azioni, relative alla conservazione digitale dei documenti informatici, è corretta secondo la normativa vigente?

A) I documenti informatici possono essere conservati su qualsiasi supporto digitale, inclusi hard disk esterni non certificati

B) I documenti informatici devono essere conservati in un sistema di conservazione a norma, che garantisca autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo

C) I documenti informatici devono essere sempre stampati e conservati anche in formato cartaceo per garantirne la validità legale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo gli artt. 43 e 44 del CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate al 2024, i documenti informatici devono essere conservati in un sistema di conservazione a norma che garantisca autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo. Il processo di conservazione deve assicurare che i documenti informatici mantengano le caratteristiche di immodificabilità, autenticità e integrità nel tempo, attraverso l'uso di formati idonei (come PDF/A), metadati adeguati, riferimenti temporali opponibili a terzi, e misure di sicurezza appropriate. Il Responsabile della Conservazione, figura prevista dall'art. 44 del CAD, ha il compito di definire e attuare le politiche di conservazione. La risposta A è errata perché la conservazione su supporti non certificati non garantisce i requisiti normativi. La risposta C è errata perché il principio del "digital first" sancito dal CAD prevede la formazione e conservazione dei documenti come originali informatici, senza necessità di stampa e conservazione cartacea (salvo eccezioni specifiche).

29. Secondo la normativa sulla privacy aggiornata al 2025, cosa deve fare un istruttore comunale che riceve una richiesta di cancellazione dei dati personali (diritto all'oblio) da parte di un cittadino?

A) Deve sempre procedere immediatamente alla cancellazione di tutti i dati richiesti

B) Deve valutare se sussistono i presupposti per la cancellazione o se vi sono basi giuridiche che giustificano il mantenimento dei dati, come obblighi legali o interesse pubblico

C) Deve rifiutare la richiesta perché il diritto all'oblio non si applica alle pubbliche amministrazioni

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 17 del GDPR e le precisazioni del D.Lgs.

10/2023, quando un istruttore comunale riceve una richiesta di cancellazione dei dati personali (diritto all'oblio), deve valutare attentamente se sussistono i presupposti per accoglierla o se si applicano le eccezioni previste dall'art. 17, par. 3 del GDPR. In particolare, il diritto all'oblio non si applica se il trattamento è necessario: per l'adempimento di un obbligo legale; per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; per motivi di interesse pubblico nel settore della sanità pubblica; per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Le Linee Guida del Garante Privacy sui diritti degli interessati, aggiornate nel 2024, hanno fornito indicazioni operative su come gestire queste richieste, sottolineando che nelle PA spesso prevalgono le eccezioni legate all'interesse pubblico o agli obblighi legali. La risposta A è errata perché non sempre è possibile procedere alla cancellazione. La risposta C è errata perché il diritto all'oblio si applica anche ai dati trattati dalle PA, sebbene con le eccezioni previste.

30. In un Comune, quale misura tecnica e organizzativa è obbligatoria secondo il GDPR per garantire un livello di sicurezza adeguato al rischio nel trattamento dei dati personali?

A) Nominare sempre una guardia giurata che sorvegli l'ufficio protocollo

B) Adottare una politica di autenticazione sicura per l'accesso ai sistemi informatici, con username e password individuali, e implementare sistemi di backup regolari

C) Installare telecamere di sorveglianza in tutti gli uffici per monitorare l'operato dei dipendenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 32 del GDPR, confermato dal D.Lgs. 10/2023, il titolare del trattamento deve implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento. Tra queste misure, l'adozione di una politica di autenticazione sicura (con credenziali individuali, password robuste e periodicamente modificate) e l'implementazione di sistemi di backup regolari sono considerate basilari dalle Linee Guida del Garante Privacy sulla sicurezza dei dati, aggiornate nel 2024, e dai provvedimenti specifici per gli enti locali. Tali misure rispondono alla necessità di garantire la riservatezza, l'integrità e la disponibilità dei dati. La risposta A è errata perché, sebbene le misure di sicurezza fisica possano essere appropriate in alcuni contesti, la nomina di una guardia giurata per l'ufficio protocollo non è una misura obbligatoria secondo il GDPR. La risposta C è errata perché l'installazione di telecamere per monitorare l'operato dei dipendenti sarebbe sproporzionata e potrebbe violare altri diritti, come la dignità sul luogo di lavoro.

31. Un Comune intende attivare un sistema di videosorveglianza per motivi di sicurezza urbana. Quale delle seguenti affermazioni è corretta secondo la normativa sulla privacy aggiornata al 2025?

