VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

in relazione alle attività di partecipazione ai bandi per l'assegnazione d'alloggio di edilizia sovvenzionata, redazione delle relative graduatorie e conseguente procedimento di assegnazione.

Premessa

La valutazione d'impatto sulla protezione dei dati consiste in un'auto-valutazione aziendale, come prevista dall'art. 35 del Regolamento (Ue) 2016/679 (GDPR), che ha come obiettivo quello di valutare i possibili rischi attinenti il trattamento dei dati personali in una specifica attività aziendale. L'attività di valutazione è strumentale all'implementazione di idonee misure di mitigazione di tali rischi.

Trattamento in oggetto

Partecipazione ai bandi per l'assegnazione d'alloggio di edilizia sovvenzionata, redazione delle relative graduatorie e conseguente procedimento di assegnazione.

La natura del processo sensibile

L'ATER tratta i dati personali dei soggetti con cui stabilisce rapporti contrattuali e/o pre-contrattuali, necessari per lo svolgimento del rapporto sulla base delle normative nazionali e regionali. Per ottemperare alle finalità statutarie ed agli specifici obblighi normativamente attribuitegli quale ente pubblico, l'Azienda viene a conoscenza di dati personali, anche particolari (che nel recente passato venivano definiti "dati sensibili"), necessari per la stesura della graduatoria, quali:

- dati e documenti anagrafici (degli istanti e dei componenti dei loro nuclei familiari);
- dati relativi al reddito ed alla situazione patrimoniale;
- dati relativi allo stato di salute;
- dati giudiziari;
- altri dati personali che siano strettamente pertinenti allo svolgimento delle descritte attività.

La normativa di settore (L.R. 39/2017) dispone che l'attività di bandizione sia di competenza comunale. Tale attività è sovente delegata ad ATER, attraverso la sottoscrizione di apposita convenzione. ATER e Comune risultano in questo caso contitolari del trattamento dei dati: per tale ragione si è ritenuto di unire sistematicamente alle citate convenzioni un apposito accordo di contitolarità nel trattamento (vedasi documentazione allegata).

La raccolta dati riguarda sia l'intestatario della domanda che i suoi familiari. In ipotesi di delega comunale, il bando per l'assegnazione d'alloggio e.r.p. viene pubblicato sul sito aziendale e sul portale informatico regionale dedicato allo scopo, ordinariamente nel mese di ottobre di ogni anno, per un periodo di 60 giorni. Le domande sono presentate generalmente allo sportello aziendale o

trasmesse a mezzo posta, mail o pec e vengono protocollate. Le informazioni necessarie all'istruttoria sono comunicate dagli interessati attraverso la compilazione di apposito modello di domanda (redatto sotto forma di autocertificazione), e possono essere integrate d'ufficio attingendo da banche dati pubbliche (ad esempio anagrafe comunale, Agenzia delle Entrate, catasto, INPS, …).

Il contesto di trattamento

Il trattamento ha ad oggetto i dati personali di quanti partecipino ai bandi per l'assegnazione di un alloggio di edilizia residenziale pubblica, sia che risultino assegnatari, sia che risultino non assegnatari.

Il trattamento si inserisce nell'ambito dell'attuazione di un diritto costituzionale (diritto alla casa, art. 47 comma 1 Cost.), a sua volta affermato da plurime Convenzioni Internazionali (ex plurimis art. 25 Dichiarazione Universale dei diritti dell'Uomo, art. 11 Convenzione Internazionale dei diritti sociali ed economici, art. 28 della Convenzione ONU per i diritti delle persone con disabilità, dall'art. 31 della Carta sociale europea riveduta).

La base giuridica del trattamento è rappresentata dalle norme nazionali e regionali (L.R. del Veneto n.39/2017 e relativo regolamento di esecuzione n.4/2018) che regolano l'edilizia residenziale pubblica.

I dati trattati da Ater provengono direttamente dall'interessato all'assegnazione dell'alloggio (la domanda di partecipazione al concorso di assegnazione è redatta in forma di autocertificazione), ma possono essere anche integrati d'ufficio, oppure divenire oggetto di verifica da parte aziendale, attingendo da banche dati di enti pubblici (Anagrafe, Catasto, INPS, Agenzia delle Entrate, ecc.) con i quali Ater abbia stipulato una convenzione ai sensi di legge. Vi è infatti un preciso obbligo di verifica in capo all'amministrazione, tenuta – ex artt.71 e 72 del DPR 445/2000 - ad effettuare idonei controlli riguardanti le dichiarazioni sostitutive di certificazione rilasciate dagli istanti.

Il rapporto giuridico con quanti partecipano ai bandi per l'assegnazione dell'alloggio è regolato dalle normative nazionali e regionali applicabili alla procedura di bando. Con quanti, fra i partecipanti al bando medesimo, risultino assegnatari dell'alloggio, il rapporto assume anche natura contrattuale.

