# UNIONE LOMBARDA DEI COMUNI CENTURIATI DI BONEMERSE E MALAGNINO

PROVINCIA DI CREMONA

**ORIGINALE**
**Deliberazione n. 72** del **14.12.2023**

## VERBALE DI DELIBERAZIONE DELLA GIUNTA DELL'UNIONE

OGGETTO: **Approvazione valutazione d'impatto sulla protezione dei dati (DPIA) relativa ai canali di segnalazione per il 'whistleblowing'**

L'anno **duemilaventitre** e questo giorno **quattordici** del mese di **dicembre** alle ore **12.30** nella sala delle adunanze della Sede dell'Ente, si è riunita la Giunta dell'Unione convocata nelle forme di legge.

Presiede l'adunanza il Sig. **Luca Ferrarini** nella sua qualità di PRESIDENTE e sono rispettivamente presenti ed assenti i seguenti sigg.:

| NOME | INCARICO | Presente / Assente / Dimissionario |
|---|---|---|
| FERRARINI LUCA | PRESIDENTE | Presente |
| LOSITO DONATO | VICEPRESIDENTE | Presente |
| BERETTINI FRANCESCO | ASSESSORE | Presente |
| BEDANI IVANO | ASSESSORE | Assente |
| ZINI EUGENIO GIUSEPPE | ASSESSORE | Presente |
| GERVASI SERGIO | ASSESSORE | Assente |

Totale presenti: n. 4
Totale assenti: n. 2

Assiste il Segretario dell'Unione, Sig. **Matteo Malvicini,** incaricato della redazione del presente verbale.

IL PRESIDENTE

Constatato il numero degli intervenuti, invita i presenti alla trattazione dell'argomento indicato in oggetto.

## LA GIUNTA DELL'UNIONE

**VISTI:**

- la Deliberazione dell'Assemblea dell'Unione n. 2 del 14.03.2023 di approvazione della nota di aggiornamento al documento unico di programmazione (D.U.P.) per il periodo 2023/2025;
- la Deliberazione dell'Assemblea dell'Unione n. 3 del 14.03.2023 di approvazione del Bilancio di Previsione 2023/2025;
- la Deliberazione di Giunta dell'Unione n. 12 del 15.03.2023 con la quale è stato approvato il PEG anno 2023;
- la Deliberazione di Giunta dell'Unione n. 30 del 28.06.2023 con la quale è stato approvato il PIAO 2023/2025;

**VISTI**:

- la Legge n. 190 del 6 novembre 2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" con la quale è stato introdotto nell'Ordinamento italiano un sistema organico di disposizioni finalizzate alla prevenzione della corruzione e alla promozione dell'integrità in tutti i processi e le attività pubbliche;
- la Legge n. 179 del 30 novembre 2017 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".
- La Direttiva (UE) 2019/1937 del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
- Il D.lgs. 10/03/2023, n. 24: "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" entrato in vigore il 30 marzo 2023 con efficacia dal 15 luglio 2023, in particolare gli articoli:
  *Art. 1 Ambito di applicazione oggettivo Il presente decreto disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato. […].*
  *Art. 4 Canali di segnalazione interna I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali […], attivano, […] propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione […]"*
  *Art. 13. Trattamento dei dati personali […] 6 [I comuni …] definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018. […]";*

**RILEVATO** che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

**CONSIDERATO** che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

**TENUTO PRESENTE** che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

**DATO ATTO** che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

**RILEVATO CHE**, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

**VISTO** il D. lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

**DATO ATTO CHE**, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere:

- una "determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
- una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

**TENUTO PRESENTE** che la DPIA è una procedura prevista dall'art. 35 del Regolamento UE 206/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonchè i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;

**TENUTO PRESENTE** l'obbligo, in capo ai titolari, di consultare l'Autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

**RILEVATO** che la DPIA deve essere condotta prima di procedere al trattamento e che, deve comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari;

**DATO ATTO CHE** la responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione;

**TENUTO PRESENTE** che, ferma restando la discrezionalità dell'amministrazione nell'effettuare la determinazione preliminare e la valutazione di impatto, il Garante, con provvedimento n. 467 dell'11 ottobre 2018, ha reso pubblico l'Elenco delle tipologie di trattamenti da sottoporre OBBLIGATORIAMENTE a valutazione d'impatto, tra cui si menzionano:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

