DATA PROTECTION IMPACT ASSESSMENT

NATIONAL BUSINESS CRIME SOLUTION LTD (NBCS)
And
NATIONAL POLICE CHIEF'S COUNCIL (NPCC)

Freedom of Information Act
This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with you on receipt of a request prior to any disclosure. For external Public Authorities in receipt of an FOI, please consult with npcc.foi.request@cru.pnn.police.uk

Government Security Classification	**Official**
Publication Scheme Y/N	**No**
Title	**Data Protection Impact Assessment: NATIONAL BUSINESS CRIME SOLUTION**
Version	**V1.0**
Summary	The NBCS brings together a number of businesses that in isolation are having a minimal effect on crime reduction, but in collaboration are capable of pooling sufficient resource and information to have a significant effect on crime reduction within their member's geographical locations.
Unit, Dept	**National Business Crime Centre, City of London Police**
Author	**Supt. 13631 Patrick Holdaway**
Review Date	01/11/2022
Date Issued	06/05/2022
ISA Ref	NPFDU ISA ref 019

Information Governance & Security
In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this paper is strictly on a need to know basis and in compliance with other security controls and legislative obligations. If you require any advice, please contact npcc.foi.request@cru.pnn.police.uk https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework#risk-management

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Parts 1-4 should be completed by the business area / subject matter expert for the data processing activity.

1. NPCC National Portfolio Lead details

National Portfolio Lead	**AC Paul Betts**
Coordination Committee	**NPCC Business Crime**
Subject/title of activity	**National Business Crime Solution**
Name of SME contact	**Supt. Patrick Holdaway, National Business Crime Centre**
Name of DP contact	****S40(2)**, Senior Information Officer, City of London Police**

2. Introduction

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. What (non-DP) legislative framework supports the data processing activity?

Aim and Purpose

The project aims to bring together all police forces in England and Wales and the business community, on a national basis, to protect life, limb and property, commerce and productivity, and prevent and reduce crime. The purpose of the data processing is allow individual businesses to be better informed, bridge gaps in intelligence and enable the identification of known suspects or offenders, in order to better protect employees and customers.

The type of processing is manual and requires human intervention at all stages. The processing includes collection, storage, recording, use, alteration, disclosure, sharing, retention, erasure and deletion.

Legislative Framework

The non-data protection legislation that supports this processing activity is as follows;

1. The Crime and Disorder Act 1998
2. The Police Reform Act 1999
3. The Police Reform and Social Responsibility Act 2011
4. Anti-social Behaviour, Crime and Policing Act 2014

3. Describe the processing

3a) Describe the nature of the processing: *how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*

Collection;
Data is collected by the police when data subjects are processed through custody. Data is collected by NBCS from its members.

a) Via member direct entry – the member inputs the crime and intelligence data directly into the NBCS secure software, iNTEL ONE.
b) Via CSV – The member exports their data and sends it to the NBCS. The NBCS then imports the data and deletes the CSV export.
c) Via API – The members software speaks directly to NBCS iNTEL ONE and the data is transferred from one system into the other. The data remains in a secure environment at all times.
d) Via CJSM secure email – The member shares intelligence via CJSM. This intelligence is then inputted manually into the iNTEL ONE secure software.

Usage;
Data is used to prevent further crime, reduced crime and disorder, and reoffending, as well as protecting employees and customers. Data is also used to ensure civil restrictions can be imposed and/or fulfilled.
Primarily, NBCS uses the data to identify series offending where a particular offender or group of offenders are targeting multiple businesses or a single business multiple times (this includes both UK and foreign nationals). NBCS reviews that data and sends secure alerts to members making them aware of the risk against their business and supporting member internal crime reduction processes. NBCS also creates series linked investigations which are then shared with UK Policing. This is incredibly important as often UK businesses and independent Police Forces are not aware of the scale of the offending and the threat.
The NBCS also collects the data in order to identify business crime trends across the business landscape, data is anonymised and feeds mapping and analytics enabling NBCS members to understand the true nature of the threat against them and apply target hardening methodologies to protect their staff and customers and to reduce shrink.

Storage;
Data is stored on national and local crime recording systems and NBCS systems and sub-processors' systems.

Deletion;
Data is retained, reviewed and deleted in line with Management of Police Information (MoPI) Guidance for the police service. The data will be retained for 25 months by NBCS.