I dati possono riguardare soggetti minorenni, persone fragili, soggetti in condizione di disagio economico.

Proposta di interventi finalizzati a ridurre il rischio

I dati personali in possesso dell'Azienda oggetto di trattamento, detenuti ai fini dell'assegnazione dell'alloggio, sono pertinenti e limitati a quanto indicato nella finalità del trattamento (c.d. principio di minimizzazione dei dati). Gli stessi dati possono essere detenuti oltre che dal personale interno, anche da soggetti pubblici a cui la comunicazione avviene in forza di obblighi di legge, da soggetti terzi (persone fisiche o giuridiche) che svolgono servizi di verifica della conformità normativa di ATER (ad es. Organismo di vigilanza, istituito ai sensi del D.Lgs. n.231/2001), da soggetti che svolgono attività di verifica relativamente ai sistemi di gestione certificati applicati da ATER, da soggetti a cui la comunicazione è necessaria per la gestione del rapporto contrattuale, a personale informatico (interno od esterno) in modo limitato a quanto strettamente necessario. I dati sono trasmessi solo per necessità contrattuali o per necessità di gestione.

Valutazione dell'impatto

Al fine di valutare l'impatto sui diritti degli interessati, l'Ater ha analizzato 3 diversi ambiti: riservatezza, integrità, disponibilità dei dati.

Ambito	**Domanda**	**Valutazione**
1) Riservatezza	Quale impatto in termini di conseguenze negative, può avere sui diritti dell'interessato la divulgazione non autorizzata dei suoi dati personali conferiti ad Ater?	○ Basso ○ Medio ○ **Alto** ☑ ○ Molto Alto
2) Integrità	Quale impatto, in termini di conseguenze negative, può avere sull'interessato l'alterazione non autorizzata dei suoi dati personali conferiti ad Ater?	○ Basso ○ Medio ○ **Alto** ☑ ○ Molto Alto
3) Disponibilità dei dati	Quale impatto sui diritti dell'interessato, in termini di conseguenze negative, può avere la distruzione, la perdita, la criptazione non autorizzata, dei suoi dati personali conferiti ad Ater?	○ Basso ○ Medio ○ **Alto** ☑ ○ Molto Alto

Nella tabella sotto indicata sono riportati 4 livelli di impatto del trattamento in oggetto.

Livello di impatto	**Descrizione**
Basso ☐	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (ad esempio: necessità per gli interessati di dedicare altro tempo per inoltrare nuovamente i dati eventualmente smarriti da ATER).
Medio ☐	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, impossibilità temporanea di accedere ai servizi aziendali).
Alto ☑	**Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.**
Molto Alto ☐	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (danni fisici o psicologici a lungo termine, incapacità lavorative).

Attese le valutazioni di cui sopra, si ritiene di attribuire alle attività di bandizione, redazione delle graduatorie ed assegnazioni d'alloggio di edilizia sovvenzionata in esame, il livello **alto** di valutazione di impatto.

Valutazione della probabilità

Di seguito vengono individuate esempi di domande per la valutazione della probabilità di accadimento di una minaccia nelle 4 aree sotto riportate, nello specifico:

i) Risorse di rete;

ii) Processi/procedure relativi all'operazione di trattamento dei dati;

iii) Diverse parti e persone coinvolte nel trattamento;

iv) Settore di operatività e scala del trattamento.

i) Risorse tecniche di rete

Domande	**Spiegazione**	**Risposte**
Quale parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte degli aggressori esterni online, soprattutto quando il servizio è disponibile a tutti gli utenti di Internet.	Inserimento delle domande nel portale informatico regionale; Elaborazione delle graduatorie da portale regionale. Assegnazione degli alloggi da portale regionale. **[1]**
E' possibile fornire l'accesso ad un sistema interno di trattamento di dati personali tramite Internet?	Quando l'accesso ad un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterna aumenta. Allo stesso modo aumenta anche la probabilità di abuso dei dati da parte degli utenti. Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione/amministrazione remota del sistema IT.	L'accesso al gestionale aziendale avviene esclusivamente tramite rete interna (offline). **[1]**
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (ed ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunatamente configurati, tali connessioni possono consentire l'accesso ai dati personali a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate all'accesso).	Non sono connessi sistemi IT esterni. Sono configurati differenti livelli di autorizzazione alla consultazione dei dati a seconda del ruolo rivestito in azienda e le specifiche mansioni svolte. **[1]**
Persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza.	Le domande di assegnazione dono tenute in armadi muniti di chiave. **[1]**
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza eseguire le migliori prassi?	Componenti hardware e software mal progettate, implementate e/o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione e raggiungere determinati livelli di resilenza.	L'Azienda effettua regolarmente la manutenzione delle componenti hardware e provvede al periodico aggiornamento del software. **[1]**

