



Data Protection Impact Assessment

This document identifies all possible impacts of the processing of Offenders' personal data by the York BID Safety Network on the rights and freedoms of those Offenders.

York BID Safety Network (YBSN) is the Business Crime Reduction Partnership (BCRP) for York.

Business Crime Reduction Partnerships bring together members of the business community and other agencies, such as the police, community safety partnerships and local authorities, to work together with the aim of reducing crime against business. YBSN covers York BID's geographical member area.

YBSN is a not for profit organisation and part of York BID, the Board of Membership. The Board is supported by steering groups who represent Member Business, North Yorkshire Police and other interests of the partnership.

York BID and York PubWatch are registered with the Information Commissioner for the Data Protection Act 2018, to store and share information and are covered by the necessary insurance.

All members of the Business Crime Reduction Partnership have a responsibility to ensure they are aware of and comply with the Data Protection Principles in the Data Protection Act 2018 incorporating the General Data Protection Regulations. You can find further information at www.informationcommissioner.gov.uk

All relevant intelligence will be recorded on the ShopSafe Alert! database. The database is managed by the BCRP Crime Coordinator who reports to the BCRP Crime Manager. They can be contacted at York BID Safety Network, The Red House, 1 Duncombe Place, York, YO1 7ED.

Intelligence / information will be gathered on persons who cause an incident or commit an offence, which affects any member of the BCRP. The information collated will be stored on a database and accessible to members of the BCRP, for the prevention and detection of crime, who have:

- Read, understood, agreed and signed the Alert! Terms of Use that governs access to and use of the ShopSafe Alert! System prior to enabling access to the system.
- Read and understood YBSN's Personal Data Processing Policy (Members) that describes the way that personal data is processed and secured.

For the purposes of the Data Protection Act 2018, the Data Controller for the BCRP is the BCRP Manager who can be contacted at the above address. The Data Processor is Shop Safe Limited.

Retention and Disposal of Data

Offender Data

Offender data files on ShopSafe Alert! will be automatically removed after 12 months. Any files containing offender data over 12 months old will be removed from the system. If the information is still relevant it will be reposted with written justification for the extension. Data files held on Excluded persons will be reviewed within one month of the expiry of the notice, warning period or other relevant order, and deleted if there is no justification for retention. If there is information or evidence to justify the extension of the notice, warning or other order, because of further offending or activity impacting on the business community - including breaches of the exclusion notice, this will be sufficient justification for retention of the data file for the period of the extension of such notice, warning or other order.

Member Data

Members data will be retained for the duration of their membership of the scheme, when it will then be deleted from the YBSN database.

Potential members' data will be retained until it is confirmed that they do not wish to join the scheme.

Members can unsubscribe from mailing lists at any time.

North Yorkshire Police and other Statutory Agencies

North Yorkshire Police as a partner of the BCRP will share and have access to the intelligence collated. If required, Police Inspectors may authorise an officer to have full access to the BCRP database for the purposes of the Prevention and Detection of crime in *North Yorkshire*. Nominated officers will be issued with their own passwords and a full data trail will be available for inspection if required. Information from the BCRP database may be provided to North Yorkshire Police and other statutory agencies in support of any applications or proceedings being taken against an individual which is impacting on the business community. This will include statistics as well as personal information.

Categories and Types of Personal Data Processed

ShopSafe Alert! collates the following information on Offenders:

- Biographic Data - Name
- Appearance Data – Physical description including hair colour etc.
- Special Category Data – Ethnicity, Criminal Records
- Biographic Data – Date of birth
- Offender address – Known addresses of the offender
- Offender images – Images of the offenders uploaded to the platform by the user
- Face Hash – Unique hash of face data created at facial recognition
- Vehicle Description – Physical description of vehicles including registration plate

The purpose of this processing is to enable Members to identify Offenders; to submit reports about them; to include them in a list or gallery of excluded persons; and to provide information about them which may be necessary to protect the personal safety of Members and their staff, customers etc.

Lawful Basis of Processing

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.

Conditions for Processing Special Category Data

YBSN process Special Category Data:

- Personal Data revealing **racial or ethnic origin**;
- Criminal Offence Data

Legal Basis for Processing Special Category Data

YBSN confirms processing of Special Category Data is necessary for the purpose of performing tasks carried out in the public interest, namely:

- **Preventing or detecting unlawful acts**, and/or
- **Protecting the public**, including through crime prevention and asset protection.

For further information see YBSN's *Appropriate Policy Document*

Personal Data Processing on Children

Under ShopSafe Alert! Terms of Use:

"5.5 No personal data should be uploaded of any Data Subject that is believed to be below the age of 18 years."

Because of this YBSN will not be processing personal data of anyone under the age of 18.

Consultation Process

The Board of Management considers it inappropriate and impractical to consult with Offenders on this *Data Protection Impact Assessment*.

