Brighton & Hove Business Crime Reduction Partnership [the Scheme]

PERSONAL DATA PROCESSING DOCUMENTATION [Offenders]

1. This document describes the way that personal data is processed and secured by the Scheme.

2. **Contact details**
Brighton & Hove BCRP Ltd
PO Box 5398
Brighton BN50 8GQ
Email address: noreply@bcrpbrighton.com
Tel: 01273 733393

3. 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

4. The Scheme processes the personal data of:
'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 or disrupt the peaceful enjoyment that their customers expect from the goods and/or services that our Members offer. Minors between the ages of 14 and 17 are subject to an additional policy on processing their data.

Purpose of processing personal data

Offenders

5. Members of the Scheme have the right [a legitimate interest] 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 or disrupt the peaceful enjoyment that their customers expect from the goods and/or services that our Members offer. The Scheme processes Offenders' personal data for the specific purpose of managing its Exclusion Scheme on behalf of its Members, to inform Members of an offender's modus operandi, to collate intelligence on criminal activity within the area of the Scheme's operation and to contribute to legal proceedings against Offenders where appropriate.

6. The Scheme's area of operation, and its Exclusion Scheme, is within the boundaries of the city of Brighton & Hove.

Lawful Basis of Processing

For Offenders

7. 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.

8. 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 and operating the business crime reduction partnership including its Exclusion Notices, 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.

Categories and types of personal data processed

9. **Offender's name and facial image [a picture made using a camera] and any relevant information about the nature of his/her anti-social activities in connection with our Members' interests**; 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;

10. **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.

11. **Information and evidence about incidents in which an Offender has been involved**; the purpose of this processing is to enable the Scheme to assess the suitability of an exclusion notice against the Offender and to defend its legal rights against any claim or suit by an Offender or other party. Details of such data will not be shared with Members but rather a one or two word description of the general offence for which the offender is known. Details of such data may be shared with the Scheme's Data Controller and Board of Management as necessary and also in the course of any legal proceedings.

Special Category Data

12. In order to lawfully process special category data, GDPR makes it clear that an organisation must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

13. The lawful basis for the processing of special category data is Article 6. 1(e) - processing is necessary for the performance of a task carried out in the public interest. The processing of special category data is also allowed under UK derogations for the purposes of the prevention of crime and disorder.

14. Such processing [necessary for reasons of substantial public interest, on the basis of Union or Member State law] will be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject [Article 9. 2(g)].

15. The following table outlines what special category data will be processed, with whom it will be shared and the reason for distribution:

Category	Processed?	May be shared with?	Justification
Race	Will not be processed	Will not be shared	
Ethnic origin	May be processed	Members. Other accredited BCRPs in Sussex. National Business Crime Solution.	For the purposes of assisting BCRP Members to identify excluded individuals
Politics	Will not be processed	Will not be shared	
Religion	Will not be processed	Will not be shared	
Trade Union Membership	Will not be processed	Will not be shared	
Genetic data	Will not be processed	Will not be shared	
Biometric data	Only a photograph taken with a camera and not subject to any specific technical processing may be processed[1]. No other biometric data will be processed.	Members. Other accredited BCRPs in Sussex. National Business Crime Solution.	For the purposes of assisting BCRP Members to identify excluded individuals
Health data	Will not be processed	Will not be shared	
Sex life	May be processed	Will not be shared	To protect an individual's vital interests when deemed at risk e.g. potential for Child Sexual Exploitation. There will be no additional processing other than implicit references from other data sources where necessary. This information will be redacted where possible from other reports.
Sexual orientation	May be processed	Will not be shared	To protect an individual's vital interests when deemed at risk e.g. potential for Child Sexual Exploitation. There will be no additional processing other than implicit references from other data sources where necessary. This information will be redacted where possible from other reports.

[1] A photograph was deemed to be biometric data in the Judicial Review M vs Chief Constable of Sussex Police

16. **Sources of personal data**

For Offenders

a. **Offenders** themselves who may voluntarily offer information about themselves;
b. **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;
c. **Other business crime reduction partnerships** or similar accredited private sector agencies with which we have a data sharing agreement
d. **Police or other public agencies** may provide Offenders' personal data under a formal Information Sharing Agreement
e. **Social media platforms** may provide information that is in the public realm by virtue of being displayed without privacy controls on a publicly accessible platform.

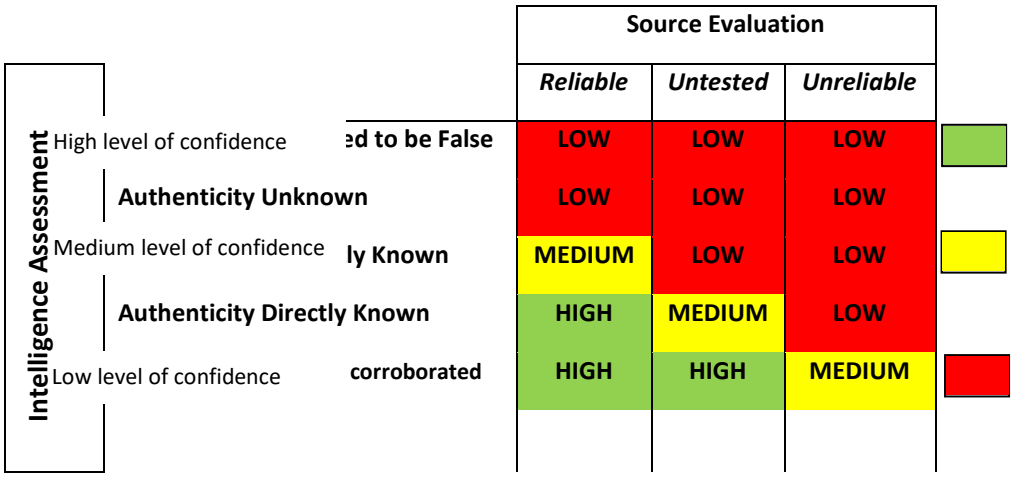
17. **Recipients of offender's personal data**