**TENUTO PRESENTE** che, ai sensi dell'art. 29 delle linee guida elaborate dal Gruppo di Lavoro 29 per la protezione dei dati, la DPIA, non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche
- hanno natura, ambito, contesto, e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni non hanno subito modifiche
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA
- fanno riferimento a norme e regolamenti per la cui definizione è stata condotta una DPIA

**RILEVATO CHE**, per quanto sopra, è necessario istituire:

1. una "Determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
2. una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

**CONSIDERATO che:**

- Il decreto legislativo 10 marzo 2023 n. 24, divenuto efficace il 15 luglio 2023, disciplina la materia del whistleblowing, abrogando le normative precedentemente in vigore in materia.
- Tale decreto disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica *o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato"*.
- Il segnalante, peraltro, può fare la segnalazione, trovando la tutela fornita dal d.lgs. 24/2023, non solo durante il rapporto di lavoro, bensì anche prima che sia iniziato il rapporto stesso, qualora la segnalazione riguardi violazioni rilevate durante il processo di selezione o in altre fasi precontrattuali oppure durante il periodo di prova.
- La tutela è garantita anche nel caso di segnalazione fatta in seguito alla cessazione del rapporto di lavoro, sempreché la segnalazione riguardi una violazione di cui il segnalante è venuto a conoscenza nel corso del rapporto di lavoro.
- La novità di tale decreto risiede non tanto nella trattazione della materia, che peraltro veniva già precedentemente trattata, quanto nella tutela che viene apprestata alla figura del segnalante e alle altre figure che coadiuvano il segnalante.
- L'obiettivo di questo decreto non è solo quello di incentivare le segnalazioni, ma soprattutto di tutelare la riservatezza sull'identità del segnalante e delle persone coinvolte nella segnalazione.
- Un'altra importante novità che il decreto introduce riguarda la necessaria previsione di un canale di segnalazione interna, il quale deve prevedere più modalità di segnalazione, lasciando al segnalante la possibilità di scegliere quale utilizzare.

**VISTA** La delibera dell'ANAC Delibera n. 311 del 12 luglio 2023 – "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone

che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne", che in particolare prevede:

"Paragrafo 3.1. – I canali interni

[…] Istituzione dei canali di segnalazione … Nell'atto organizzativo, adottato dall'organo di indirizzo, è opportuno che almeno vengano definiti:

- ➢ il ruolo e i compiti dei soggetti che gestiscono le segnalazioni;
- ➢ le modalità e i termini di conservazione dei dati, appropriati e proporzionati in relazione alla procedura di whistleblowing e alle disposizioni di legge. […]

I canali di segnalazione interna devono garantire la riservatezza, anche tramite il ricorso a strumenti di crittografia, ove siano utilizzati strumenti informatici:

- ➢ della persona segnalante;
- ➢ del facilitatore;
- ➢ della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- ➢ del contenuto della segnalazione e della relativa documentazione.

Inoltre, al fine di agevolare il segnalante, a quest'ultimo va garantita la scelta fra diverse modalità di segnalazione:

- ➢ in forma scritta, anche con modalità informatiche (piattaforma online). La posta elettronica ordinaria e la PEC si ritiene siano strumenti non adeguati a garantire la riservatezza. Qualora si utilizzino canali e tecniche tradizionali, da disciplinare nell'atto organizzativo, è opportuno indicare gli strumenti previsti per garantire la riservatezza richiesta dalla normativa.
- ➢ in forma orale, alternativamente, attraverso linee telefoniche, con sistemi di messaggistica vocale, ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. […]"

**DATO ATTO CHE** il provvedimento, attuativo della direttiva europea 2019/1937, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato e prescrive l'obbligatorietà della DPIA per la gestione delle segnalazioni attraverso piattaforme esterne. Il trattamento di cui alla presente DPIA riguarda l'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo.

