Comune di Cinisello Balsamo

Valutazione di impatto sulla protezione dei dati del sistema di accertamento delle infrazioni di cui all'Art. 142 CDS mediante apparecchiatura autovelox in postazione fissa

(*Data protection impact assessment* o "DPIA")

Informazioni sulla DPIA

Nome della DPIA
DPIA del sistema di accertamento delle infrazioni di cui all'Art. 142 Codice della Strada (CDS) mediante postazioni fisse, del Comune di Cinisello Balsamo

Nome autore
Commissario di Polizia Locale ADAMOLI Velasco

Nome valutatore
Comandante della Polizia Locale CRIPPA Fabio massimo

Data di creazione
25/02/2025

Nome del DPO/RPD
SALVI Manuel

Richiesta del parere degli interessati
Non è stato richiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Questo trattamento ex-lege non prevede il consenso/parere degli interessati.

Panoramica del trattamento

Quale è il trattamento in considerazione?

- Sistema di accertamento di infrazioni all'Art. 142 del Codice della Strada, mediante dispositivi approvati/omologati ai sensi del D.Lgs 285/92 e del DPR 495/92 ai fini esclusivi dell'applicazione delle sanzioni amministrative previste in caso del superamento dei limiti di velocità, nell'ambito delle funzioni proprie della Polizia Locale, attraverso l'uso di sistemi di rilevazione automatica (autovelox) delle targhe dei veicoli che commettano le predette infrazioni.

Quali sono le responsabilità connesse al trattamento?

- Titolare del trattamento è il Comune di Cinisello Balsamo

- Soggetti designati o autorizzati: Il Comandante ed i dipendenti del corpo di Polizia Locale (agenti di pubblica sicurezza) che possono trattare i dati personali e che hanno accesso al sistema di accertamento delle infrazioni mediante apparecchiatura autovelox,

Dati, processi e risorse di supporto

Quali sono i dati trattati?

- Numeri di targa acquisiti mediante autovelox con software di lettura targhe;
- Immagini di contesto raccolte tramite fotocamere;

Tali dati verranno, in fase di verifica ed accertamento dell'infrazione, correlati alle banche dati disponibili al Corpo di Polizia Locale, per redigere il verbale sanzionatorio e provvedere alle necessarie attività amministrative correlate.
I dati ulteriormente trattati per finalità amministrative sono:

- Dati anagrafici
- Dati relativi i documenti di guida e circolazione

- Dati relativi il proprietario del veicolo

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

ACQUISIZIONE:

I dispositivi acquisiscono immagini di contesto, accompagnate da ulteriori informazioni quali targhe di autoveicoli che vengono ripresi solo qualora transitino in prossimità dei sistemi di rilevazione della velocità, superando i limiti fissati sulla strada, con i relativi riferimenti temporali e di velocità rilevata.

TRASMISSIONE:

La trasmissione dei dati avviene su una rete privata, di proprietà del Comune, in fibra ottica e non connessa a reti pubbliche o Internet. Il traffico dati è separato anche dalle altre reti comunali, mediante una VLAN dedicata esclusivamente agli autovelox, diversa anche dalla rete della videosorveglianza generica.
La fibra ottica raggiunge su percorsi ridondati le 2 sale server on premise del Comune, la capacità di banda di 2 Gbit/s è idonea al trasferimento delle immagini ed eventuali altri contenuti di contesto.
I dati sono quindi inviati ad un server che si trova on premise nei datacenter Comunali.

MEMORIZZAZIONE:

Un server virtuale dedicato agli autovelox, presso i datacenter onpremise del Comune, è connesso sia alla rete dedicata agli autovelox, sia alla rete locale degli uffici della Polizia Locale.
Il personale autorizzato accede al server, da postazioni di lavoro predeterminate e mediante credenziali nominative.
Il server onpremise del Comune sono in configurazione di business continuity: i dati sono scritti in modo sincrono su storage paralleli nelle 2 sale server.

CONSERVAZIONE:

I dati relativi agli impianti di lettura targhe vengono registrati tramite autovelox approvati/omologati e conformi alle norme ministeriali, tipo autovelox MOD 106. Lo storage di archiviazione viene trasferito con cadenza periodica nel sistema di gestione delle infrazioni al CDS, in uso al Comando di Polizia Locale.

Le informazioni sono conservate e trattate per tutto il periodo necessario alla gestione dell'illecito amministrativo, comprese eventuali contestazioni e ricorsi.

Quali sono le risorse di supporto ai dati?