Source of data;

The source of the data is directly from suspects for the police service, whilst processed through custody. The source may also be victims or witnesses reporting details to police. The NBCS data is sourced from the members of NBCS.

Sharing;
The sharing of data from the police will be with NBCS. Data will be further shared with Business Crime Reduction Partnerships (BCRP) and/or Business Improvement Districts (BID), and where relevant with from NBCS to police forces.

Type of processing;
The type of processing undertaken is not considered to be in conventional terms; batch; real-time, online, multi or time-sharing, as the data processing method between police and NBCS is manual. The collection is real-time, however, the usage, filtering, sorting and other logical operations require human intervention.

Data Flow Diagram;
Please see process map and guidance.

High Risk Processing;
The processing stage considered to be high in risk is the sharing; range, volume and sensitivity of the data shared. There is also a loss of control, to a degree, once the data leaves the police environment.

3b) Describe the scope of the processing: *what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*

Nature of the data
The nature of the data may include the following;

- The subject's police custody photograph (if relevant, necessary and available)
- The subject's name
- The subject's DOB and age (if relevant, necessary and proportionate)
- The subject's residential address (for the service of exclusion notices only)
- Where a photo is not shared or available, a description of the suspect's appearance may be disclosed, which may include ethnicity, gender, height, build and any distinguishing features.

This information is considered to be contain special category data and/or criminal offence data. The above nature may be disclosed where a relevant policing incident is recorded.

Collect and Use
The NBCS receives and shares business crime data from member businesses with a view to enabling businesses to take preventative action, or make consumer decisions regarding data subjects, the NBCS will not make denial of service decisions, the NBCS member will make these of their own accord.

The data will be collected from multiple national businesses meaning the amount of data collected and processes will be sizeable; estimated to be between 50 and 100 thousand incidents per annum, enabling extensive intelligence opportunities for policing across England and Wales. An automated deletion process is built into the system, negating the need for manual intervention. When the data reaches the 25 month threshold it is automatically erased by the software.

There are strict deletion protocols built into the system, negating the need for manual intervention. As soon as the data reaches the 25 month threshold it is automatically erased by the software, preventing retention beyond that limit. The nature of the service means the data coverage will be national, covering England and Wales, no data will be processed or stored where the source is from outside of these countries. Multiple individuals concerned with criminality will be affected by the data processing.

Each police force will collect relevant information in the course of policing and use the data for a policing purpose. This information will differ from police force to police force and is dependent upon size.

The Business Crime data received from members can include any of the following, when relevant and lawful:

- Photographs/CCTV
- Vehicle registration information
- Names
- Addresses
- Modus operandi of known or suspected criminals.

Information Sharing Agreements with law enforcement authorities provide a mechanism for such authorities to share certain personal and criminal conviction and offence data, as well as detailed crime statistics, as appropriate, with NBCS in respect of persons convicted or suspected of involvement in business related crime. This information may comprise of:

- Relevant and proportionate extracts of data from police crime recording and custody imaging systems.
- Relevant and proportionate conviction information and also non-conviction information in respect of arrests, charges and cautions, on a case by case basis. A necessity test on a case by case basis will be required.
- Other non-conviction information and images may be shared to achieve the purpose on a case by case basis if it is deemed to be proportionate, lawful and necessary.

This information will only be shared with NBCS Members.

Information sharing agreements with law enforcement bodies allow such bodies to share with NBCS, any offenders who are likely to be cross company, or cross force, persistent, prolific offenders, or who have received an Order under relevant Anti-Social Behaviour legislation which prohibits them from entering any part of the area, or member premises. NBCS members will be able to assist the police in identifying persons in breach of these Orders.

Volume, frequency, retention and geographics

The volume, frequency, range and geographical areas will be diverse across police forces nationally and likely to be triggered by specific requests from NBCS, BCRP or BID, or undertaken as a matter course, in line with BCRP Managers, depending upon local resources. Nationally, the number of data subjects is expected to be millions and certainly over 5,000 data subjects.

3c) Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?*

Nature of Relationship with Individuals/Data Subjects
The nature of the relationship between the data subjects and the police; persons suspected of or offenders, having committed or being about to commit a criminal offence; and persons convicted of a criminal or civil (anti-social behaviour) offence.

Control
The control of processing by data subjects; none, other than information rights to request access, erasure and restriction.