A) Non è necessario alcun adempimento specifico, essendo il trattamento effettuato per finalità di sicurezza urbana

B) È necessario effettuare una valutazione d'impatto sulla protezione dei dati (DPIA), installare cartelli informativi nelle aree videosorvegliate e definire tempi di conservazione limitati

C) È sufficiente installare i cartelli informativi, senza altri adempimenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 35 del GDPR, le Linee Guida del Comitato Europeo per la Protezione dei Dati (EDPB) e i provvedimenti del Garante Privacy aggiornati al 2024-2025, l'installazione di un sistema di videosorveglianza per motivi di sicurezza urbana richiede necessariamente una valutazione d'impatto sulla protezione dei dati (DPIA), essendo un trattamento che comporta il monitoraggio sistematico di una zona accessibile al pubblico su larga scala. Inoltre, secondo il principio di trasparenza, è obbligatoria l'installazione di cartelli informativi che segnalino la presenza delle telecamere e forniscano le informazioni essenziali sul trattamento. Infine, in base al principio di limitazione della conservazione, i tempi di conservazione delle immagini devono essere limitati a quanto strettamente necessario per le finalità di sicurezza (generalmente non oltre 7 giorni, salvo specifiche esigenze). Le Linee Guida sulla videosorveglianza per gli enti locali, emanate dal Garante Privacy e aggiornate nel 2024, hanno ulteriormente specificato questi adempimenti, prevedendo anche l'obbligo di adottare un regolamento comunale specifico. La risposta A è errata perché sono necessari specifici adempimenti. La risposta C è errata perché l'installazione dei soli cartelli informativi non è sufficiente.

32. Un Comune intende pubblicare all'albo pretorio online una determina dirigenziale che contiene dati personali dei beneficiari di un contributo sociale. Quale procedura è corretta secondo la normativa vigente?

A) Pubblicare il documento integrale senza alcuna limitazione, essendo un atto amministrativo

B) Pubblicare una versione con i dati personali oscurati o pseudonimizzati, mantenendo solo quelli essenziali al fine di trasparenza

C) Non pubblicare affatto la determina per evitare problemi di privacy

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 7-bis del D.Lgs. 33/2013 (Decreto Trasparenza) e l'art. 2-ter del D.Lgs. 196/2003 (Codice Privacy), come modificato dal D.Lgs. 10/2023, la pubblicazione di documenti contenenti dati personali all'albo pretorio online deve rispettare i principi di necessità, pertinenza e non eccedenza. Quando si tratta di dati relativi a beneficiari di contributi sociali, che possono rivelare informazioni sullo stato di disagio economico-sociale, è necessario adottare accorgimenti come l'oscuramento o la pseudonimizzazione, mantenendo solo i dati essenziali per il fine di trasparenza. Le Linee Guida del Garante Privacy sulla trasparenza e pubblicazione di atti, aggiornate nel 2024, hanno ulteriormente specificato che per questo tipo di dati è necessario pubblicare versioni "minimizzate", che non consentano di identificare direttamente i beneficiari o di risalire alla loro condizione di disagio. La risposta A è errata perché la pubblicazione integrale violerebbe i principi di minimizzazione e proporzionalità del trattamento. La risposta C è errata perché la normativa sulla trasparenza impone comunque la pubblicazione degli atti amministrativi, ma nel rispetto delle garanzie per la protezione dei dati personali.

33. Secondo il CAD aggiornato al 2025, come deve essere gestita la PEC istituzionale di un Comune?

A) Può essere consultata solo dal Sindaco, essendo il rappresentante legale dell'ente

B) Deve essere gestita nell'ambito del sistema di protocollo informatico, con verifica quotidiana, protocollazione e assegnazione dei messaggi in arrivo

C) È sufficiente verificarla una volta alla settimana, non essendo un canale ufficiale di comunicazione

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 47 del CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate al 2024, la PEC

istituzionale (o il servizio elettronico di recapito certificato qualificato) deve essere integrata con il sistema di protocollo informatico e verificata quotidianamente. I messaggi in arrivo devono essere protocollati il giorno di ricezione o, al più tardi, il primo giorno lavorativo successivo, e devono essere assegnati agli uffici competenti. Questa gestione è essenziale poiché la PEC è un canale ufficiale di comunicazione che garantisce valore legale, opponibilità a terzi e certezza della data di invio e ricezione. Le riforme 2024-2025 hanno ulteriormente rafforzato l'importanza della PEC e degli altri recapiti digitali certificati, prevedendo anche la possibilità di integrazione con l'App IO. La risposta A è errata perché la PEC istituzionale non è ad uso esclusivo del Sindaco, ma uno strumento dell'ente nel suo complesso. La risposta C è errata perché la verifica settimanale non è sufficiente e potrebbe causare gravi ritardi nella gestione delle comunicazioni ufficiali.

34. Quale delle seguenti affermazioni sull'accesso all'anagrafe (ANPR) è corretta secondo la normativa aggiornata al 2025?

