Cheltenham Safe business crime reduction partnership

PERSONAL DATA PROCESSING DOCUMENTATION

This document describes the way that personal data is processed and secured by Cheltenham Safe business crime reduction partnership (the Scheme).

Contact details

Cheltenham Safe
2 Trafalgar Street
Cheltenham
GL50 1UH
Email address: info@cheltenham-safe.org
Telephone: 01242 252323
www.cheltenham-safe.org

The Scheme's Data Controller is responsible for ensuring its compliance with current Data Protection law and can be contacted at the above address, email address or telephone number. The Scheme is registered with the Information Commissioners Office as a Business Crime Reduction Partnership.

Types of Data Subjects processed

The Scheme processes the personal data of two types of Data Subjects:

- **'Offenders'**: individuals aged 14 years and over who have been reported to have been actively involved in incidents which have presented a threat or damage to the property or safety of Members or Members' staff or customers.
- **'Members'**: owners or lessees of commercial property, including their staff or agents, who offer an implicit licence to the public to enter their property.

Purpose of processing personal data

Offenders

- Members of the Scheme have the right to protect their property, staff and customers from crime and anti-social behaviour and to exclude from their premises any individuals who are proven threats to their property, staff or customers. The Scheme processes Offenders' personal data for the specific purpose of managing its Exclusion Scheme on behalf of its Members.
- The Scheme's area of operation, and its Exclusion Scheme, extends across the Boroughs of Cheltenham and Tewkesbury.

Members

- The Scheme processes Members' personal data for the following purposes:

- to enable the efficient management of the Scheme; to manage the membership of the Scheme including subscriptions where relevant; invitations to the Scheme's Annual General Meeting and other meetings where relevant etc;
- to defend and indemnify the Scheme in case of any Member's non-compliance with the Scheme's Rules & Protocols;
- to enable the Scheme to communicate efficiently to Members by sending only relevant news, alerts and documents, and information about events which are relevant, to them.

Lawful Basis of Processing

Offenders

- The Scheme's Members' 'legitimate interests' provides the lawful basis on which it may process specific items of Offenders' personal data for specific purposes without Offenders' consent.
- The Scheme has assessed the impact of its processing on Offenders' rights and freedoms, has balanced these with its Members' own rights, and has concluded that its Members' rights prevail over Offenders' rights in this specific matter. This means that, for the specific purpose of managing an exclusion scheme, the Scheme's lawful basis for processing Offenders' personal data is 'legitimate interests' and therefore the Scheme can process Offenders' personal data without requiring their consent.

Members

- The Scheme's existing contract/agreement between itself and its Members requires that Members provide their name, postal and email addresses, telephone etc to the Scheme. This contract/agreement means that the Scheme's lawful basis for processing Members' personal data is 'contract' and therefore the Scheme can process Members' personal data without their further consent.

Categories and types of personal data processed

Offenders:

- **Offender's name and facial image and any relevant information about the nature of his/her activities**; the purpose of this processing is to enable Members to identify Offenders in order to submit reports about them, to include them in a list or gallery of excluded persons (if appropriate and in line with the Scheme's Rules & Protocols), and to provide information about them which may be necessary to protect the personal safety of Members and their staff, customers etc. This data may be shared among Members;
- **Offenders' postal and email addresses, telephone number(s) and other contact details**; the purpose of this processing is to enable the Scheme to communicate with Offenders from time to time, for example to send

confirmation of exclusions, rules of the exclusion scheme, or confirmation that exclusions have expired. Such data will not be shared with Members;

- **Information and evidence about incidents in which an Offender has been involved**; the purpose of this processing is to enable the Scheme to defend its legal rights against any claim or suit by an Offender or other party. Such data will not be shared with Members but only with the Scheme's Data Controller and Board of Management as necessary in the course of any legal proceedings.
- No sensitive or 'special category' personal data (ethnicity, sexuality, religious beliefs etc) is processed by the Scheme.

Members

- Name, name and place of employment, postal and email addresses, telephone and other contact details will be processed;
- No sensitive or 'special category' personal data (ethnicity, sexuality, religious beliefs etc) is processed by the Scheme.

