National Infrastructure Crime Reduction Partnership [the Scheme]

PERSONAL DATA PROCESSING DOCUMENTATION [NICRP]

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

2. **Contact details**
NICRP
c/o Safer Business Network CIC
Brighton Police Station
John Street
Brighton
BN2 0LA
Email address: info@nicrp.org

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 or email address. The Controller is registered with the Information Commissioners Office as a Business Crime Reduction Partnership.

4. 'Members' are defined interested parties who have opted to become Members of the Scheme and have paid any relevant fees. Upon application, there is no automatic right to become a Member and no reason will be given for refusal to grant membership.

Purpose of processing personal data

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

    a) to enable the efficient management of the Scheme; to manage the membership of the subscriptions where relevant; invitations to the Scheme's meetings and training opportunities where relevant etc;

    b. to defend and indemnify the Scheme in case of any Member's non-compliance with the Scheme's Protocols;

    c. to enable the Scheme to communicate efficiently with Members by sending news, alerts and documents, and information about events which are relevant, to them.

Lawful Basis of Processing

6. The existing contract/agreement between the Scheme 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 consent via contract and therefore, once consent is given, the Scheme can process Members' personal data without their further consent.

Categories and types of personal data processed

7. Name of contact, 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.

8. **Sources of personal data**
    a. Existing contracts/agreements with Members;
    b. Members may themselves update their personal data.

9. **Recipients of personal data**

    a. The Scheme's Data Controller, authorised personnel and formally contracted Data Processors may access Members' personal data;
    b. Members' personal data will not be passed to any third party unless to the police or other crime prevention agency under warrant or with the expressed permission of the Member;
    c. The Scheme will not transfer Members' personal data outside the UK.

Data retention period

10. 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 administrator at which time all associated personal data will be irrevocably deleted.

11. In the case of any reports or intelligence submitted to the Scheme, 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 may be used for evidential purposes in legal proceedings.

Data Processors

12. The Scheme does not employ the services of a Data Processor(s):

Standard Operating Procedures

13. 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

14. Every six months the Data Controller will review all documentation relating to the management of personal data, including the Scheme's *Privacy Notice* and, where relevant, Information Sharing Agreement(s).

15. 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);

16. 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

17. 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;

18. 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;

19. 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

20. Within 72 hours of becoming aware of a breach of personal data the Data Controller must report the breach to:-
    a. the DPO
    b. the Board;
    c. the Information Commissioner's Office if deemed sufficiently serious;
    d. any relevant Data Processor;

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

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

Privacy Notices distribution

For Offenders

23. Privacy Notice (Member) must be served to the Member at the time and place of data collection. It will also be displayed on the Scheme's website so that it is publicly available.

Registration of the Scheme with the Information Commissioners Office

24. 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;

25. 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)

26. The Scheme processes all personal data within the DISC and SentrySIS online 'secure environments' in which all personal data processed by the Scheme is secured. These systems align with the principles of 'Data Protection by Design and Default'.

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?	