A) I dati anagrafici sono pubblici e possono essere liberamente consultati da chiunque

B) L'accesso ai dati anagrafici è consentito agli uffici pubblici per finalità istituzionali e ai soggetti privati solo per comprovati motivi secondo specifiche modalità

C) I dati anagrafici sono riservati e possono essere consultati solo dai dipendenti comunali

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 33 del D.P.R. 223/1989 (Regolamento anagrafico) e le modifiche introdotte con l'istituzione dell'Anagrafe Nazionale della Popolazione Residente (ANPR) ai sensi dell'art. 62 del CAD, l'accesso ai dati anagrafici è consentito agli uffici pubblici per finalità istituzionali. Per i soggetti privati, l'accesso è limitato ai casi in cui il richiedente dimostri di avere un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata. Il Decreto interministeriale del 2023-2024 sull'ANPR ha ulteriormente specificato le modalità di accesso, prevedendo diversi livelli di consultazione a seconda del soggetto richiedente e delle finalità. In particolare, le PA possono accedere tramite la Piattaforma Digitale Nazionale Dati (PDND) secondo il principio "once only", mentre i privati devono presentare richiesta motivata. La risposta A è errata perché i dati anagrafici non sono liberamente consultabili da chiunque, ma soggetti a limitazioni. La risposta C è errata perché l'accesso non è riservato ai soli dipendenti comunali ma esteso ad altri soggetti pubblici per finalità istituzionali e ai privati nei casi previsti.

35. In base al GDPR e al D.Lgs. 10/2023, cosa deve fare un istruttore comunale che scopre una violazione di dati personali (data breach) nel proprio ufficio?

A) Risolvere autonomamente il problema senza informare nessuno

B) Segnalare immediatamente l'incidente al Responsabile della Protezione Dati e al titolare, secondo la procedura interna di gestione dei data breach

C) Informare esclusivamente il proprio dirigente, che valuterà autonomamente come procedere

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo gli artt. 33 e 34 del GDPR e le precisazioni del D.Lgs. 10/2023, in caso di violazione dei dati personali (data breach), il dipendente che ne viene a conoscenza deve segnalare immediatamente l'incidente secondo la procedura interna stabilita dall'ente. Tipicamente, questa prevede la comunicazione al RPD/DPO e al titolare del trattamento (o ai suoi delegati), utilizzando l'apposita modulistica predisposta. Questa segnalazione tempestiva è essenziale per consentire al titolare di valutare la gravità della violazione e, se necessario, notificarla al Garante Privacy entro 72 ore e agli interessati senza ingiustificato ritardo. Le Linee Guida del Garante Privacy sulla gestione dei data breach, aggiornate nel 2024, hanno sottolineato l'importanza di procedure interne chiare e della formazione del personale per garantire una gestione efficace degli incidenti. La risposta A è errata perché la violazione non può essere gestita autonomamente dal singolo dipendente senza coinvolgere i responsabili. La risposta C è errata perché, sebbene il dirigente vada informato, la procedura corretta richiede di coinvolgere anche il RPD/DPO, figura specializzata nella protezione dei dati.

36. Quale delle seguenti affermazioni sul protocollo informatico è corretta secondo il CAD aggiornato al 2025?

A) È un sistema di registrazione facoltativo che può essere sostituito da registri cartacei

B) È un sistema obbligatorio per tutte le PA che garantisce l'identificazione univoca dei documenti, la certezza della data e l'integrità del registro

C) È obbligatorio solo per i documenti in uscita, mentre quelli in entrata possono essere registrati anche manualmente

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 40-bis del CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate al 2024, il protocollo informatico è un sistema obbligatorio per tutte le pubbliche amministrazioni. Le sue funzionalità essenziali garantiscono: l'identificazione univoca e certa dei documenti tramite il numero di

protocollo e la classificazione, la certezza della data e dell'ora di registrazione, l'immodificabilità del registro, la tracciabilità delle operazioni. Il sistema di protocollo informatico deve inoltre assicurare l'interoperabilità e l'integrazione con i sistemi di gestione documentale e gli altri sistemi informativi dell'ente. Le riforme 2024-2025 hanno ulteriormente rafforzato questi requisiti, prevedendo anche l'integrazione con le piattaforme nazionali come la PDND. La risposta A è errata perché il protocollo informatico non è facoltativo ma obbligatorio per tutte le PA e non può essere sostituito da registri cartacei. La risposta C è errata perché l'obbligo di protocollazione informatica si applica sia ai documenti in uscita che a quelli in entrata.

37. Quale modalità di pubblicazione all'Albo Pretorio online è corretta per un bando di concorso pubblico secondo la normativa vigente?