Sources of personal data

Offenders

- **Offenders** who may voluntarily offer information about themselves;
- **Members** who may submit reports about incidents in which Offenders have been involved. They may also send relevant 'intelligence' about Offenders, for example they may provide a name when asked to identify an unidentified CCTV image;
- **Police or other public agencies** may provide Offenders' personal data under a formal Information Sharing Agreement.

Members

- Existing contracts/agreements with Members;
- Members may themselves update their personal data on the Scheme's online system (My Account).

Recipients or categories of recipients of Members' personal data

Offenders

- **Members** who are property owners, agents or their employees working within the operational area of the Scheme who share the same legitimate interests;
- **Employees and officers of public agencies involved in the prevention and detection of crime**, such as police, whose lawful basis for processing Offenders' data is their public task;
- **Data Controllers of other organisations**, like the Scheme, in neighbouring areas if there is evidence that an Offender has participated, or is likely to participate, in any threat or damage to property, staff and customers in areas outside the Scheme's area of operation.

- The Scheme will not transfer Offenders' data outside the UK.

Members

- The Scheme's Board of Management, Data Controller and formally contracted Data Processors may access Members' personal data;
- Members' personal data will not be passed to any third party unless to the police under warrant or with the expressed permission of the Member;
- The Scheme will not transfer Members' personal data outside the UK.

Data retention period

Offenders

- When an Offender is reported by a Member for participating in any threat or damage to any Member's property, staff or customers, his/her name and facial image may be shared among Members for 12 months. If no further report is submitted during that period, the Offender's data will be withdrawn from Members at the expiry of that period. It will be retained for a further 12 months in the Scheme's database (which can only be accessed by the Data Controller) after which time it will be irrevocably deleted.
- If during the 12 months when an Offender's data is circulated among Members he/she is reported for another incident involving a threat or damage to any Member's property, staff or customers, his/her name and facial image may be circulated among Members for a further 24 months from the date of the second report. Where an Offender has been made subject of a scheme wide exclusion, that offender will be excluded from the properties of all Members premises for a fixed period which shall be made known to the person subject of that exclusion. This will be shared with Members. If no further report is submitted by a Member during that exclusion period, the Offender's data will be withdrawn from Members at the expiry of that period of exclusion. It will be retained for a further 12 months in the Scheme's database (which can only be accessed by the Data Controller) after which it will be irrevocably deleted.

Members

- The Scheme will retain Members' personal data only for as long as each Member remains a Member of the Scheme; when a Member ceases to be a Member of the Scheme he/she must confirm this with the Scheme's Board of Management as specified in the Scheme's Rules & Protocols at which time all associated personal data will be irrevocably deleted.
- In the case of submitted reports, the submitting Member's email address only will continue to be associated with such reports for as long as the report is retained by the Scheme; this is required where a report is used for evidential purposes in legal proceedings.

Data Processors

The Scheme employs the services of the following Data Processor(s):

- **Littoralis Limited**; access the Littoralis Standard Terms & Conditions including our Data Processor Contract with the company here

Standard Operating Procedures

The following Standard Operating Procedures have been defined relating to the processing of personal data by the Scheme and in compliance with current Data Protection law:

Documentation management

- Every six months the Data Controller will review all documentation relating to the management of personal data, including the Scheme's *Privacy Notices* (Offenders and Members), *Personal Data Processing Documentation*, *Legitimate Interests Statement, Data Protection Impact Assessment(s)* and *Balance of Interests Statement(s)* and, where relevant, Information Sharing Agreement(s) and Data Processing Agreement(s).
- Where any revision is necessary, a new version of the relevant document will be created to replace the previous version (which will be retained by the Data Controller);
- Where it is necessary that Members re-certify against any revised document, the Data Controller will secure re-certification by all Members when they next access the Scheme's data.

