This register entry describes, in very general terms, the personal data being processed by: Institute of Hotel Security Management ICO register https://ico.org.uk/ESDWebPages/Entry/ZA236907

Nature of work - Business Crime Reduction Partnerships, shopwatches and pubwatches

Description of processing

The following is a broad description of the way this organisation/data controller & data processes deal with personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices provided or contact us to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to provide a valuable source of information and practical steps to identify offenders and anti-social elements working with other members, police and local statutory agencies and organisations to enable us to manage their behaviour more effectively. We collect visual images taken from a variety of CCTV systems which may be used for the purpose of security, the prevention and detection of crime and prosecution of offenders. We also process personal information to enable us to administer membership records.

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- financial and membership details
- goods and services
- visual images, personal appearance and behaviour

We also process sensitive classes of information that may include:

- offences including alleged offences
- criminal proceedings, outcomes and sentences
- physical or mental health details
- racial or ethnic origin.
- suspicious activity or behaviour

Who the information is processed about

We process personal information about:

- members
- victims of crime
- people in the area which is under surveillance
- offenders and suspected offenders
- associates of offenders or suspected offenders
- consultants and professional experts
- complainants and enquirers

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- members
- police forces
- security organisations
- central and local government
- other business crime reduction partnerships, shopwatches, pubwatches and similar schemes including regional and national schemes
- business associates
- consultants and professional advisers
- suppliers, providers of goods and services
- people making an enquiry or complaint
- healthcare professionals, social and welfare organisations
- voluntary and charitable organisations
- current, past or prospective employers

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the data protection act.

IHSM process the following information as a requirement to being a member.

Your name
Your email address
Your employer/hotel name
Your company address
Your home address
Your contact telephone number .

You may also provide your whatsapp, twitter, facebook or other social media contacts, and your photograph and your date of birth.
The are personally identifiable.

We will process the following information for the beneifts of crime reducation, prevention and solutions. These may lead to being able to positively identify a person.

A persons image.
A persons description.
A persons name.
A persons crime number.
A persons place of employment.

Under the GDPR; the following rights are detailed.

Application for membership of the IHSM is paper based and no facilities for direct user registration on this website exist.
Applying to be a member of the IHSM indicates consent to registration on this website and processing of your data.
Applying to be a member of the IHSM indicates consent to be placed on the Alerter Email system.
We transfer data to other members, which may include police forces, and via the internet cloud service to and from servers hosted in the UK and USA.

Rights of access:
A member who is registered on our system has the right to be provided with the personal data and information on processing, recipients, data transfers, and subsequent rights (such as the right to complain to a supervisory authority, or the right to request rectification, erasure, or a restriction on future processing).

Persons not members but submitted through members under the "Alerter" system via the website.
People who are confirmed to be listed on the website, and have provided sufficient proof they are listed, and on submission of full

identification, may request copies of their data and their requests under their rights under Article 15 must be clearly detailed.
We will not respond to speculative enquiries as to what data we hold about a non member.

Right to Rectification
If any change of circumstances occour, it is the members responsibility to ensure they update their details via the profile/members page.
Persons not members but submitted through members under the "Alerter" system via the website.
People who are confirmed to be listed on the website, and have provided sufficient proof they are listed, and on submission of full identification, may request copies of their data and their requests under their rights under Article 16 must be clearly detailed. We will not respond to speculative enquiries as to what data we hold about a non member.

Right to Erasure (Right to be Forgotten)

Subject to certain conditions, a data subject has the right to request the erasure of his or her personal data held by a data controller, this usually occours at the end of the membership.
In the case of RTBF/RTE being enacted, the alerts provided by the user may still be in place, the user persoanl data will be assigned a non personal numeric ID.

Non members:
We have the ability under the GDPR to decline an erasure request if it falls within one of the several exclusions in Article 17(3). We will not respond to speculative enquiries as to what data we hold about a non member.

Right to Restriction of Processing
A member can request to have alerts suspended or terminated. Personal Data provided by the member via the profile page may be removed via the member.
Persons not members but submitted through members under the "Alerter" system via the website.
People who are confirmed to be listed on the website, and have provided sufficient proof they are listed, and on submission of full identification, may request copies of their data and their requests under their rights under Article 15 must be clearly detailed. We will not respond to speculative enquiries as to what data we hold about a non member.

Notification Obligation for Controllers
We will notify each member of any impacting data rectification, erasure, or restriction. If the data subject requests details on recipients, the data controller is required to supply it.

Right to Object
A data subject has the right to object to the processing of his or her personal data at any time where the legal basis is "the performance of a task carried out in the public interest," "the exercise of official authority vested in the controller," or for the purposes of the "legitimate interests" of the controller or a third party (Article 6(e) and (f)).
The data subject can also object to processing for the purposes of direct marketing and profiling for direct marketing activities.

Automated individual decision-making, including profiling.
We do not participate in this activity.

Processor Requirements
We do not currently engage any 3rd party data processors.

Records of Processing Activities
We keep records of applications,
Members logins time and dates (including log out)
Data adjustment requests,
IP addresses used to send alerts and contact forms.
Data provided by members themsleves under their profile is not under the control of the DC/DP

Security of Processing Data
Our servers are protected by SSL encryption. Our website is members login protected, IP tracked and may user 2FA logins for administrative works. Registration can not occour without going through the site adminstrator, data controller, or data processors first.

Transfers of Personal Data to Third Countries or International Organizations.
Our servers are based in the EU and USA. Our USA servers are considered to conform to EU-US Privacy Shield.

Data loss prevention.
All data is held on the website. All alerts are notified to members via a link to the website when a new alert is generated. The members must log into see the alert details.
If any server downtime ocours then data may be sent via the google email system which is based in the USA and has suitable data security and is sent to explicit consented members only.

Consent
We recognise the consent requirements. Becoming a member post GDPR (25th May 2018) will require you to consent to receiving information and your details as the membership requires. You can withdraw consent but that may affect your membership.
PRE GDPR date, you may in future be asked to reconfirm your cosent, however consent is not retrospective.