A) È sufficiente pubblicare l'estratto del bando contenente solo il titolo e la data di scadenza

B) Il bando deve essere pubblicato integralmente, in formato accessibile, per il periodo stabilito dalla legge, con indicazione della data di pubblicazione e scadenza

C) È obbligatorio pubblicare solo la versione cartacea affissa presso la sede comunale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 32 della L. 69/2009, come modificato dagli aggiornamenti normativi fino al 2025, e le Linee Guida AgID sull'accessibilità, la pubblicazione all'Albo Pretorio online di un bando di concorso pubblico deve avvenire in forma integrale, in formato accessibile secondo le norme vigenti (in particolare le Linee Guida AgID sull'accessibilità dei siti web). La pubblicazione deve riportare chiaramente la data di inizio e fine pubblicazione, deve rispettare il periodo minimo stabilito dalla legge (in genere 30 giorni per i bandi di concorso) e deve garantire la possibilità di download del documento integrale. I bandi di concorso devono inoltre essere pubblicati anche nella sezione "Amministrazione Trasparente" sotto la voce "Bandi di concorso" ai sensi dell'art. 19 del D.Lgs. 33/2013. La risposta A è errata perché non è sufficiente pubblicare un estratto, ma è necessaria la pubblicazione integrale. La risposta C è errata perché la legge prevede che la pubblicazione online sostituisca quella cartacea, producendo gli stessi effetti di pubblicità legale.

38. Cosa prevede il CAD aggiornato al 2025 in merito alla formazione informatica dei dipendenti pubblici?

A) La formazione è facoltativa e a carico dei singoli dipendenti

B) Le PA devono programmare e attuare la formazione informatica dei dipendenti come parte del Piano Triennale per l'Informatica e del Piano Integrato di Attività e Organizzazione (PIAO)

C) La formazione è obbligatoria solo per i dirigenti, non per gli altri dipendenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 13 del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, devono attuare politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive. La formazione informatica dei dipendenti deve essere programmata nel Piano Triennale per l'Informatica della singola amministrazione, previsto dall'art. 14-bis del CAD, e nel Piano Integrato di Attività e Organizzazione (PIAO), in particolare nella sezione dedicata al valore pubblico e alla performance. La Strategia Italia Digitale 2026 e il Piano Triennale per l'informatica nella PA 2024-2026 hanno ulteriormente rafforzato l'importanza della formazione digitale, prevedendo specifici obiettivi e indicatori. La risposta A è errata perché la formazione non è facoltativa ma obbligatoria e a carico dell'amministrazione. La risposta C è errata perché l'obbligo di formazione riguarda tutto il personale, non solo i dirigenti.

39. Secondo il GDPR e il D.Lgs. 10/2023, quale delle seguenti affermazioni sul principio di accountability (responsabilizzazione) è corretta?

A) Il principio si applica solo alle grandi aziende private, non alle pubbliche amministrazioni

B) Il principio richiede al titolare del trattamento di implementare misure tecniche e organizzative adeguate e di essere in grado di dimostrare la conformità del trattamento al GDPR

C) Il principio impone solo l'obbligo di redigere il registro dei trattamenti, senza altri adempimenti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 5, par. 2, e l'art. 24 del GDPR, confermati dal D.Lgs. 10/2023, il principio di accountability (responsabilizzazione) richiede al titolare del trattamento non solo di implementare misure tecniche e organizzative adeguate per garantire e dimostrare la conformità del trattamento alla normativa, ma anche di essere in grado di dimostrare tale conformità. Questo approccio basato sul rischio prevede una serie di adempimenti concreti, tra cui: l'adozione di politiche in materia di protezione dei dati, l'adesione a codici di condotta,

l'attuazione di misure di sicurezza adeguate, la tenuta del registro dei trattamenti, la valutazione d'impatto sulla protezione dei dati quando necessario, la formazione del personale. Le Linee Guida del Garante Privacy sull'accountability, aggiornate nel 2024, hanno ulteriormente sottolineato l'importanza di questo principio per le PA, suggerendo l'implementazione di sistemi di gestione privacy basati su standard internazionali come la ISO 27701. La risposta A è errata perché il principio si applica a tutti i titolari, incluse le PA. La risposta C è errata perché il registro dei trattamenti è solo uno degli adempimenti richiesti.

40. Quale delle seguenti procedure è corretta per richiedere l'accesso ai servizi digitali di un Comune tramite SPID secondo la normativa aggiornata al 2025?

A) Il cittadino deve recarsi fisicamente allo sportello comunale per ogni servizio, anche se possiede SPID

B) Il cittadino può accedere direttamente online ai servizi tramite SPID, senza necessità di ulteriori credenziali rilasciate dal Comune

C) Il cittadino deve prima richiedere al Comune l'autorizzazione per utilizzare SPID sui servizi comunali

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 64 del CAD, come modificato dagli aggiornamenti legislativi fino al 2025, l'accesso ai servizi in rete delle pubbliche amministrazioni deve avvenire tramite SPID (Sistema Pubblico di Identità Digitale) o CIE (Carta d'Identità Elettronica), consentendo al cittadino di accedere direttamente online senza necessità di ulteriori credenziali rilasciate dalla singola amministrazione. Il "Decreto Semplificazioni" (D.L. 76/2020) ha reso obbligatorio per tutte le PA l'utilizzo esclusivo di queste modalità di identificazione, con la dismissione delle credenziali proprietarie. Gli aggiornamenti 2024 hanno ulteriormente ampliato questo sistema, prevedendo l'integrazione con il Wallet Digitale Europeo introdotto dal Regolamento eIDAS 2.0. La risposta A è errata perché SPID è stato istituito proprio per evitare la necessità di recarsi fisicamente agli sportelli. La risposta C è errata perché non è necessaria alcuna autorizzazione preventiva del Comune per utilizzare SPID sui suoi servizi; anzi, è il Comune che deve obbligatoriamente accettare SPID come strumento di identificazione.