Il sistema è composto dalle seguenti componenti:

- Sistemi di acquisizione: composti da telecamere di lettura targhe
- Sistemi di trasmissione: switch di rete managed, protetti da UPS e cavo di rete in fibra ottica.
- Sistemi di memorizzazione: n. 1 server virtuale dedicato, con sistema operativo Linux Debian

Principi Fondamentali

Proporzionalità e necessità

Quai sono le finalità del trattamento?

La finalità del trattamento, mediante l'accertamento delle infrazioni di cui all'Art. 142 del Codice della Strada, attraverso sistema autovelox a postazione fissa, è incentivare il rispetto del codice della strada, contrastare il superamento dei limiti di velocità, riducendo il tasso di incidenti e preservando vite umane.

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento e i dati trattati:

- Sono conformi al principio di minimizzazione dei dati acquisiti e trattati, sono esplicitati nelle informative rese agli interessati, mediante cartellonistica e informativa estesa presente sul sito web comunale e a disposizione su richiesta in formato cartaceo;
- Sono legittime in quanto supportate da idonea base giuridica;
- Sono legittime in quanto perseguono finalità di interesse pubblico.

Il trattamento dei dati personali è conforme al principio di limitazione della finalità di cui all'art. 5 par. 1 lett. b) del GDPR.

In particolare, le finalità del trattamento sono:

- Specifiche ed esplicite: le finalità del trattamento sono indicate specificamente nell'informativa di primo livello (cartellonistica), nell'informativa di secondo livello (informativa estesa sul sito internet dell'ente).
- Legittime: le finalità del trattamento sono supportate da idonea base giuridica, rappresentata nello specifico dall'art. 6 par. 1 lett. e) del GDPR.

La proporzionalità del trattamento rispetto alle finalità perseguite è giustificata dal fatto che sulle strade in cui sono posizionati i sistemi di rilevamento della velocità mediante postazione fissa, si sono verificati diversi incidenti stradali proprio a causa del superamento dei limiti di velocità e che solo grazie all'impiego degli strumenti di rilevamento automatico, si rende possibile ridurre nella pericolosità e nella quantità.

Quali sono le basi giuridiche che rendono lecito il trattamento?

La base giuridica che legittima il trattamento è rappresentata dall'art. 6 lett. e) del Regolamento UE 2016/679 secondo cui il trattamento è svolto per l'esecuzione di un compito di interesse pubblico o comunque connesso all'esercizio di pubblici poteri.

In particolare, il trattamento trova la sua base giuridica principale nel Decreto legislativo n.285/92 (cs Codice della Strada) e in particolar modo nell'Art. 142 "Limiti di velocità".

I dati trattati sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati trattati sono esclusivamente quelli necessari per le finalità perseguite in ordine all'accertamento delle infrazioni di cui all'Art. 142 CDS.

Il sistema di fotocamere dedicate alla lettura delle targhe riprende sono dotate effettua lo zoom sulle targhe dei veicoli in passaggio, oltre a fornire una foto di contesto.

I dati sono esatti e aggiornati?

Le immagini di contesto e le targhe raccolte sono esatti. Nel caso di errata lettura per qualsiasi ragione, la foto non viene scattata.

Qual è il periodo di conservazione dei dati?

Come previsto nel Regolamento comunale sulla videosorveglianza, i termini di conservazione dei dati sono stabiliti in conformità alla normativa applicabile sia europea sia di livello nazionale (GDPR, D.lgs. n. 51 del 2018, Provvedimenti Garante Privacy, eventuale normativa o provvedimenti o circolari speciale per casistiche specifiche). I termini di conservazione delle immagini e delle videoriprese sono determinati considerando ciascuna finalità in concreto perseguita e sulla base del principio di limitazione della conservazione di cui all'art. 5 par. 1 lett. e) del Regolamento (UE) 2016/679

e di cui all'art. 3 comma 1 lett. e) del D.lgs. n. 51/2018 attuativo della Direttiva (UE) 2016/680.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

- Cartellonistica conforme alle indicazioni fornite dall'EDPB;
- Informativa estesa reperibile sul sito web istituzionale;

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

L'accesso ai dati è regolato secondo le norme di cui alla Legge n.241/90 e ss.mm.ii. Essi sono altresì resi disponibili mediante il sistema di gestione delle infrazioni amministrative per il cui impiego sono state adempiute le formalità di cui all'Art. 28 GDPR.

