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

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

Non Members,
We collect anonymous information such as your IP and in site tracking via google analytics. We may collect your name, email address and other information you give us via our contact form.

Members

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 rely on a wide variety of information to run our association. In some instances, this information may include data that could be used to identify a particular individual, otherwise referred to as Personal Information. In this Notice, we will provide multiple examples of how Personal Information we collect may be used and why it is important. For example, when a member joins we must collect their name, email address, location and payment information to complete the membership. Some of the reasons that we collect Personal Information include to:

Allow you to be a member, receive news and services;
Investigate, respond to, and manage inquiries or events;
Work with and respond to law enforcement and regulators; and
Research matters relating such as security threats.

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.

Type/classes of information processed

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

- personal details (such as name, email address, mailing address, and phone number,);
- financial and membership details
- 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

Membership Uses.

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 contact telephone number.

In addition, we may use Personal Information for other purposes, including to:

- Analyse users' behaviour when using our website to customize preferences;
- Establish and manage user accounts;
- Collect and process payments and complete transactions;
- Manage subscriptions, and respond to requests, questions, and comments;
- Communicate about, and administer participation in, meetings, special events;
- Enable posting and other communications;
- Customize, measure, and improve our websites, products, services, and advertising;
- Perform accounting, auditing, billing, reconciliation, and collection activities;
- Prevent, detect, identify, investigate, respond, and protect against potential or actual claims,
- liabilities, prohibited behavior, and criminal activity;

- Comply with and enforce applicable legal requirements, agreements, and policies;
- and Perform other activities consistent with this Notice.

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.

If you decide to limit how much information to share with us, but not sharing required information may limit your ability to engage in certain activities.

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
- Current and future members of the IHSM for the purposes described in this Notice, such as to:
  (i) provide services and content;
  (ii) help detect and prevent illegal acts and violations; and
  (iii) guide our decisions about our institute, services, and communications;
- Other members where you have chosen to share such information, or where you have posted alerts;
- Authorized service providers who perform services for us (including cloud services, data storage, google email).

Our contracts with our service providers include commitments that they agree to limit their use of Personal Information and to comply with privacy and security standards at least as stringent as the terms of this Privacy Notice. Remember that if you provide Personal Information directly to a third party, such as through a link on the Institute website, the processing is typically based on their standards (which may not be the same as ours);
If we believe disclosure is necessary and appropriate to prevent physical, financial, or other harm, injury, or loss, including to protect against fraud or credit risk.
To legal, governmental, or judicial authorities, as instructed or required by those authorities or applicable laws, or in relation to a legal activity, such as in response to a court order or investigating suspected illicit activity (including identifying those who use member services for illegal activities). We reserve the right to report to law enforcement agencies activities that we in good faith believe to be illegal.
With others only after obtaining your consent. If we want to share Personal Information other than as permitted or described above, we will provide you with a choice to opt in to such sharing and you may choose to instruct us not to share the information.

We will process the following information for the benefits of crime reduction, 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.
Security and Threat Detection.
By collecting and processing data, including Personal Information, we may use your information to
Participate in threat intelligence networks and conduct research and analysis,
Respond to new threats.

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).

Right to Rectification
If any change of circumstances occur, 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 15 & 16 must be clearly detailed. We will not respond to speculative enquiries as to what data we hold about a non member from 3rd parties.

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 occurs 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 personal data will be assigned a non personal alpha 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 from 3rd parties.

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 and 16 must be clearly detailed.
We will not respond to speculative enquiries as to what data we hold about a non member from 3rd parties.

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 currently engage google for email, analytics as our 3rd party data processors and cloudaccess as our host. Our assigned data processor is SecureHotel

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 themselves 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 use 2FA logins for administrative works. Registration can not occur without going through the site administrator, data controller, or data processors first.

Transfers of Personal Data to Third Countries or International Organizations.
Our servers are based in the EU and may default backup to the USA. Our USA servers are considered to conform to EU-US Privacy Shield. We have agreements that any data transferred outside the EU is used via a system registered with PrivacyShield. If you are located in the European Economic Area or Switzerland, we provide adequate protection for the transfer of Personal Information to countries outside of the EEA or Switzerland through a series of agreements based on the Standard Contractual Clauses authorized under the EU Data Protection Directive 95/46/EC.

Data loss prevention.
All data is held on the website. All alerts are notified to members via a link to the website . The members must log into see the alert details.
If any server downtime occurs 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 consent, however consent is not retrospective.

Data Retention

The time periods for which we retain your Personal Information depend on the purposes for which we use it. We will keep your Personal Information for as long as you are a registered member or for as long

as we have another legal and legitimate purpose to do so and, thereafter, for no longer than is required or permitted by law, or our Records Retention Policy, reasonably necessary for internal reporting and reconciliation purposes, or to provide you with feedback or information you might request.

Children’s Privacy
We have no members under the age of 13.

0418