41. Quali informazioni deve contenere il registro delle attività di trattamento di un Comune per essere conforme al GDPR e al D.Lgs. 10/2023?

A) Solo l'elenco dei dipendenti autorizzati al trattamento dei dati personali

B) Nome e dati di contatto del titolare, finalità del trattamento, categorie di interessati e di dati personali, categorie di destinatari, eventuali trasferimenti verso paesi terzi, termini previsti per la cancellazione, descrizione delle misure di sicurezza

C) Esclusivamente l'elenco dei software utilizzati per il trattamento dei dati

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 30 del GDPR, confermato dal D.Lgs. 10/2023, il registro delle attività di trattamento deve contenere tutte le seguenti informazioni: il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare, del rappresentante del titolare e del responsabile della protezione dei dati; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale; ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative. Le Linee Guida del Garante Privacy sul registro dei trattamenti, aggiornate nel 2024, hanno fornito modelli standard e chiarito che questo strumento è fondamentale per dimostrare l'accountability del titolare. La risposta A è errata perché il registro non deve contenere solo l'elenco dei dipendenti autorizzati. La risposta C è errata perché il registro non si limita all'elenco dei software utilizzati.

42. Secondo la normativa aggiornata al 2025, come deve essere gestito l'utilizzo dell'intelligenza artificiale nei servizi pubblici comunali?

A) Non esistono limitazioni specifiche, l'ente può utilizzare qualsiasi sistema di IA

B) I sistemi di IA devono rispettare i principi di trasparenza, non discriminazione, proporzionalità e devono prevedere sempre la supervisione umana per le decisioni rilevanti sui diritti delle persone

C) L'uso dell'IA è completamente vietato nella pubblica amministrazione

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'AI Act europeo (Regolamento UE 2023/2024) e le sue norme di attuazione in Italia, integrate nel CAD agli artt. 12 e 13-bis nel 2024, i sistemi di intelligenza artificiale utilizzati dalle pubbliche amministrazioni devono rispettare rigorosi principi:

trasparenza (l'utente deve essere informato di interagire con un sistema di IA), non discriminazione (il sistema non deve produrre risultati discriminatori basati su caratteristiche protette), proporzionalità (l'uso deve essere proporzionato alle finalità perseguite) e supervisione umana (le decisioni significative che incidono sui diritti delle persone devono sempre prevedere un intervento umano). La "Strategia Italiana per l'Intelligenza Artificiale 2024-2026" e le Linee Guida AgID sull'IA nella PA hanno ulteriormente precisato questi principi, prevedendo anche la necessità di valutazioni d'impatto preliminari e di meccanismi di spiegabilità degli algoritmi. La risposta A è errata perché esistono limitazioni specifiche all'uso dell'IA nella PA. La risposta C è errata perché l'uso dell'IA non è vietato ma regolamentato.

43. In base al GDPR e al D.Lgs. 10/2023, quale delle seguenti affermazioni è corretta riguardo al trattamento di dati biometrici per finalità di controllo accessi in un edificio comunale?

A) È sempre vietato in quanto i dati biometrici sono dati particolari

B) È consentito solo se strettamente necessario, previa valutazione d'impatto (DPIA), adozione di misure di sicurezza adeguate e con base giuridica specifica

C) È liberamente consentito per tutti i dipendenti e visitatori dell'edificio

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 9 del GDPR e l'art. 2-sexies del D.Lgs. 196/2003 (Codice Privacy), come modificato dal D.Lgs. 10/2023, il trattamento di dati biometrici, essendo dati particolari, è in linea di principio vietato salvo specifiche eccezioni. Per il controllo accessi in un edificio comunale, il trattamento può essere consentito solo se sussistono tutte le seguenti condizioni: è strettamente necessario (principio di necessità), è supportato da una base giuridica specifica (ad esempio, motivi di interesse pubblico rilevante previsti da una norma di legge o regolamento), è preceduto da una valutazione d'impatto sulla protezione dei dati (DPIA) che ha dato esito positivo, sono adottate misure di sicurezza adeguate al rischio elevato (come la cifratura e la pseudonimizzazione). Il Garante Privacy, nei suoi provvedimenti specifici sui dati biometrici aggiornati nel 2024, ha sottolineato la necessità di rispettare il principio di proporzionalità, limitando l'uso dei dati biometrici ai casi in cui altre misure meno invasive risultino insufficienti. La risposta A è errata perché il trattamento non è sempre vietato, ma sottoposto a condizioni stringenti. La risposta C è errata perché il trattamento non è liberamente consentito ma soggetto a numerose limitazioni.