Expectation
The expectation of processing from data subjects; each police forces' privacy notice should/will be clear in what, why, whose, when and how data subjects personal data is processed.

Children and Vulnerable Groups
Data subjects may include children or vulnerable groups; there may be data subjects that are children and/or vulnerable, being processed and this requires specific consideration.
To help manage the risk, police will only share details of children, or those deemed vulnerable, unless authority has been given from an officer not below the rank of inspector.

Concerns and security
BCRPs do not have the equivalent capacity or powers to prevent crime, detect crime or bring offenders to justice in the same context as the police service; the control of the police data is to a degree lost, once it is shared with NBCS; the security features of the NBCS system are comprehensive and well documented, see Information Security Factsheet (3) appendix NBCS01. The iNTEL ONE (Zinc Synapse) software is also G cloud Secure and approved.
Is this novel processing; whilst it is new to undertake a national processing arrangement, PubWatch, FaceWatch and similar schemes have been undertaken previously.

Novelty and technology
Using data in this way is not considered to be novel, as organisations have been successfully using data in this way for some time; e.g. BCRP and the processing is considered to be an extension of the Chief Constables/Commissioners purpose.

Current issues of public concern
The retail sector in particular has seen an exponential rise of assaults on staff, which in January 2021 led to the launch of a Home Affairs Select Committee on the subject. Following this a number of recommendations were made, many of which were

supported by the Government. An increasing number of Police and Crime Commissioners now have business crime as part of their policing plan, this is in direct response to increased engagement with business leaders and an acknowledgement that thriving businesses support local communities.

Approved code of conduct or certification scheme

The security features of the iNTEL ONE software are significant. The Zinc Systems SYNAPSE platform is a Government approved (G-Cloud 12) incident, crisis and threat management platform used by major UK Government agencies such as the Environmental Agency, a category 1 responder, City of London Police and well as high risk global organisations. Subsequently, the information security, cyber hygiene and infrastructure practices and been assessed and passed to the highest level of compliance and security.

Zinc Systems is ISO 27001 accredited and holds Cyber Essentials accreditation.

Zinc Systems are subscribed to the Risk Ledger platform as prescribed by City of London Police (CoLP0 and has completed a DPIA specific to the use of the SYNAPSE application. The Risk Ledger assessment was assessed and passed by the Director of Information (CISO & DPO) for the City of London Police. Key areas included;

- Security Governance
- HR Security
- IT Operations
- Software Development
- Network and Cloud Security
- Physical Security
- Business Resilience
- Supply Chain Management
- Financial Risk
- Environmental, Social and Governance

3d) Describe the purposes of the processing: *what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?*

Aim

The aim of the processing is to support member businesses, crime partnerships, the police and other agencies in the reduction of business crime through partnership work, intelligence sharing and target hardening strategies. The parties benefit from this type of processing through increased credibility and increased membership, this in turn allows the development of new products and services, and further support the business community through enhanced local, regional and national prosperity.

Intended effect on individuals

The intended effect on the data subjects, as suspects or offenders; is to disrupt, deter and curtail criminal and nuisance behaviour, prevent and detect crime and, bring offenders to justice. It is also intended that suspects/offenders experience an absence of their rights regarding freedom of movement and that this is upheld, particularly if guilt is found or admitted, and an order or notice of the court is issued. The intended effect on data subjects, as victims or witnesses, is to increase the awareness of potential threat, protect life, limb and property.

The NBCS brings together a number of businesses that in isolation are having a minimal effect on crime reduction, but in collaboration are capable of pooling sufficient resource and information to have a significant effect on crime reduction within their member's geographical locations.

Benefits to Police and law enforcement bodies

The collaboration supports such partnerships as recommended in the Crime and Disorder Act 1998, which places a responsibility on Police to work in partnership with other agencies, organisations and individuals in the furtherance of the reduction of crime and anti-social behaviour and the reduction of the fear of crime and anti-social behaviour in the community.

Benefits to the Police will include the reduction of crime and anti-social behaviour; improved opportunities for the apprehension of offenders; and reduction in the fear of crime.

This information sharing process will increase opportunity for better consistency and partnership working within the business community. It may also assist in any local crime reduction strategy. Statistically, levels of detections in areas participating in a crime reduction scheme improve, on a national level.