ii) Processi relativi all'operazione di trattamento dei dati

Domande	Spiegazione	Risposte
I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza comprensiva del sistema.	L'Azienda ha definito le competenze dei singoli uffici. Coerentemente alle competenze dei singoli uffici, il reparto IT ha organizzato uno schema di accessi per ruolo per ciascun utente-dipendente, in modo che le attività di trattamento che esso può svolgere siano coerenti e sufficienti all'espletamento delle proprie mansioni, nell'ambito della competenza dell'ufficio a cui il dipendente medesimo è assegnato. Lo schema di accessi per ruolo consente di risalire, mediante i *"log"*, all'identificazione dell'utente che abbia svolto attività sui dati personali in possesso dell'Ater ad al tipo di attività svolte. Il *log* registra le lavorazioni avvenute sul dato, e viene automaticamente generato al salvataggio del dato nel gestionale aziendale. **[2]**
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	L'Azienda si è dotata di un Codice etico e di comportamento che disciplinano anche le modalità di accesso alle risorse informatiche aziendali ed alla rete internet. **[1]**
I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	I dipendenti non sono autorizzati a collegare dispositivi informatici personali ai PC aziendali. **[1]**
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi - Fi aperte), sia uso non autorizzato di queste informazioni.	I dipendenti in *smart working* (gli unici a poter visualizzare dati personali degli utenti all'esterno dalla sede aziendale), sono connessi in VPN (Virtual Private Network). **[1]**
Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file del registro?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/procedure e risorse, con conseguente abuso di dati personali.	Ogni operazione sul gestionale aziendale nonché sul portale regionale è tracciata (file LOG o sistema analogo). **[1]**

iii) Persone coinvolte nel trattamento de dati personali

Domande	Spiegazione	Risposte
Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	Relativamente alle attività in esame, i dati personali degli utenti sono trattati esclusivamente dai dipendenti dell'ufficio inquilinato, dell'ufficio protocollo e dell'ufficio manutenzioni, nonché dalla Dirigenza aziendale. **[2]**
Quale parte dell'operazione di trattamento dei dati è eseguita da un appaltatore/terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. E' importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	Le informazioni vengono caricate sul portale informatico regionale istituito allo scopo. Se l'istante necessita di accedere agli uffici aziendale, alcuni suoi dati personali (non sensibili) vengono inseriti nella Applicazione deputata alla calendarizzazione degli accessi, attualmente gestita dalla ditta Tecnosys (che è stata naturalmente nominata responsabile esterno del trattamento). **[1]**
Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.	Nel corso dell'anno 2020 si è tenuto un ciclo di formazione in materia di privacy, trasparenza ed anticorruzione, a cui hanno partecipato tutti i dipendenti aziendali. **[1]**
Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	E' previsto a breve (4 maggio 2021) un ulteriore corso di formazione in argomento rivolto a tutto il personale. **[1]**
Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I documenti cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazioni e riutilizzo non autorizzati.	Gli armadietti deputati alla conservazione delle pratiche sono muniti di chiave. E' presente in azienda un macchinario per la distruzione dei documenti. **[2]**

iv) Settore di operatività e scala del trattamento

Domande	Spiegazione	Risposte
Ater ritiene che il suo settore di attività sia esposto ad attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento, questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.	Non sembra che il settore di attività sia particolarmente soggetto ad attacchi informatici. **[2]**
Ater ha subito attacchi informatici o a altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caos, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	Ad oggi l'Azienda non è mai stata oggetto di attacchi informatici. **[1]**
Ater ha ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico (utilizzando per il trattamento dei dati personali) nell'ultimo anno?	Bug di sicurezza/vulnerabilità possono essere sfruttai per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alla vulnerabilità della sicurezza che potrebbero influire sui sistemi e servizi menzionati sopra.	L'Azienda non ha ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico. **[1]**
Un'operazione di elaborazione riguarda un grande volume di individui e/o dati personali?	Il tipo ed il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	Mediamente ogni anno vengono presentate presso l'ATER di Belluno circa 200/300 domande di assegnazione d'alloggio. Mediamente l'Azienda assegna una settantina di alloggi l'anno. **[1]**
Esistono *best practice* di sicurezza specifica per il tuo settore di operatività che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni e ai rischi del particolare settore. La mancanza di conformità con le *best practice* pertinenti potrebbe essere un indicatore si scarsa gestione della sicurezza.	Gran parte delle operazioni relative all'attività in esame è svolta attraverso l'utilizzo della piattaforma informatica regionale. **[1]**

Una volta calcolate le probabilità delle 4 aree, si determina il punteggio con la tabella sottostante.