44. Quale dei seguenti adempimenti è obbligatorio secondo il CAD aggiornato al 2025 per garantire l'accessibilità dei siti web e delle applicazioni mobili delle pubbliche amministrazioni?

A) Pubblicare solo contenuti in formato PDF scansionato

B) Pubblicare e aggiornare annualmente la dichiarazione di accessibilità, garantire la conformità alle Linee Guida AgID e fornire un meccanismo di feedback

C) Limitare l'accesso al sito web comunale ai soli cittadini residenti nel territorio comunale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 9 del CAD, la Legge 4/2004 (Legge Stanca) e le Linee Guida AgID sull'accessibilità degli strumenti informatici, aggiornate nel 2024 in conformità alla Direttiva UE 2016/2102, le pubbliche amministrazioni hanno l'obbligo di: 1) pubblicare sul proprio sito web la dichiarazione di accessibilità conforme al modello fornito da AgID e aggiornarla annualmente; 2) garantire la conformità dei propri siti web e applicazioni mobili ai requisiti tecnici delle WCAG 2.1 (Web Content Accessibility Guidelines) livello AA; 3) fornire un meccanismo di feedback che permetta a chiunque di segnalare problemi di accessibilità e richiedere contenuti alternativi; 4) formare adeguatamente il personale che si occupa della pubblicazione di contenuti. La risposta A è errata perché i PDF scansionati sono generalmente poco accessibili, non consentendo la lettura tramite screen reader e altre tecnologie assistive. La risposta C è errata perché l'accesso ai siti web pubblici non può essere limitato in base alla residenza, ma deve essere garantito a tutti, incluse le persone con disabilità.

45. Secondo la normativa vigente sul fascicolo sanitario elettronico (FSE 2.0), quale affermazione è corretta riguardo al trattamento dei dati sanitari da parte di un Comune?

A) I Comuni possono accedere liberamente ai dati del FSE dei propri cittadini per finalità amministrative

B) I Comuni non possono accedere direttamente ai dati clinici del FSE, ma solo alle informazioni amministrative per cui sono autorizzati secondo specifiche convenzioni e nel rispetto della normativa sulla privacy

C) I Comuni possono accedere solo ai dati sanitari relativi a malattie infettive per finalità di tutela della salute pubblica

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo il D.L. 34/2020 (art. 11), come modificato dalle successive disposizioni fino al 2025, e il D.M. Salute del 2023-2024 sull'FSE 2.0, i Comuni non possono accedere direttamente ai dati clinici contenuti nel Fascicolo Sanitario Elettronico, essendo questo accesso riservato principalmente agli operatori sanitari autorizzati e al cittadino stesso. Tuttavia, i Comuni possono accedere, sulla base di specifiche convenzioni con le autorità sanitarie e nel rispetto della normativa sulla privacy, a determinate informazioni amministrative necessarie per l'erogazione di servizi socio-sanitari di loro competenza (ad esempio, per la gestione di servizi di assistenza domiciliare o per l'erogazione di benefici sociali legati a condizioni di salute). Le Linee Guida del Garante Privacy sul trattamento dei dati sanitari, aggiornate nel 2024, hanno ulteriormente precisato i limiti di tale accesso, evidenziando la necessità di misure tecniche che limitino la visibilità ai soli dati effettivamente necessari. La risposta A è errata perché i Comuni non possono accedere liberamente a tutti i dati del FSE. La risposta C è errata perché l'accesso non è limitato ai soli dati relativi alle malattie infettive.

46. Quale delle seguenti affermazioni sul whistleblowing digitale nelle pubbliche amministrazioni è corretta secondo la normativa aggiornata al 2025?

A) Le segnalazioni di illeciti possono essere effettuate solo in formato cartaceo

B) Le PA devono dotarsi di canali di segnalazione digitali che garantiscano la riservatezza del segnalante, con crittografia e sistema di pseudonimizzazione

C) Le segnalazioni digitali devono essere sempre nominative per essere prese in considerazione

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 54-bis del D.Lgs. 165/2001, come modificato dalla Legge 179/2017 e ulteriormente aggiornato dal D.Lgs. 24/2023 di recepimento della Direttiva UE 2019/1937 (Whistleblowing), le pubbliche amministrazioni devono dotarsi di canali di segnalazione digitali che garantiscano la riservatezza dell'identità del segnalante. Questi canali devono implementare misure tecniche avanzate, tra cui la crittografia dei dati e sistemi di pseudonimizzazione, per impedire l'identificazione non autorizzata del whistleblower. Le Linee Guida ANAC, aggiornate nel 2024, hanno ulteriormente specificato i requisiti tecnici di questi canali, includendo: separazione dei dati identificativi dal contenuto della segnalazione, tracciamento delle operazioni effettuate, impossibilità di modifica dei contenuti, e conservazione sicura. È anche prevista la possibilità di integrare questi canali con l'App IO. La risposta A è errata perché le segnalazioni possono e devono essere effettuate anche in formato digitale. La risposta C è errata perché le segnalazioni digitali possono essere anche anonime, purché adeguatamente circostanziate.