Subject Access Requests

- Within 30 days of an applicant submitting a Subject Access Request to the Data Controller or Board of Management, the Data Controller must confirm its receipt with the applicant;
- As soon as practical thereafter the Data Controller must satisfy itself as to the identity of the applicant; where necessary this may require identification in person by personal facial recognition;
- As soon as practical thereafter the Data Controller must:
    - collect all personal data relating to the applicant, including image(s);
    - redact all data identifying any other person from the data;
    - provide the relevant personal data to the applicant, in a conventional, readable format;
    - provide all documentation demonstrating the Scheme's compliance with Data Protection law;
    - inform the applicant of his/her right to require corrections of any data which the applicant can demonstrate to the satisfaction of the Data Controller is incorrect, unnecessary or disproportionate.
- Document the completion of the SAR process

Reporting a Personal Data Breach

- Within 72 hours of becoming aware of a breach of personal data the Data Controller must report the breach to
    - the Board of Management;
    - the Information Commissioner's Office;
    - any relevant Data Processor;
- As soon as possible thereafter, in the case of a data breach which, in the view of the Board of Management, is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Data Controller must inform those individuals of the breach and the nature of the resulting risk to their rights and freedoms.
- The Data Controller must document each Personal Data Breach in **Appendix A** of this document

Privacy Notices distribution

Offenders

- **Where data is collected directly from the Offender:** Privacy Notice (Offender) must be served to the Offender at the time and place of data collection;
- Use best endeavours to record service of Privacy Notice and retain record of service;
- **Where data is not collected directly from the Offender:** as soon as possible thereafter use best endeavours to serve Privacy Notice and record service of Privacy Notice and retain record of service;
- In any case to display Privacy Notice (Offenders) to maximise likelihood and possibility of access by Offender

Members

- Privacy Notice (Member) must be served to the Member at the time and place of data collection.

Registration of the Scheme with the Information Commissioners Office

- Each year, at the notification to the Data Controller of the annual renewal of the Scheme's registration with the ICO, the Data Controller must review the Scheme's registration with the ICO;
- As soon as possible thereafter, where the registration requires updating or revision, the Data Controller must communicate the proposed revision to the ICO's Registration department at registration@ico.org.uk

Description of security methods (Technical and Organisational)

The Scheme processes all personal data within the DISC online 'secure environment' in which all personal data processed by the Scheme is secured. The DISC system aligns with the principles of 'Data Protection by Design and Default' as defined in the latest version of the *DISC Information Security Management and Policy* which can be accessed **here**

Appendix A

PERSONAL DATA BREACHES

Copy-and-paste the following form to create a new form for each reported Breach; be sure to document all communications with your Data Processor, ICO and, where necessary, any relevant Data Subjects.

			Notes
1	Date and time of detection of Breach		
2	Date and time of Breach		*If known; if not known, best estimate*
3	Cause of Breach		*Eg: Malicious attack (internal or external?); accidental (technical security failure); negligence/human error (operation security failure); other (specify)*
4	Likely impact(s) of Breach		*Eg: data publication; data theft; identity theft or fraud; loss of data; loss of confidentiality of personal data; property damage; direct financial loss; business interruption; liability issues; reputational damage; other(specify)*
5	Type of data breached		*Ie: Personal; Non-Personal*
6	If Personal Data, what impact may the Breach have on the rights and/or freedoms of relevant Data Subjects?		*If Personal Data has been breached, document all possible significant negative impacts on the legitimate interests of Data Subjects; consider any possible distress to Data Subjects. If no significant negative impacts can be identified it is not necessary to notify Data Subjects (see 9 below)*
7	Date of notification to relevant Data Processor		*Notify the relevant Data Processor as soon as you are aware of the Breach*
8	Date of notification to Information Commissioners Office		*Notify the ICO within 72 hours of the detection of the Breach (see 1 above)*
9	Date of notification to Data Subjects if necessary		*See 6 above*
10	Data format		*Digital (encrypted/unencrypted?); paper-based; on removable media (USB stick, CD, laptop?)*
11	What measures have been taken to mitigate adverse effects of the Breach?		*Describe what actions you have taken to minimise any negative impacts of the Breach (see 6 above)*
12	What measures have been taken to minimise the re-occurrence of a similar Breach?		