ShopSafe Alert! Information Sharing Platform

To ensure the integrity of the ShopSafe Alert! database the following guidelines must be followed.

1. Intelligence / information held on the Alert! database will solely be used for the prevention and detection of crime or Civil Recovery and reducing anti-social behaviour creating a safe environment within the city.
2. To ensure an accurate audit trail only intelligence / information from identifiable sources will be placed on the database: information where the originator cannot be identified will be destroyed.
3. The information is confidential and must not be disclosed to any third party who is not a member of the BCRP or a member who has not signed the necessary Alert! agreement.
4. The responsibility and potential liability for inappropriate disclosure rests with the data controller as well as the individual members.
5. Breaches of confidentiality by members or their representatives may be subject to sanctions by the YBSN Business Crime Reduction Partnership. This may include withdrawal from the BCRP (without recompense) or the suspension from the BCRP / Exclusion Order Scheme.
6. Members must ensure the Exclusion Notices they receive are kept in a secure place and away from public view. All data issued to members will remain the ownership of the BCRP. Any member who attempts to copy, retain or distribute the information without the proper authority will be in breach of the Data Protection act 2018.
7. Members accessing data via Alert! provided by YBSN must not copy or reproduce any information obtained via that source. Quarterly audits of the on-line system will be carried out by the Business Crime Coordinator.
8. Only members of the BCRP, North Yorkshire Police or other statutory agency, who have signed the Alert! Terms of use, will be permitted to remain at briefings or meetings at the point when confidential personal information is discussed or brought to the attention of the meeting. Any individual or organisation represented at the meeting for other purposes, for example, to discuss an initiative or participate in discussions on trends etc, will be asked to leave. All persons attending a meeting will be requested to sign in to confirm eligibility to attend for the purposes during the period of discussion of personal information.
9. Members must keep any information or intelligence made available to them at briefings or meetings confidential and it will be used only for the purposes for it was generated, i.e. prevention and detection of crime and legitimate interests of the BCRP.

Necessity and Proportionality of Processing Offenders' Personal Data

It is necessary for the purposes of the Scheme to process appropriate personal data of Offenders as defined in the Scheme's *Data Protection Processing Policy (Offenders)* wholly or partly by automated means. This because:

- the number of Offenders of legitimate interest to Members, and the number of Scheme Members makes it impractical to process Offenders' personal data in any other way

- processing Offenders' personal data in any other way, for example in paper-form only, presents unacceptable risks in terms of data integrity, security and confidentiality
- adherence to the Scheme's data retention policy requires processing in this way

It is proportionate for the purposes of the Scheme to process Offenders' personal data as defined in the Scheme's *Data Protection Processing Policy (Offenders)* because:

- only the specific types of Offenders' data defined in the Scheme's *Data Protection Processing Policy (Offenders)* will be shared among the Scheme's Members, Data Controller, Board of Management etc in the manner defined in the policy.
- the Scheme's data retention policy as defined in the Scheme's *Data Protection Processing Policy (Offenders)* observes its obligation to process Offenders' personal data only for as long as is justified by the purpose for which the processing was originally undertaken.

Risk Assessment

Source of risk		Likelihood of harm Remote, Possible, Probable	Severity of harm Minimal, Significant, Severe	Overall risk Low, Medium, High
1	Offender may suffer distress if information about their involvement in a relevant incident is shared among their community, peer group etc	Possible	Minimal	Low
2	Offender may suffer distress if information about their exclusion is shared among their community, peer group etc	Possible	Minimal	Low
3	Offender may be incorrectly associated with an incident reported by a Members	Possible	Significant	Low
4	Offender may be known to a Member accessing the database	Possible	Significant	Low
5	Offender may be concerned about privacy intrusion	Possible	Minimal	Low

Measures Identified to Reduce Risk

Source of risk See Risk Assessment above	Option to reduce or eliminate risk	Effect on risk Eliminated, Reduced, Accepted	Residual risk Low, Medium, High	Measure approved Yes / no
1	Maximise security protocol Ensure Members' compliance with the <i>Data Integrity Statement</i>	Accepted	Low	Yes
2	Maximise security protocol	Accepted	Low	Yes

	Ensure Members' compliance with the <i>Data Integrity Statement</i>			
3	User submits Offender in compliance with the <i>Data Integrity Statement</i> Data Controller processes personal data only if confident in Member's compliance and data originality	Accepted	Low	Yes
4	Photos can be uploaded by members this is monitored at the Data Coordinator Any inappropriate post will be removed from the database. If a member continually breaches the Data Integrity Agreement it could result in expulsion from the scheme.	Accepted	Low	Yes
5	Information collected is in line with all relevant legislation, including Data Protection Act 2018 and Lawful Basis	Accepted	Low	Yes