Why TownSafe is GDPR Compliant

(when using Police / PubWatch Watchlist Images)

Summary Statement

TownSafe processes only those images already lawfully maintained by PubWatch schemes for the prevention of crime within licensed premises. The system does not create new offender records or make automated decisions, but assists venue staff in performing required manual watchlist checks more consistently. All alerts require human review prior to action, and data is processed in accordance with Article 10 UK GDPR and Schedule 1 of the Data Protection Act 2018 for the purpose of crime prevention and public safety.

In Detail

1. The images used by PubWatch are Criminal Offence Data

Police custody images (mugshots) used within PubWatch exclusion schemes are classed under UK GDPR as:

> *“personal data relating to criminal convictions and offences”*

This type of data receives **additional legal protection** under:

- **Article 10 UK GDPR**
- **Data Protection Act 2018 Schedule 1**

and **cannot be processed in the same way as normal personal data**.

---

2. PubWatch already has a lawful basis to hold this data

Local PubWatch schemes operate for:

- prevention of crime
- protection of staff
- enforcement of exclusion orders
- safeguarding licensed premises

UK law specifically allows the processing of criminal offence data where it is:

> *“authorised by domestic law providing appropriate safeguards”*

In the UK this authorisation is provided through:

- **Data Protection Act 2018 – Schedule 1 conditions**

including:

✔ Preventing unlawful acts
✔ Protecting the public against dishonesty, violence or anti-social behaviour
✔ Safeguarding individuals at risk

Processing is lawful where it is:

> **necessary and proportionate for the purpose of crime prevention**

---

3. TownSafe does NOT create a new watchlist

This is the **most important GDPR point**.

TownSafe:

- ✗ does not generate new criminal records
- ✗ does not build an independent offender database
- ✗ does not determine guilt
- ✗ does not issue bans
- ✗ does not make automated decisions

Instead:

- ✓ uses the **existing PubWatch exclusion list**
- ✓ processes images already lawfully held by PubWatch
- ✓ assists staff in performing a check that they are already required to carry out manually

Participating venues are already obligated to visually compare entrants against:

- PubWatch App images
- printed exclusion sheets
- circulated custody photographs

TownSafe simply improves the **consistency** of this legally required manual process.

---

4. Human Review is Always Required

UK GDPR prohibits automated decision-making in cases which may significantly affect individuals.

TownSafe:

- ✔ flags a *possible* match only
- ✔ sends the image to venue staff
- ✔ requires a human decision before any action is taken

No automated refusal of entry occurs.

This keeps TownSafe fully aligned with:

- Article 22 UK GDPR
- ICO guidance on surveillance systems

---

5. Data Minimisation & Retention

TownSafe systems:

- ✔ store only name + image already on PubWatch list
- ✔ do not retain facial recognition templates long-term
- ✔ do not continuously track individuals
- ✔ timestamp potential matches
- ✔ automatically delete unmatched images

UK GDPR requires personal data to be:

> *“adequate, relevant and not excessive”*

TownSafe is designed specifically around this principle.

---

6. Substantial Public Interest

Hospitality watchlists exist to:

- reduce violence
- prevent repeat offending
- safeguard staff and customers
- enforce legally issued exclusion notices

UK GDPR allows criminal offence data processing where it supports:

- ✔ crime prevention
- ✔ public safety
- ✔ protection of individuals

under **Substantial Public Interest conditions** in the
Data Protection Act 2018 Schedule 1.

TownSafe operates solely for these purposes.