A) Valutazione della probabilità di occorrenza delle minacce per area

Area di valutazione	Probabilità	
	Livello	**Punteggio**
Rete e risorse tecniche	Basso	**1**☑
	Medio	2
	Alto	3
Processi/Procedure relativi al trattamento dei dati personali	Basso	**1**☑
	Medio	2
	Alto	3
Parti/Persone Coinvolte nel trattamento dei dati personali	Basso	**1**☑
	Medio	2
	Alto	3
Parti/Persone Coinvolte nel trattamento dei dati personali	Basso	**1**☑
	Medio	2
	Alto	3
Settore di operatività dei dati personali	Basso	**1**☑
	Medio	2
	Alto	3

Infine, con la tabella sotto riportata si può ottenere il livello della probabilità della minaccia.

B) Valutazione della probabilità di occorrenza di una minaccia

Somma globale della probabilità di occorrenza di una minaccia	Livello di probabilità delle minacce
5-6	**Basso** ☑
7-8	Medio
9-12	Alto

La probabilità di occorrenza finale della minaccia viene calcolata dopo aver sommato i 4 punteggi ottenuti nella Tabella (A) e associato il risultato complessivo alle somme globali della Tabella (B).

Attese le valutazioni suesposte, si ritiene di considerare le attività in esame a **bassa** probabilità di occorrenza di una minaccia.

Calcolo del rischio

Dopo aver valutato l'impatto (alto) dell'operazione di trattamento dei dati personali e la probabilità (bassa) di accadimento della minaccia, è possibile effettuare la valutazione finale del rischio.

L'incrocio dei due valori di *impatto* e *probabilità* ci fornisce l'indicazione del valore del rischio risultante.

		IMPATTO		
		BASSO	**MEDIO**	**ALTO / MOLTO ALTO ☑**
PROBABILITA'	**BASSA ☑**	**Rischio basso**	**Rischio medio**	**Rischio alto ☑**
	MEDIA	**Rischio basso**	**Rischio medio**	**Rischio alto**
	ALTA	**Rischio medio**	**Rischio alto**	**Rischio alto**

Come desumibile dalla tabella sopra riportata, pur avendo valutato come bassa la probabilità di occorrenza, la valutazione alta dell'impatto attribuito determina una valutazione complessiva di **Rischio alto** connessa alle attività oggetto della presente indagine.

Misure previste per ridurre il rischio

Al fine di ridurre il rischio, sono attualmente previste in azienda le seguenti precauzioni:

- nel gestionale aziendale sono previsti diversi livelli di accesso alle informazioni ivi contenute, differenziati in relazione alle mansioni svolte dal singolo dipendente;
- è previsto l'accesso ai dati particolari degli istanti/assegnatari esclusivamente da parte del personale in forza agli uffici Inquilinato, Manutenzioni e Protocollo, nonché da parte dalla Dirigenza aziendale;
- l'utilizzo della piattaforma informatica regionale, unica a livello di tutte le AATTER del Veneto, è consentito esclusivamente all'operatore autorizzato in possesso di password personale;
- è previsto il sistematico ricorso alla designazione di un Responsabile del trattamento dei dati, nei casi in cui ATER condivida dati personali degli istanti/assegnatari con soggetti terzi (ad esempio con la Regione, i Comuni, imprese esecutrici di lavori in appalto, …), attraverso la sottoscrizione di specifici accordi che disciplinano il trattamento dei dati;
- sono periodicamente previsti dei seminari di formazione in materia di *privacy* rivolti a tutto il personale aziendale (l'ultimo tenutosi nella giornata del 4 maggio 2021);
- la conservazione dei documenti in formato cartaceo contenenti dati personali di istanti/assegnatari avviene in armadi o locali non accessibili liberamente e custoditi sotto chiave.

Conclusioni

Pure considerato come alto il rischio potenzialmente connesso al trattamento di dati degli istanti in relazione alle attività di bandizione, redazione delle graduatorie e di assegnazione d'alloggio di edilizia sovvenzionata, si ritengono adeguate le misure di mitigazione del rischio adottate in azienda, la cui scrupolosa osservanza determina un rischio residuo accettabile.

La presente è stata redatta dall'*Ufficio affari generali, segreteria e protocollo* in data 29/04/2021, anche sulla base delle informazioni fornite dall'*Ufficio inquilinato*, nel cui ambito di operatività ricadono le procedure in esame. Anche sulla base delle informazioni tecniche fornite dall'*Ufficio sviluppo informatico*, per quanto di competenza.

Il presente documento è stato da ultimo modificato in data 01/09/2021, attese le osservazioni pervenute dal DPO aziendale.

Ufficio affari generali,
segreteria e protocollo.

dott. Fabrizio Fiabane

Con il visto della Direzione aziendale.

dott. Alberto Pinto

Sottoposto al vaglio del Consiglio di Amministrazione aziendale in data 09/09/2021.