a. **Members** who are business and/or property owners, their 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. **Charitable organisations** also involved in the prevention of crime and public disorder
d. **Data Controllers of other organisations**, similar in nature to the Scheme, in neighbouring areas if there is evidence that an Offender has participated in any threat or damage to property, staff and customers in areas outside the Scheme's area of operation.

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

Data retention period

19. When an Offender is reported by a Member for participating in any threat or damage to any Member's property, staff or customers or disrupting the peaceful enjoyment that customers expect from the goods and/or services that our Members offer, the information received will be subjected to a confidence test shown below:-



22. If the data fails the confidence test it will be irrevocably destroyed immediately without any further processing. If it passes the confidence test and meets the points criterion for sharing or exclusion, the Offender's name, date of birth, facial image and the offence for which they are known may be shared among Members for a maximum of 12 months or the full term of any relevant court imposed sanction. 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 may be retained for a further maximum of 12 months in the Scheme's database [a maximum of 6 months for

Offenders under the age of 18]. During this latter period it will not be shared with members and can only be accessed by the Data Controller and authorised personnel. At the end of this latter period data must be irrevocably deleted unless further reports of criminal and/or anti-social behaviour involving a threat or damage to any Member's property, staff or customers are reported to the BCRP.

23. If, during the 12 months when an Offender is excluded, he/she commits further incidents involving a threat or damage to any Member's property, staff or customers, and reaches the appropriate threshold his/her exclusion may be renewed and their name and facial image may be circulated among Members for a further maximum of 12 months from the date of the further report. If no further report is submitted by a Member or public agency 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 maximum of 12 months [6 months for Offenders under the age of 18] in the Scheme's database (which can only be accessed by the Data Controller and authorised personnel) after which it will be irrevocably deleted.

24. Personal data may also be transmitted via the radio network operating in the city. All radio transmissions will be recorded on the BCRP's Safety Net radio management system and will be stored for a period of 28 days after which they will be erased. They will be shared with law enforcement agencies upon request to support the investigation of a crime and the original owner of any transmission may request a copy [.wav file] for their own internal processing purposes.

Data Processors

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

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

Standard Operating Procedures

27. 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

28. 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).

29. 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);

30. 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

31. 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;

32. 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 or the presentation of a photo identification document;

33. As soon as practical thereafter the Data Controller must:

a. collect all personal data relating to the applicant, including image(s);
b. redact all data identifying any other person from the data;
c. provide the relevant personal data to the applicant, in a conventional, readable format;
d. provide all documentation demonstrating the Scheme's compliance with Data Protection law;
e. 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.
f. Document the completion of the SAR process

Reporting a Personal Data Breach

34. Within 72 hours of becoming aware of a breach of personal data the Data Controller must report the breach to:-

a. the Board of Management;
b. the Information Commissioner's Office if deemed sufficiently serious;
c. any relevant Data Processor;

35. 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.

36. The Data Controller must document each Personal Data Breach in **Appendix A** of this document

Privacy Notices distribution

37. **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.

38. Use best endeavours to record the service of the Privacy Notice and retain record of service;

39. **Where data is not collected directly from the Offender:** as soon as possible thereafter use best endeavours to serve a Privacy Notice unless the provision of such information proves impossible [Article 14, para 5(b) of GDPR] and record service of Privacy Notice and retain record of service;

40. In any case to display Privacy Notice (Offenders) on the Scheme's website where it is publicly available to maximise likelihood and possibility of access by Offender

Registration of the Scheme with the Information Commissioners Office

41. 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;

42. 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)

43. 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.

Date and time of detection of Breach		***Notes***
Date and time of Breach		*If known; if not known, best estimate*
Cause of Breach		*Eg: Malicious attack (internal or external?); accidental (technical security failure); negligence/human error (operation security failure); other (specify)*
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)*
Type of data breached		*Ie: Personal; Non-Personal*
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).*
Date of notification to relevant Data Processor		*Notify the relevant Data Processor as soon as you are aware of the Breach*
Date of notification to Information Commissioners Office		*Notify the ICO within 72 hours of the detection of the Breach (see 1 above)*

Date of notification to Data Subjects if necessary		*See 6 above*
Data format		*Digital (encrypted/unencrypted?); paper-based; on removable media (USB stick, CD, laptop?)*
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)*
What measures have been taken to minimise the re-occurrence of a similar Breach?		