47. In base al Piano Triennale per l'Informatica nella PA 2024-2026, quale delle seguenti affermazioni sul cloud computing è corretta?

A) Le pubbliche amministrazioni possono utilizzare qualsiasi servizio cloud, inclusi quelli consumer, per ospitare i propri dati

B) Le PA devono adottare il paradigma cloud first, privilegiando il Polo Strategico Nazionale (PSN) per i dati critici e servizi qualificati ACN per gli altri dati

C) L'utilizzo del cloud è vietato per le amministrazioni pubbliche per motivi di sicurezza nazionale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo il Piano Triennale per l'Informatica nella PA 2024-2026 e la Strategia Cloud Italia, aggiornata nel 2024 e integrata nel CAD all'art. 68, le pubbliche amministrazioni devono adottare il paradigma "cloud first", privilegiando il Polo Strategico Nazionale (PSN) per i dati e i servizi critici/strategici e i servizi cloud qualificati dall'Agenzia per la Cybersicurezza Nazionale (ACN) per gli altri dati. La migrazione al cloud è considerata prioritaria per modernizzare i servizi pubblici, aumentare la sicurezza e ridurre la frammentazione dei data center. Il PSN, operativo dal 2023-2024, è un'infrastruttura ad alta affidabilità progettata per ospitare i dati e i servizi critici delle PA, garantendo elevati standard di sicurezza e sovranità digitale. La risposta A è errata perché le PA non possono utilizzare qualsiasi servizio cloud, ma solo quelli qualificati secondo gli standard di sicurezza previsti. La risposta C è errata perché l'utilizzo del cloud non è vietato ma fortemente incoraggiato, purché rispetti determinati requisiti di sicurezza.

48. Quale delle seguenti affermazioni sull'App IO come punto di accesso ai servizi pubblici digitali è corretta secondo il CAD aggiornato al 2025?

A) L'integrazione dei servizi comunali con l'App IO è facoltativa e a discrezione dell'ente

B) I Comuni hanno l'obbligo di integrare progressivamente i propri servizi digitali con l'App IO, rendendo disponibili almeno i servizi di pagamento, le comunicazioni ufficiali e i principali servizi ai cittadini

C) L'App IO può essere utilizzata solo dai cittadini maggiorenni

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 64-bis del CAD, come modificato dal D.L. 76/2020 e dagli aggiornamenti legislativi fino al 2025, le pubbliche amministrazioni hanno l'obbligo di rendere fruibili i propri servizi in rete anche attraverso l'applicazione App IO, il punto unico di accesso per interagire in modo semplice e sicuro con i servizi pubblici locali e nazionali. In particolare, i Comuni sono tenuti a integrare con App IO almeno: i servizi di pagamento (attraverso la piattaforma PagoPA), le comunicazioni ufficiali (avvisi, scadenze, promemoria), i principali servizi ai cittadini (certificati, prenotazioni, segnalazioni). Le Linee Guida AgID sull'integrazione con App IO, aggiornate nel 2024, hanno ulteriormente specificato i tempi e le modalità di questa integrazione, prevedendo anche incentivi per gli enti più virtuosi. La risposta A è errata perché l'integrazione non è facoltativa ma obbligatoria. La risposta C è errata perché l'App IO può essere utilizzata da tutti i cittadini, anche minorenni, purché dispongano di SPID o CIE (per i minori di 14 anni tramite l'identità digitale dei genitori).

49. Quale delle seguenti affermazioni sulla conservazione a norma dei documenti informatici è corretta secondo la normativa aggiornata al 2025?

A) La conservazione può essere effettuata esclusivamente in-house dal Comune, senza possibilità di esternalizzazione

B) La conservazione può essere affidata a conservatori accreditati AgID, ma il Responsabile della Conservazione interno all'ente mantiene la responsabilità complessiva del processo

C) La conservazione dei documenti informatici è facoltativa per i Comuni con meno di 5.000 abitanti

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo gli artt. 43-44 del CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, aggiornate nel 2024, la

conservazione dei documenti informatici può essere affidata a conservatori accreditati da AgID, che garantiscono il rispetto dei requisiti tecnici e di sicurezza previsti dalla normativa. Tuttavia, anche in caso di esternalizzazione, il Responsabile della Conservazione interno all'ente mantiene la responsabilità complessiva del processo, dovendo verificare il corretto svolgimento delle attività del conservatore, definire le politiche di conservazione, predisporre il manuale di conservazione e garantire il rispetto della normativa. L'accordo di servizio con il conservatore accreditato deve definire chiaramente i ruoli e le responsabilità delle parti. La risposta A è errata perché la conservazione può essere anche esternalizzata a conservatori accreditati. La risposta C è errata perché la conservazione dei documenti informatici è obbligatoria per tutte le PA, indipendentemente dalle dimensioni, sebbene per i piccoli Comuni siano previste forme di gestione associata o convenzioni.

