Allegato D

CARATTERISTICHE TECNICHE DEL SISTEMA DI CONSULTAZIONE DATI ANAGRAFICI DEL COMUNE DI VICENZA

Oggetto
Con il presente documento vengono descritte le caratteristiche tecniche del sistema di consultazione tramite "Visure" in riferimento ai requisiti indicati dal Codice dell'Amministrazione Digitale, dalle "Linee guida per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni" (giugno 2013 v.2.0) e dalle "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" approvate in data 2 luglio 2015 dal Garante alla privacy (pubblicate nella G.U. n.179 del 4.08.2015).

Descrizione dell'infrastruttura tecnologica
Il sistema di consultazione tramite "Visure" è una procedura web installata su server della rete del Comune di Vicenza. Il sistema è pubblicato ed accessibile da Internet attraverso un meccanismo di reverse proxy e firewalling , che "maschera" e limita attraverso opportuni filtri, l'accesso ai dati.

Modalità di accesso
L'accesso al sistema avviene via web su canale sicuro HTTPS.

Servizi per l'accesso ai dati
Il sistema offre funzioni di ricerca e consultazione dei dati anagrafici di cittadini residenti nel Comune di Vicenza attraverso diversi profili autorizzativi per lo svolgimento dei soli compiti istituzionali dell'ente consultante (allegato B).
Il sistema prevede la possibilità di ricerca indicando: cognome/nome e data di nascita; cognome/nome e indirizzo; codice fiscale.

Livelli di servizio
Il sistema di consultazione è attivo 24 h su 24 – sette giorni alla settimana; l'erogazione dello stesso è subordinata al funzionamento dell'infrastruttura ICT (Informatica e TeleComunicazioni).
L'assistenza può essere sempre richiesta via e-mail, telefonica è garantita durante gli orari d'uffici, garantendo gli stessi livelli di servizio erogati all'attuale portale di visure enti.

Aspetti di protezione dei dati personali
L'accesso ai dati personali consultabili è stabilito dalla convenzione sottoscritta dal Comune di Vicenza con l'ente fruitore tenendo in considerazione le necessità minime che lo stesso ha di trattare il dato consultato.
L'accesso alla banca dati anagrafica è effettuato in modo limitato alle sole tabelle della banca dati oggetto delle informazioni d'interesse attraverso un utente di sola lettura che non può in alcun modo effettuare modifiche alle informazioni stesse.

Selezione dei dati
Il livello di dettaglio delle informazioni restituite è attribuibile ad ogni singolo operatore attraverso livelli di accesso distinti che prevedono la selezione delle informazioni personali oggetto di accesso, nel rispetto dei principi di pertinenza e non eccedenza concordati con il fruitore sulla base delle proprie esigenze istituzionali.

Procedura di autenticazione e autorizzazione degli utenti
L'accesso al sistema avviene via web attraverso l'utilizzo di password univoche create su richieste dell'ente interessato che indica i dati anagrafici degli operatori da abilitare. Le credenziali vengono inviate via e-mail al referente per la relativa distribuzione con obbligo cambio password al primo accesso.

Misure di sicurezza

Il sistema “Visure” è erogato tramite canale https attraverso l’uso di un certificato digitale rilasciato da CA accreditata che protegge la trasmissione dei dati dal rischio d’intercettazione delle credenziali e dei dati personali tramite meccanismi crittografici di adeguata robustezza.

La configurazione della postazione dev’essere garantita dal fruitore secondo le regole dell’infrastruttura locale di collegamento utilizzata e messa a disposizione al proprio personale.

Gli accessi alle banche dati avvengono soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato.

L'applicazione è realizzata con protocolli di sicurezza provvedendo ad asseverare l'identita' digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014, emessi da una Certification Authority e riconosciuti dai piu' diffusi browser e sistemi operativi.

Le procedure di registrazione avvengono con il riconoscimento diretto e l'identificazione certa dell'utente.

Le regole di gestione delle credenziali di autenticazione prevedono, in ogni caso:

- l'identificazione univoca di una persona fisica;
- processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura;
- le credenziali sono costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato provvisto di una coppia username/password.

La gestione delle password prevede che:

- la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate;
- le password devono rispondere a requisiti di complessità (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);
- quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;
- le credenziali verranno bloccate a fronte di reiterati tentativi falliti di autenticazione;
- i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server che sulle postazioni di lavoro;
-la procedura di autenticazione dell'utente sarà protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata;
- gli accessi saranno controllati al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;
- è esclusa la possibilita' di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;
- anche al fine di ottemperare all'obbligo di comunicare al Garante entro 48 ore i casi di data breach, l’ente erogatore e l’ente fruitore si impegnano a comunicare tempestivamente:

incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilita' di dati oggetto di convenzione;

ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

ogni modificazione tecnica od organizzativa del proprio dominio,che comporti l'impossibilità di garantire l'applicazione delle regole di sopra riportate o la loro perdita di efficacia;

- tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. Al tal fine:

il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata,il codice identificativo dell'utenza che ha posto in essere l'operazione;

il suddetto codice identificativo, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione.

Il sistema è esposto su rete internet e per l'accesso all’applicazione è richiesto l'uso di certificati digitali client, più le credenziali di accesso.

Più dettagliatamente l'accesso alle "Visure" avviene in 2 step:

1. per la fase di autenticazione tramite l'utilizzo del certificato digitale client
   (Nel caso l'operatore non disponga di un certificato digitale rilasciato da una CA accreditata, il Comune di Vicenza procederà al rilascio di un certificato autoprodotto)
2. superato il 1^ controllo l'utente dovrà inserire le proprie credenziali di accesso (costituite dalla coppia utenza e password ad uso esclusivo del'incaricato, cui è fatto obbligo di garantire altresì condizioni di sicurezza).

Il mancato accesso al sistema per oltre 90 giorni da parte dell'utente comporta la disabilitazione dello stesso. La password potrà essere nuovamente attivata previa richiesta formulata entro 120 giorni dalla disabilitazione tramite e-mail da parte del responsabile della convenzione all'indirizzo uffanagrafe@comune.vicenza.it. Diversamente l'utenza viene bloccata.
Le misure di sicurezza sono periodicamente riconsiderate e adeguate ai progressi tecnici ed all'evoluzione dei rischi.
Il sistema "Visure" prevede la registrazione delle operazioni di consultazione e ricerca effettuate dall'operatore. Tali operazioni sono archiviate in tabella di "LOG" e possono essere consultate attraverso meccanismi di reporting per individuare eventuali abusi di accesso da parte degli operatori.
L'accesso via web da una rete esterna a quella del Comune non può garantire con la massima efficacia il controllo che l'accesso con le medesime credenziali avvenga da postazioni diverse (reti private esterne al Comune di Vicenza che si "presentano" su internet con lo stesso ip address).
Le operazioni di trattamento di dati personali effettuati dagli utenti autorizzati sono adeguatamente tracciate: le modalità di accesso al sistema danno garanzia di riconducibilità al codice identificativo dell'utenza; il codice identificativo è riferito al singolo utente incaricato del trattamento, il fruitore deve garantire la possibilità di identificare l'utente nei casi in cui ciò si renda necessario.

Controlli
Il Comune di Vicenza effettua controlli a campione relativamente al numero di accessi effettuati ed ai tempi dell'accesso (fasce orarie d'accesso coerenti con gli orari di servizio per individuare eventuali comportamenti anomali o a rischio).
Provvederà inoltre a chiedere conferma del perseguimento del fine istituzionale rispetto ad un campione di accessi effettuati.
A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati va inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

Periodicità di aggiornamento dei dati
I dati sono aggiornati in tempo reale.