Privacy Notice

Company Name: **SGN LTD**

        TG Convenience Stores Ltd

        Global Fuels (UK) Ltd

Contact details for Data Protection enquiries:

    Email address: **customerservices@sgnretail.uk**

We use Facewatch facial recognition for the prevention of crime and protection of our staff and customers.

We supply facial images and incident details to Facewatch Ltd (Facewatch) of individuals reasonably suspected of having committed unlawful acts (Subjects of Interest). We also supply CCTV images of people entering our store(s) to Facewatch who, in real time, convert the images to biometric templates and compare them to their watchlist of Subjects of Interest and alert us if there are matches against SOIs relevant to our store (using proportionality rules). Biometric templates relating to faces not matched to the watchlist are deleted by Facewatch immediately to protect individual privacy and CCTV images are retained for up to 5 days in order to enable stores to report incidents post event.

We receive Facial Recognition Alerts instantly when a Subject of Interest enters our properties and these are always checked for accuracy by a staff member before acted upon them. If the staff member considers there is not a match between the alert they receive and the relevant person, they indicate this to Facewatch who instantly delete the alert data. If the staff member considers there to be a match with a subject of interest they indicate this to Facewatch who retain the alert data briefly in accordance with their policy.

We may access Facewatch CCTV images for up to 5 days in order to report unlawful acts carried out by an individual which we normally only identify after they have left the store.

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, security guards and police as part of a formal post event crime report.

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

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

  The legitimate interest for the processing 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.

  Our business is experiencing an ongoing crime problem. The business, staff and customers are experiencing significant harm as a result. We have tried reasonable measures other than Facewatch to prevent these crimes, including police reporting, human guarding (employees) and CCTV. These methods have failed to prevent the crime problem. We have considered the effectiveness of these and other methods to prevent crime. We consider it necessary to use Facewatch to prevent crime in our premises as we cannot reasonably otherwise protect our business, staff and customers from the harm caused by crime.

August 2022

The processing of personal 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 traditional tools available 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 a 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 do not retain alert data supplied to us by Facewatch. 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 31 days.

  - 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

August 2022