Benefits to NBCS members

The furtherance of BCRP/BID/NBCS partnership working helps to focus partnership awareness of local crime and improve the quality of shared intelligence with police and other agencies. All businesses will benefit from the reduction of crime and anti-social behaviour within the business district. This in turn encourages better co-ordination of police and partnership resources to deter and prevent crime.

Sharing relevant information improves the safety of employees within the area. It also assists in protecting the assets of the businesses trading within the area. The increased levels of detection will improve profitability and maintain a healthy consumer market, which is currently maintained by a combination of residents, commuters and tourists. Protecting these sections of the community improves the sustainability and continuity of the local business partners.

In addition, members will be alerted to the fact that habitual troublemakers who may already be subject to their exclusion schemes, or other interventions may also be subject to orders or restrictions imposed under relevant ASB legislation and thus will identify occasions when police may be best suited to deal with certain issues rather than placing employees at risk.

Specific examples to NBCS members of results achieved through data sharing with NBCS are set out below:

- NBCS is able to collate and link offence data provided by individual NBCS Members; this means offence data can be collated and provided to the Police as series linked investigations, making it more likely that offender will be apprehended through Police action. Such reporting makes eventual apprehension much more likely than individual reporting of crimes to the Police

by NBCS members.

- Members are more likely to report known or suspected offenders to NBCS than to the Police; NBCS is able use such offence data provided by Members to identify and analyse trends and generate reports; this in turn helps the Police and the member develop better strategies for dealing with crime.
- NBCS can identify prolific and persistent offenders targeting multiple businesses and personally serve exclusion notices against these individuals removing their implied right to enter those businesses; this in turn reduces the likelihood that those individuals will re-enter those business premises and commit further crime. Additionally, should that individual breach the exclusion notices then the NBCS can support that Member Business with Civil Court Injunction. This action further prevents the individual entering the member premises and if breached can constitute contempt of court.

Benefits to the Community

Local communities will benefit from being able to enjoy safer environments in which to shop, live, work and commute. This may also encourage more shoppers to the areas and thereby stimulate local economic growth. Some businesses may be encouraged to invest some profits back into community ventures through sponsorship or other funding, thus stimulating society and cohesion. An increase in consumers could create more employment opportunities and increased area affluence can have a positive impact on local safety, wellbeing and community.

3e) Necessity and proportionality: *Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? Does the processing affect or interfere with an individual's human rights, how & why? Does the activity address a pressing social need? Is the processing a proportionate response to this?*

Necessity: Businesses, particularly retail, experience crime on a regular basis. Policing are not always informed or able to respond to each incident, so there is an expectation that businesses do what they can to protect themselves. The effects of crime are both monetary in terms of lost stock, as well as the physical and mental health of retailers reporting increasing levels of violence and abuse aimed at their staff. A national ISA with policing will allow for greater information sharing, which would support both policing and the business community. Conversely, failure to share information risks eroding public confidence, leaving employees at risk of harm as well as affecting the viability of a business, affecting local communities.

Proportionality: The proportionality test is defined as "the public interest for disclosure outweighs the individual's right to privacy." As outlined above, business suffers not just from the event of the criminality but also ongoing from loss of business, cost of recovery and effects on employees. That effect is recurring and applies on each event regardless of the individual involved. Many offences also involve the public being targeted as victims also, who then have the disheartening burden and cost of replacing valuable items, if they can. That event is suffered by numerous parties in their own way as they are subject to these high-harm individuals. It necessarily follows that a case can be made that recidivist offenders who do pose these risks as active criminals have their right to privacy outweighed by that risk and the harm they are likely to cause to the public and business.

The police will only share information in limited circumstances where absolutely necessary i.e. where there is a repeat offender and a relevant incident recorded on a policing crime management system.

4. Consultation process

Consider how to consult with relevant stakeholders: *describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*

The main stakeholders are the businesses, who support NBCS, NBCS themselves and policing. The demand to be able to share information securely and efficiently with policing by business is over whelming. Improved reporting mechanisms will allow policing to see a clearer picture of the true extent of crimes that affect business, which will only increase the need to share data so allowing businesses to better protect themselves.

