| Version | Description of Change | Author | Approved | Version Date |
|---|---|---|---|---|
| 10 | Amended "criminal data" to personal data for uploaded data of soi's | Dave Sumner (DPO) | Simon Gordon (Chairman) | 10/12/19 |
| 9 | Updated lawful basis for criminal offence data following QC final report | Simon Gordon (Chairman) | Dave Sumner (DPO) | 05/06/19 |
| 7 & 8 | Added sections 2 and 4 following customer enquiry plus signage section 5 | Dave Sumner (DPO) | Simon Gordon (Chairman) | 10/05/19 |
| 6 | Review by Queens Counsel | Dave Sumner (DPO) | Dean Armstrong QC | 27/02/19 |
| 5 | Public Interest removed as legal basis so that Legitimate Interest is the sole legal basis | Dave Sumner (DPO) | Dave Sumner (DPO) | 02/02/19 |
| 4 | Incorporate clarifications for Legitimate interest following Counsel comments | Simon Gordon (Chairman) | Dave Sumner (DPO) | 01/01/19 |
| 2 & 3 | Re-format and review with D Sumner | Simon Gordon (Chairman) | Dave Sumner (DPO) | 12/9/18 |
| 1 | Initial version prepared by D Sumner, GDPR expert | Dave Sumner (DPO) | Simon Gordon (Chairman) | 31/7/18 |

Important disclaimer:

Please note this guidance note is prepared by Facewatch to assist you in complying with the Data Protection Act 2018 (DPA) when using the Facewatch system. Whilst every care has been taken to provide accurate guidance it is your responsibility to review the regulations and ensure compliance with the DPA, taking any legal advice you consider necessary.

## 1. Introduction

As a Facewatch customer you will have access to watchlists and/or facial recognition alerts about Subjects of Interest (SOIs).

Whilst Facewatch is the primary Data Controller and is responsible for sharing of all data, your business acts as a Data Controller, and is therefore responsible for, processing personal data when it conducts any of the following:

- Records and stores images of people on CCTV;
- Records details of crimes committed (criminal offence data);
- Uploads images of people reasonably suspected of crime or disorder to Facewatch (personal data);
- Receives and acts on facial recognition alerts;
- Updates or deletes that information.

This guidance note is to help you with preparation of the documentation required under the Data Protection Act 2018.

**Facewatch has received advice from a leading expert in data protection, Dean Armstrong QC to confirm its compliance with GDPR and DPA 2018. This advice does not cover anyone other than Facewatch and this document is for guidance only – you must take your own legal advice where necessary.**

## 2. ICO Registration number

Most companies will be registered with the ICO and fully conversant with data protection legislation but if you are a small company or sole trader and unsure this section explains more.

The ICO (Information Commissioners Office) is the body that ensures businesses comply with data protection legislation. We request your ICO registration number as part of the legal documentation just to make sure that all our customers have considered their responsibilities for complying with data protection legislation.

Your legal entity will need to be registered with the ICO even if you only use CCTV or hold computer records of your staff. Registration is simple and inexpensive for small companies – please see here for a simple guide from the ICO.

## 3. Data Protection Impact Assessment (DPIA)

A DPIA is a process to help you identify and minimise the data protection risks to individuals when processing personal data.

As a Data Controller you must perform a DPIA for processing that is likely to result in a high risk to individuals. There is unlikely to be a high risk if your business conducts this processing for the purposes of crime prevention and detection in line with your business' procedures, the 6 Data Protection Principles[1] and the Facewatch Subscriber Agreement.

[1] DPA Principles (1) used fairly, lawfully and transparently; (2) used for specified, explicit purposes; (3) used in a way that is adequate, relevant and limited to only what is necessary; (4) accurate and, where necessary,

However, it is good practice to prepare a DPIA for any processing of personal data where there is a risk to individuals from such things as human error, misuse, unauthorised access or a disproportionate response.

A DPIA, whilst not strictly necessary in most cases, will help you identify the measures your business takes in order to reduce the likelihood or impact of those risks, and thereby fulfil both the Accountability Principle and the requirement for Data Protection by Design and Default contained within the UK Data Protection Act 2018 and GDPR.

The ICO guidance on DPIA's can be found on the ICO website here.

To assist you to assess risks to individuals arising from your processing and the measures you can take to reduce the risks to acceptable levels, we have enclosed a template DPIA with suggested examples in the attached separate document.

## 4. Privacy Notice - Example for Facewatch Service Users

As a Data Controller your business will already be providing individuals with information about the collection and use of their personal data in a Privacy Notice. This is a key transparency requirement under the DPA.

A Privacy Notice sets out, among other things:

- your purposes for processing their personal data;
- your retention periods for that personal data;
- who it will be shared with.

You must provide privacy information to individuals at the time you collect their personal data from them and a common way to do this is by signposting people to a copy of the privacy notice on your website.

Your privacy notice should refer to your sharing of CCTV images and information with Facewatch (our Privacy notice can be viewed here).

Guidance from the ICO on what information needs to be in a privacy notice can be found here.

To assist you to update your existing privacy notice regarding your use of Facewatch Watchlists and Facial Recognition Alerts, we attach an example of wording in Appendix 1 which could be added to your Privacy Notice suitably edited for your organisation.