**VISTI**:

- il D.Lgs. 18 agosto 2000, n. 267, e successive modificazioni, recante: "Testo unico delle leggi sull'ordinamento degli enti locali";
- il vigente "Regolamento dell'Ente sull'ordinamento degli uffici e dei servizi";
- la legge 7 agosto 1990, n. 241 e successive modificazioni, recante: "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- il D.Lgs. 30 giugno 2003, n. 196, recante: "Codice in materia di protezione dei dati personali", per quanto tuttora in vigore;
- il Regolamento UE 2016/679 del 27 aprile 2016 relativo alla "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati";
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida sul diritto alla “portabilità dei dati” - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l’individuazione dell’autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto dell’Ente;
- Circolari e direttive del RPC;

**RICHIAMATA** la Deliberazione della Giunta dell’Unione n. 58 del 11.11.2023 avente ad oggetto “Istituzione del canale interno per le segnalazioni di cui al d.lgs. 10/03/2023 n. 24 e misure a tutela del whistleblower”;

**RITENUTO,** per le motivazioni che precedono, di approvare la Valutazione d’impatto sulla protezione dei dati (DPIA) relativa all'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo, ai sensi del Regolamento (UE) n.679/2016 e del D.Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

**DATO ATTO CHE** il responsabile del procedimento, è il Segretario dell’Ente, e che lo stesso, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità dei trattamenti oggetto di DPIA, nonché delle misure tecniche e organizzative individuate dai titolari per mitigare l’impatto del trattamento, è tenuto a garantire la conoscibilità della Valutazione d’impatto sulla protezione dei dati (DPIA) a tutti i dipendenti dell’Ente;

**VISTO** il parere favorevole espresso dal Segretario dell’Ente, in qualità di Responsabile del Servizio amministrativo in ordine alla regolarità del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

**DATO ATTO** che dal presente provvedimento non derivano impatti economici o patrimoniali a carico del bilancio dell’Ente e che dunque non risulta necessaria l’espressione del parere di regolarità contabile del Responsabile del Servizio finanziario ai sensi e per gli effetti degli artt. 49 del D.Lgs. 18.08.2000, n. 267;

**CON VOTI** unanimi favorevoli, resi nelle forme di legge

## DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. **DI APPROVARE** la Valutazione d’impatto sulla protezione dei dati (DPIA) relativa all'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito

del contesto lavorativo, ai sensi del Regolamento (UE) n.679/2016 e del D.Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

2. **DI DISPORRE** che al presente provvedimento venga assicurata:
   a) la pubblicità legale con pubblicazione all'Albo Pretorio per 15 gg. consecutivi;
   b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";

3. **DI DARE ATTO** che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.

4. **DI DISPORRE** che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

5. **DI DARE ATTO**, ai sensi dell'art. 3 della Legge n. 241/90 e ss.mm.ii. sul procedimento amministrativo, che qualunque soggetto ritenga il presente atto illegittimo e si ritenga dallo stesso direttamente leso, può proporre ricorso innanzi al Tribunale Amministrativo Regionale, Sezione di Brescia, al quale è possibile presentare i propri rilievi in ordine alla legittimità del presente atto, entro e non oltre 60 giorni dall'ultimo di pubblicazione all'Albo on line;

6. **DI DICHIARARE**, con apposita separata votazione e con voti unanimi favorevoli, resi nelle forme di legge, la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, 4° comma, del D.Lgs. 18.08.2000, n. 267.

Letto, confermato e sottoscritto:

| Il Presidente<br>Luca Ferrarini | Il Segretario dell'Unione<br>Matteo Malvicini |
|---|---|

Firmato da:
FERRARINI LUCA
Codice fiscale: FRRLCU73A21D150C
Valido da: 30-11-2021 11:53:32 a: 30-11-2024 01:00:00
Certificato emesso da: InfoCamere Qualified Electronic Signature CA, InfoCamere S.C.p.A., IT
Riferimento temporale 'SigningTime': 21-12-2023 14:43:11
Motivo: Approvo il documento

Firmato da:
Malvicini Matteo
Codice fiscale: MLVMTT77C04D150B
Valido da: 11-12-2023 11:44:08 a: 11-12-2026 01:00:00
Certificato emesso da: InfoCamere Qualified Electronic Signature CA, InfoCamere S.C.p.A., IT
Riferimento temporale 'SigningTime': 21-12-2023 14:36:19
Motivo: Approvo il documento