Southampton Business Crime Partnership

Privacy notice for members

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.

Personal data processing protocol for members.

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.

1. **Types of data subjects processed**

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

a. **'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.

b. **"Members'**: owners or lessees of commercial property, including their staff or agents, who offer an implicit licence to the public to enter their property.

2. **Purpose of processing personal data of members**

a. The Scheme processes members' personal data for the following purposes:
b. To enable the efficient management of the Scheme and membership of the Scheme.

c. To defend and indemnify the Scheme in case of any member's non-compliance with the Scheme's rules & protocols.

d. 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.

3. Lawful Basis of Processing members data

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.

4. Categories and types of personal data processed members

a. Their name, place of employment, postal and email addresses, telephone, and other contact details will be processed.

b. No sensitive or 'special category' personal data (ethnicity, sexuality, religious beliefs etc) is processed by the Scheme.

5. Sources of personal data members

a. Existing contracts/agreements with members.

b. Members may themselves update their personal data by emailing sbcp@gosouthampton.co.uk

6. Recipients or categories of recipients of members' personal data

a. Members who are property owners, agents or their employees working within the operational area of the scheme who share the same legitimate interests.
b. 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.
c. 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. GO! Southampton Management, SBCP data controller and staff.

d. 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.
e. The Scheme will not transfer Members' personal data outside the UK.

7. **Data retention period for members data**

a. 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 data controller as specified in the scheme's rules & protocols at which time all associated personal data will be irrevocably deleted.

b. 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.

8. **Data Processors**

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

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

c. 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:

8. **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)

9. **Standard Operating Procedures**

It is not obligatory to include any specific, standard operating procedures, however, it is obligatory to include descriptions of all processes that relate to the Management of personal data - so we recommend these inclusions.

10. **Processing Agreement(s).**

a. Members when they next access the Scheme's data, 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);

b. Where it is necessary that Members re-certify against any revised document, the data controller will secure re-certification by all.

11. **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:

a. SBCP Management.
b. The Information Commissioner's Office.
c. Any relevant Data Processor;

As soon as possible thereafter, in the case of a data breach, which in the view 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

12. Privacy Notices distribution member

Privacy Notice - This document will be available for members to access on the front screen of SBCP Disc system on first login or at any time.

13. Registration of the Scheme with the Information Commissioners Office

a. 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;

b. 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

14. 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

15. 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.

1	Date and time of detection of Breach		***Notes***
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?		