## 5. Signage

You **must** display signage saying facial recognition is in use so that customers can see them when entering your property otherwise you could be open to challenge.

---

kept up to date; (5) kept for no longer than is necessary; (6) handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Standard signage is supplied by Facewatch but can be amended to suit your requirements (eg to include your branding). These signs can replace or supplement your existing CCTV signage.

## 6. Do we need a Data Protection Officer if we use Facewatch?

Some companies have asked this question and the answer is that you are not required by law to appoint a DPO just because you are using Facewatch.

The relevant excerpt from GDPR, on which European domestic data protection law is based, is Article 37(1) b and c which relate to the mandatory appointment of a DPO –

> 37(1)(b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
>
> 37(1)c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data personal data relating to criminal convictions and offences.

These do not apply because –

a. Core Activities – the use of Facewatch is not the core activity of your business - it is ancilliary to your operation.

The EU Commission Article 29 Working Party, which is the official body to help define and understand GDPR, state in their paper "Guidelines on Data Protection Officers" at 2.1.2

1. Article 37(1)(b) and (c) of the GDPR refers to the 'core activities of the controller or processor'. Recital 97 specifies that the core activities of a controller relate to 'primary activities and do not relate to the processing of personal data as ancillary activities'.

b. Large Scale – The term is not specifically defined in GDPR but Recital 91 of GDPR gives the following example –

According to the recital, 'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk'

The processing of offence data through Facewatch by your organisation is likely to be a very long way from this example.

These are relevant clauses as the UK Data Protection Act does not extend the GDPR requirements to have a DPO.

Caveat: This does not mean that your organisation does not need a DPO per se, it simply means that using Facewatch does not create a requirement to have a DPO in itself. You should take your own advice if you are unsure whether your organisation should have a DPO due to other processing you carry out.

## APPENDIX 1: Example wording of a Privacy Notice for client processing related to Facial Recognition

Areas for completion are highlighted in yellow

[Company name and address]

[Contact details for Data Protection enquiries]

We supply facial images, descriptions, personal details and incidents details to Facewatch Ltd (Facewatch) of individuals reasonably suspected of having committed unlawful acts (Subjects of Interest). We also supply CCTV images to Facewatch who, in real time, compare the faces of people in those images to their watchlist of Subjects of Interest and alert us if there are matches. Faces not matched to a watchlist are deleted by Facewatch immediately to protect individual privacy.

We receive Facial Recognition Alerts instantly when a Subject of Interest enters our properties which are always checked for accuracy by a human before acted upon.

The recipients or categories of recipients of the personal data include our staff and may include third parties who assist us with the prevention and detection of unlawful acts, including Facewatch and police.

- The purposes of the processing is the prevention and detection of unlawful acts against our customers, staff and business assets.

- The lawful basis for the processing of personal data is – Legitimate Interests:

  The legitimate interests for the processing are – There is a compelling justification for us to protect our customers, staff and business assets from unlawful acts. Our Legitimate Interest Assessment is as follows:

  *It is our legitimate interest to be able to minimise the impact of unlawful acts by processing personal data to identify persons in our business properties who are reasonably suspected of having committed crime and taking reasonable and proportionate action. It is our legitimate interest to prevent crimes against us rather than just capture on CCTV crime that has taken place and report to police.*

  *The processing of personal data, special category data and criminal offence data is necessary to achieve our legitimate purpose as it allows us to quickly and accurately identify individuals who are reasonably suspected of having committed crime, and to take reasonable and proportionate action in the circumstances. Without processing information in this way we would be unlikely to effectively identify such persons as they enter our properties, be less likely to prevent unlawful acts, and therefore more likely to experience crime, even with existing tactics including security staff and/or CCTV monitoring. Reporting crime to police is similarly less effective than the use of Facewatch as this is post event rather than preventative.*

  *We balance our legitimate interest against the individual's interests, rights and freedoms. We distinguish those individuals reasonably suspected of having committed unlawful acts from all other persons entering our properties by the use of Watchlists and Facial Recognition Alerts. There is always human involved to verify any possible match between an individual entering our properties and an image on a Watchlist or Facial Recognition Alert. In the event of a confirmed match we may take reasonable and proportionate action in the circumstances.*

We take particular care when the data subject is, or appears to be, under 18 years of age and do not share this data with Facewatch.

- The lawful basis for the processing of criminal offence data is that it is necessary for the prevention and detection of unlawful acts.

- Facial Recognition/Special Category data:

Facial recognition algorithms are defined as Special Category data. Any such processing is conducted by Facewatch as data controller who are able to comply with the additional legal requirements for this processing as explained on their website www.facewatch.co.uk.

- Retention Period

We retain facial images, descriptions, personal details and incidents details including CCTV footage of individuals reasonably suspected of having committed unlawful acts (Subjects of Interest) for a period of [e.g. 2 years from date of incident]

- Your rights as a data subject

The right to be informed

The right of access

The right to rectification

The right to restrict processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling

The right to complain to the Information Commissioner's Office (ICO)

For a fuller explanation of these rights please see the website of the Information Commissioner's Office www.ico.org.uk