Gli interessati possono esercitare i propri diritti scrivendo direttamente al Data Protection Officer, nominato dall'Ente, all'indirizzo email:dpo-cb@comune.cinisello-balsamo.mi.it .
Sarà effettuata quindi una valutazione da parte del DPO volta a determinare, caso per caso, quali diritti potranno essere esercitati o quali di essi potranno essere negati.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono esercitare i propri diritti scrivendo direttamente al Data Protection Officer, nominato dall'Ente, all'indirizzo email: dpo-cb@comune.cinisello-balsamo.mi.it .
Sarà effettuata quindi una valutazione da parte del DPO volta a determinare, caso per caso, quali diritti potranno essere esercitati o quali di essi potranno essere negati.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare i propri diritti scrivendo direttamente al Data Protection Officer, nominato dall'Ente, all'indirizzo email:dpo-cb@comune.cinisello-balsamo.mi.it .
Sarà effettuata quindi una valutazione da parte del DPO volta a determinare, caso per caso, quali diritti potranno essere esercitati o quali di essi potranno essere negati.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto o atto di nomina?

La manutenzione degli impianti di videosorveglianza è regolamentata da apposito contratto o atto di nomina.All'interno del contratto o atto di nomina sono indicate le modalità operative per effettuare la manutenzione.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono trasferiti al di fuori dell'Unione europea o dello Spazio economico europeo (SEE).

Rischi

Misure esistenti o pianificate

Crittografia

La trasmissione dei dati avviene su rete (VLAN) dedicata agli autovelox e chiusa (priva di gateway di routing), non connessa ed Internet o altre reti pubbliche e separata sia da altre reti comunali che dalla rete della videosorveglianza comunale . In conformità rispetto a quanto richiesto al paragrafo 3.3.1 comma f) dal "Provvedimento in Materia di Videosorveglianza" dell'8 aprile 2010 del Garante per la protezione dei dati personali, qualora le telecamere lo consentano, il protocollo SFTP, con crittografia SSL, viene usato prioritariamente rispetto alla trasmissione dati in chiaro, per trasferire le immagini dalle telecamere al server, la crittografia costituisce un elemento aggiuntivo rispetto alla segregazione della rete, già descritta nel paragrafo precedente.

Controllo degli accessi logici

La consultazione dei dati acquisiti avviene attraverso l'accesso a piattaforma dedicata.

I profili di accesso alla piattaforma sono nominali. Ad ogni utente vengono assegnati credenziali d'accesso.

Ogni utente è dotato di apposito profilo che va a caratterizzare le attività che possono o non possono essere effettuate.

Tracciabilità

Il sistema è dotato di sistema di registrazione degli accessi (Log).

Archiviazione

I dati sono memorizzati su n. 1 Server virtuale on premise con storage ridondato in modo sincrono presso le 2 sale server del Comune, ubicate presso il Comando della Polizia Locale e presso il Municipio. L'accesso alla sala server è regolato tramite apposito badge.

Vulnerabilità

- Profilazione di accesso al server: l'accesso al Server sul quale sono conservati i dati legati agli impianti di lettura targhe è consentito ai sistemisti CED con specifica formazione, dipendenti del Comune di Cinisello Balsamo;
- Sono stati installati gli aggiornamenti di Linux Debian;
- L'interfaccia web per la gestione dell'applicativo utilizza certificati attivi e con algoritmi in grado di garantire adeguati standard di sicurezza;
- L'interfaccia web utilizza dei protocolli di sicurezza adeguatamente aggiornati;

L'accesso alla sala deputata ad ospitare gli apparati è regolato da elettroserratura apribile tramite badge nominativo; tale accesso è consentito alle sole persone autorizzate.

Gli accessi al software sono regolati da user e password e relativi profili.

Manutenzione

La manutenzione del Sistema è regolata da apposito contratto sottoscritto dal Titolare e dal Responsabile del trattamento.

Il soggetto manutentore può effettuare manutenzione solo previa autorizzazione e supervisione da parte di personale incaricato.

Sicurezza dell'hardware

È presente l'inventario Hardware e Software, che viene regolarmente aggiornato.

Politica di tutela della privacy

E' stato nominato il Data Protection Officer

E' stato nominato il Designato al trattamento dei dati

È stata predisposta una informativa estesa sul trattamento dei dati personali nell'ambito del sistema di rilevamento delle infrazioni di cui all'Art. 142 CDS mediante postazioni fisse.

Gestione dei rischi

Sono stati debitamente mappati i trattamenti tramite apposito registro. La costituzione della presente DPIA include l'analisi del rischio per i diritti e le libertà degli interessati

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'Ente si è dotato di apposita policy per la gestione delle violazioni di dati personali (c.d. DataBreach).

