

s40(2)

Founder
Facewatch Limited

By email only to: s40(2)@facewatch.co.uk

28 March 2023

Dear s40(2),

Facewatch Limited

I am writing to inform you that the Information Commissioner's Office ("ICO"), has now completed its investigation in relation to Facewatch Limited ("Facewatch"). The ICO conducted an investigation to understand Facewatch, and the processing activities conducted by your organisation.

This inquiry has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved. We refer to the UK GDPR and the DPA 2018 together as the 'data protection legislation'.

We understand that the purpose of Facewatch is to assist businesses to minimise unlawful acts from occurring in their premises. By using their Live Facial Recognition ("LFR") service to process the personal data of individuals who are suspected of having committed a criminal act, Facewatch aims to alert their subscribers to criminal activity in order to prevent and deter the act before it takes place. A key element of Facewatch's service is the shared national facial recognition watchlist. This enables subscribers to receive an alert when a subject of interest ("SOI") has been identified and uploaded to a watchlist by another organisation.

Our consideration of this case

We have investigated whether Facewatch has complied with the requirements of the data protection legislation. We have noted that Facewatch has been cooperative throughout – engaging with the ICO site visits and investigatory interviews, and responding to information requests in a timely manner.

During the course of our investigation, the ICO sent Facewatch a Compliance Assessment letter dated 09 February 2022 which outlined the ICO's position in relation to Facewatch's compliance with the data protection legislation, based on the documentation Facewatch had provided. We concluded that Facewatch's

processing of personal data failed to balance the legitimate interest of Facewatch and their subscribers against the rights and freedoms of individuals. The ICO advised Facewatch that the following data protection legislation had been breached:

- Article 5(1)(a) – lawfulness, fairness and transparency;
- Article 5(1)(b) – purpose limitation;
- Article 5(1)(e) – storage limitation;
- Article 6 – lawfulness of processing;
- Article 9 – processing of special categories of data;
- Article 10 – processing of personal data relating to criminal convictions and offences; and
- Recital 38 – the rights of children
- Schedule 1, Part 2, s10 of the DPA 18.

We agreed that the purpose of preventing and deterring criminal activity is in the legitimate interest of Facewatch and their subscribers. Legal gateways in the data protection legislation allow biometric data to be processed for this purpose.

The ICO provided Facewatch with the opportunity to respond to our conclusions. In mitigation, Facewatch sent further information on the 10 March 2022 and 21 November 2022, alongside our Information Request letter dated 22 September 2022.

The ICO welcomes the below steps, which have already been, or will be, actioned by Facewatch:

- [REDACTED]
- [REDACTED]

[Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

[Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

After careful consideration, and based on the information Facewatch has provided to date, we have decided that regulatory action is not required in this case.

However, it is important to note that whilst we have decided that regulatory action is not required in this case, you should consider the following information to ensure continued compliance with the relevant data protection legislation.

Further Action Recommended

- [REDACTED]
- [REDACTED]
- You should put into practice a regular audit review of your policies and procedures, and ensure the assessment is appropriately documented with any limitations and areas for improvement highlighted. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] You may wish to review the

ICO's guidance on [audits](#);

- You should regularly review and update your privacy policy, and highlight any areas for improvement. This will help ensure Facewatch's compliance with Article 5 (1)(a) of the UK GDPR, and provide individuals with the necessary information to understand Facewatch's processing and assert their data rights accordingly. You may wish to review the ICO's guidance on [transparency](#) for further information;
- You should keep your legitimate interests assessment (LIA) under regular review, and identify any changes to Facewatch's processing, such as the nature, purpose or context, that may affect the rights and freedoms of data subjects. If new and unforeseen elements are identified upon the conclusion of your review, consider whether further safeguards are needed. You may wish to review the ICO's guidance on [LIA](#);
- You should ensure your DPIA is under regular review, and update it as appropriate. We advise organisations to view their DPIA as an on-going process, in order to identify and mitigate against any potential risks that may impact individuals. For further information, please see the ICO's guidance on [DPIA](#);
- You should regularly review and update your risk matrix, and identify any areas that require further monitoring;
- [REDACTED]
- You should ensure all processes and procedures concerning the requirements of your DPO are well documented. Whilst the DPO is an asset to your organisation, the individual may leave and a replacement would be required. This will ensure a consistent approach is maintained as operations grow and assist your organisation in keeping to its data protection obligations. You may wish to review the ICO's guidance on [DPOs](#) for further

information;

- You may wish to review the ICO's guidance about processing personal data, and your organisation's obligations under the data protection legislation. For further information about compliance with relevant data protection legislation, you may wish to visit our website here:
[https://ico.org.uk/for-organisations/;](https://ico.org.uk/for-organisations/)

Please note that if further information relating to this incident comes to light, or if any further incidents involving Facewatch are reported to us, we will revisit this matter, and enforcement action may be considered as a result.

Thank you for your co-operation and assistance during the course of our inquiry.

We now consider the matter closed.

Yours sincerely,

Sally Anne Poole
Group Manager - High Priority Inquiries
Regulatory Supervision Service
Information Commissioner's Office

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (<https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/>).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

