



This document contains the information required by Data Protection law relating to your current personal data processing activities. This document may be requested by the ICO. It is not necessary to provide this document in response to a Subject Access Request by either an Offender or a Member.

Privacy Notice for Offenders

This document describes the way that personal data is processed and secured by Southampton Business Crime Partnership.

Contact details

Southampton Business Crime Partnership.

IncuHive Southampton,
182 High Street
Southampton
SO14 2BY
Landline: 02380003637
Email: sbcp@gosouthampton.co.uk

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.

The Scheme processes the personal data 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.

1. Lawful Basis of Processing Offenders data

- 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, and 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.

2. What are the reasons for processing and the types of data we process?

- We process personal data and sensitive personal data for the prevention and detection of crime and anti-social behavior. We also use this data to identify natural persons for further action such as target hardening, exclusion notices to prevent and reduce crime and enhance local prosperity based on the national intelligence model.
- We collect information relating to the above reasons/purpose from the following sources:

UK law enforcement bodies, our business members, open-source material via social media and any other relevant bodies or businesses linked to ongoing criminal investigations.

3. Types of data we process for the above reason / purpose may include.

- Name and address details
- Date of birth, age, and descriptive details
- Email address
- Phone number
- Details of associates
- Vehicle registration details
- 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 during any legal proceedings.
- No sensitive or 'special category' personal data (sexuality, religious beliefs etc) is processed by the Scheme. Ethnicity is special category data; it is required because it forms an integral part of the identification process to inform our members of individuals who are excluded or in danger of being excluded.
- 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.

4. Recipients or categories of recipients of Offenders personal data

- **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.

5. Data retention period for Offender's data

- 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 will be circulated among members for a further 24 months from the date of the second report. Additionally, the offender will be excluded from all the properties of all members for 24 months, and this fact will be shared with members. If no further report is submitted by a member 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 it will be irrevocably deleted.

6. 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

7. Standard Operating Procedures

It is not obligatory to include any specific SOPs; however, it is obligatory to include descriptions of all processes that relate to the management of personal data - so we recommend that these inclusions.

8. 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);

9. Privacy Notices distribution Offenders

- Where data is collected directly from the offender: This Privacy Notice (Offender) must be served to the offender at the time and place of data collection if practicable. If this is not practicable the offender should be directed on how he can access this information <https://www.disc-net.org/gosouthampton>
- Use best endeavours to record the service of the 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.
- You have the right to obtain a copy of all the personal data which we process. To do so, contact us (details above).
- If you believe that any of the data, we process about you is incorrect, unnecessary, or disproportionate, you can require us to correct it. You do not have the right to require us to delete correct, necessary, or proportionate information.
- You also have the right to complain about us to the Information Commissioners Office at <https://ico.org.uk/concerns/handling/>