50. Secondo la normativa vigente, come deve essere gestito il diritto di accesso ai documenti amministrativi in formato digitale?

A) I cittadini possono accedere solo ai documenti cartacei, non a quelli digitali

B) L'accesso deve essere garantito indipendentemente dal supporto, con possibilità di richiesta telematica e rilascio di copie digitali anche di documenti cartacei

C) L'accesso ai documenti digitali può essere esercitato solo recandosi fisicamente presso l'ente

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 65 del CAD, in combinato disposto con gli artt. 22-23-bis, e la Legge 241/1990 come modificata fino al 2025, il diritto di accesso ai documenti amministrativi deve essere garantito indipendentemente dal supporto sul quale i documenti sono formati, conservati o reperibili. Le istanze di accesso possono essere trasmesse per via telematica (tramite PEC, SPID, CIE o altri strumenti previsti) e i documenti possono essere rilasciati in formato digitale anche se l'originale è cartaceo (mediante scansione). Le Linee Guida AgID sull'accesso ai documenti amministrativi, aggiornate nel 2024, hanno ulteriormente specificato che le amministrazioni devono predisporre sistemi per la gestione telematica delle richieste di accesso e per il rilascio di copie digitali, anche integrate con l'App IO e il domicilio digitale. La risposta A è errata perché l'accesso può e deve essere garantito anche per i documenti digitali. La risposta C è errata perché l'accesso ai documenti digitali può avvenire anche telematicamente, senza necessità di recarsi fisicamente presso l'ente.

51. Quale delle seguenti affermazioni sul trattamento dei dati personali mediante sistemi di videosorveglianza con riconoscimento facciale in luoghi pubblici è corretta secondo la normativa aggiornata al 2025?

A) È sempre consentito per finalità di sicurezza urbana

B) È vietato, salvo casi eccezionali previsti dalla legge per finalità di sicurezza pubblica, prevenzione e repressione di reati gravi, con autorizzazione specifica

C) È consentito senza limitazioni se il sistema è gestito dalla Polizia Locale

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo l'art. 9 del GDPR, l'art. 2-sexies del Codice Privacy come modificato dal D.Lgs. 10/2023, e l'AI Act europeo (Regolamento UE 2023/2024) recepito nell'ordinamento italiano, il trattamento di dati biometrici come quelli derivanti dal riconoscimento facciale in luoghi pubblici è in linea di principio vietato. Tale trattamento può essere consentito solo in casi eccezionali, espressamente previsti dalla legge, per finalità di sicurezza pubblica, prevenzione e repressione di reati gravi, ricerca di persone scomparse o identificazione di vittime, e comunque previa autorizzazione specifica dell'autorità competente (Garante Privacy o, in casi specifici, autorità giudiziaria). I provvedimenti del Garante Privacy sulla videosorveglianza con sistemi di riconoscimento facciale, aggiornati nel 2024, hanno ribadito questo approccio restrittivo, imponendo valutazioni d'impatto rafforzate, misure di sicurezza stringenti e limitazioni temporali all'uso di questi sistemi. La risposta A è errata perché il trattamento non è sempre consentito per finalità di sicurezza urbana. La risposta C è errata perché anche per la Polizia Locale valgono le limitazioni previste dalla normativa.

52. Secondo il CAD aggiornato al 2025, quali caratteristiche deve avere la notificazione digitale degli atti amministrativi ai cittadini?

A) La notificazione può avvenire via email ordinaria, senza particolari requisiti

B) La notificazione deve garantire l'integrità, l'immodificabilità, la certezza della data e dell'ora, la verificabilità dell'avvenuta consegna e della presa visione

C) La notificazione digitale è facoltativa e può essere utilizzata solo se espressamente richiesta dal destinatario

Risposta corretta: B

Commento: La risposta corretta è la B. Secondo gli artt. 6, 45-bis e 48 del CAD, come modificati dagli aggiornamenti legislativi fino al 2025, e il D.L. 76/2020 che ha istituito la Piattaforma Notifiche Digitali (PND), la notificazione digitale degli atti amministrativi deve garantire: l'integrità e l'immodificabilità del contenuto, la certezza della data e dell'ora di invio e ricezione, la verificabilità dell'avvenuta consegna mediante ricevuta opponibile a terzi, e la possibilità di tracciare la presa visione da parte del destinatario. Questi requisiti sono soddisfatti mediante l'uso di domicili digitali (PEC o servizi elettronici di recapito certificato qualificato) o della Piattaforma Notifiche Digitali, integrata con l'App IO e il sistema di identità digitale SPID/CIE. Le Linee Guida AgID sulle comunicazioni elettroniche, aggiornate nel 2024, hanno ulteriormente dettagliato questi requisiti, specificando anche le modalità per garantire l'accessibilità degli atti notificati. La risposta A è errata perché l'email ordinaria non garantisce i requisiti necessari per la notificazione digitale. La risposta C è errata perché la notificazione digitale non è facoltativa ma obbligatoria quando il destinatario ha un domicilio digitale.