In particolare è stata creata una procedura web per la segnalazione di un data breach.

Il personale è stato debitamente formato per la gestione delle suddette violazioni.

Gestione del personale

È stata effettuata adeguata formazione del personale in materia di protezione dei dati personali.

Vengono effettuate sessioni formative specifiche in base all'evoluzione della normativa in materia.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Compromissione della riservatezza degli interessati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Accesso abusivo al sistema dell'Ente;
- Furto o smarrimento dei supporti di memorizzazione;
- Accesso non autorizzato da parte del Responsabile del trattamento;
- Malware;
- Obsolescenza e/o mancato aggiornamento dei dispositivi;
- Accesso di personale interno non autorizzato.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne;
- Fonti non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Crittografia;
- Sicurezza dei canali informatici;
- Manutenzione;
- Controllo degli accessi fisici;
- Controllo degli accessi logici;
- Tracciabilità;
- Sicurezza dell'hardware;
- Gestione dei rischi;
- Gestione del personale.
- Videosorveglianza nei pressi delle postazioni fisse di rilevamento della velocità.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Bassa. L'accesso illegittimo potrebbe comportare un danno reputazionale nei confronti degli interessati causato da una perdita di riservatezza. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile. Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascurabile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

- Alterazione delle targhe degli automezzi e conseguente sanzione a carico di ignoti;
- Impossibilità di perseguire la violazione commessa in caso di alterazione delle immagini;
- Danno reputazionale nei confronti degli interessati in caso di diffusione illecita dei dati.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

- Alterazione delle immagini;
- Malware;
- Accesso abusivo al sistema dell'Ente;
- Accesso non autorizzato da parte del Responsabile del trattamento;
- Accesso di personale interno non autorizzato;
- Malfunzionamento software.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne;
- Fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Crittografia;
- Sicurezza dei canali informatici;

- Manutenzione;
- Controllo degli accessi fisici;
- Controllo degli accessi logici;
- Tracciabilità;
- Sicurezza dell'hardware;
- Gestione dei rischi;
- Gestione del personale.
- Videosorveglianza nei pressi delle postazioni fisse di rilevamento della velocità.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Molto bassa. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile. Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascura- bile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Mancata impossibilità di elevare verbali di accertamento a carico dei soggetti resisi responsabili delle violazioni di cui all'Art. 142 CDS.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

- Eventi naturali;
- Guasti hardware;
- Malfunzionamento software;
- Manomissione delle fotocamere;
- Interruzione dei canali di trasmissione;
- Malware;
- Manomissione dell'infrastruttura.

Quali sono le fonti di rischio?

- Fonti umane interne;
- Fonti umane esterne;
- Fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Controllo degli accessi fisici;
- Controllo degli accessi logici;
- Tracciabilità;
- Archiviazione;
- Manutenzione;

- Sicurezza dell'hardware;
- Contratto con il Responsabile del trattamento;
- Gestione del personale.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Molto Bassa. L'adozione di molteplici misure di attenuazione del rischio mitigano la gravità del rischio stesso.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile. Alla luce delle misure tecniche e organizzative adottate, si stima che la probabilità del rischio sia trascurabile, al netto del possibile impatto sui diritti e sulle libertà degli interessati qualora dovesse verificarsi una violazione di dati personali.

Piano d'azione

Principi fondamentali

Il piano d'azione cui si impegna il titolare è finalizzato a conformare il trattamento in questione ai principi e alle norme applicabili in materia di videosorveglianza e trattamento dei dati personali, in modo tale che le criticità evidenziate siano rimediate e che l'impianto possa essere rimesso in funzione.

In seguito al contributo di analisi del DPO, dunque, il titolare si impegna ad adottare le misure indicate nella sezione sottostante.

Misure pianificate

Piano d'azione:

- Effettuare a cadenza periodica la Valutazione di impatto;
- Formazione continuativa del personale interno in materia di protezione dei dati personali;
- Mantenere costantemente adeguato il sistema informatico;
- Effettuazione a cedenza periodica, da parte del soggetto manutentore degli impianti, di verifiche delle apparecchiature sulle quali non è possibile attivare un aggiornamento automatico.

Annotazioni:

Non si ritiene necessaria la consultazione preventiva di cui all'Art. 36 GDPR

Commento D.P.O.

Letto il documento e suggerito alcuni correttivi migliorativi, le considerazioni svolte all'interno dello stesso sono considerate accettabili e congrue.

FABIO
MASSIMO
CRIPPA
18.03.2025
15:42:01
GMT+01:00