There are 80+ businesses supported by NBCS, within the following business sectors;
Fashion
Wholesale
Supermarket and Convenience
Speciality
DIY
Transport and distribution

Distribution Centres
Business Crime Reduction Partnerships
Business Improvement Districts
Shopping Centres
Online Retail

Consultation has taken place with the following:
The draft DPIA and ISA has been circulated to regional police Information Security and Information leads for consultation as well as the DPO the National Police Chief's Council. Feedback received has contributed to the changes made within these documents.
Within NBCS: consultation is ongoing with the following groups NBCS Leadership Team, Operations Team (Data Processors) and Member Operations Group. Privacy impact consultation and review is a formal part of the eight weekly Leadership and Team meeting agendas. It is also a regular agenda item during the NBCS Ordinary Member meetings and Operational Team meetings, which are held quarterly. NBCS has engaged with external Information Security Practitioners for advice and guidance and will maintain this relationship for the foreseeable future. Members are reminded of the data protection requirements during Service Level Agreement meetings, which take place at least bi-annually. NBCS works in partnership with its Members to ensure compliance to acceptable standards including control measures applied to identified risks for both parties both during service delivery and product onboarding.

External Consultation (Public)
No public consultation has been conducted. NBCS consider the data subjects to be offenders or suspected offenders and it is likely they would not support data being used for this purpose. NBCS considers that offenders would fully expect their details to be added to databases such as iNTEL ONE, processes in order to detect and deter crime and to be shared with UK Policing.

Part 5 should be completed with the support of your force DPO or another appropriately experienced Data Protection professional.

5. Assess compliance

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? If you are relying on consent, how will this be appropriately managed? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Principle 1: Lawful and Fair (and Transparent)

Lawfulness:
NBCS

- NBCS is not a competent authority all processing is under the UK General Data Protection Regulation (GDPR) 2016/679 and therefore its processing of criminal conviction/offence data must meet one of the conditions in Schedule 1 of the Data Protection Act 2018 (DPA 2018).
- Schedule 1, Part 2, Paragraph 10(1) of the DPA 2018 includes substantial public interest conditions for sharing data including when the processing of such offence data is (a) necessary for the purposes of the prevention or detection of an unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes and (c) is necessary for reasons of substantial public interest
- Part 2, Chapter 2, Section 10(5) of the DPA 2018; *Special categories of personal data and criminal convictions etc data*; states that the processing meets the requirement in Article 10 of the UK GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1.
- Article 10 of the UK GDPR; *Processing of personal data relating to criminal convictions and offences*; states that the processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.
- NBCS processing of criminal offence data will be reviewed on a case by case basis and the data sharing is minimal and is critical to the prevention of criminal acts. The significant and proven contribution of NBCS to crime identification and prevention is set out in 3d. Relevant information related to crime and the prevention of crime, held by NBCS, for such purposes as implementation of individual exclusion processes, the execution of proactive industry operations and other operations with the intention of lowering business-related crimes will only be passed to the Police if there is a belief that the information is not already in possession and is in the public interests of safety and social economic wellbeing.

Sharing information supports the prevention and detection of crime in several ways; 1) Assists in the identification of offenders 2) Enables the true scale of the issues to be demonstrated to Members and Policing 3) Enables effective reporting of the true scale of business crime into the Home Office to enable appropriate policy making.

The sharing is "necessary" for the prevention and detection of crime because NBCS could not reasonably achieve its purpose by any other means

Police

- The police's authorisation in law to process data for law enforcement purposes comes from Common Law. The police's first principle compliance for law enforcement processing is:
- Where the police process personal data for a law enforcement purpose under Part 3, Chapter 2, Section 31; The law enforcement purposes; *For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*
- Compliance with the first principle under Part 3, Chapter 1 Section 35 of the DPA 2018 is achieved as follows:
- The processing is based on, and underpinned by, the Common Law policing purpose
- The processing is necessary for the performance of a task carried out for a law enforcement purpose by the police, acting as a competent authority under Part 3, Chapter 1 Section 30 of the DPA 2018.
- Where sensitive processing is involved the processing is strictly necessary for a law enforcement purpose, an Appropriate Policy Document exists for each force, under Part 3, Chapter 2, Section 42 of the DPA 2018 and the following DPA 2018 Schedule 8, Paragraph 1 condition is met: (a) the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest.
- The processing is fair towards data subjects because (i) it is consistent with the data subjects' reasonable expectations that the police will process their personal data for law enforcement purposes; (ii) the police have Privacy Notices which provide privacy information, adequately describes the purposes of processing, including retention periods, recipients, and transfers; and (iii) the NBCS is promoted/advertised by members.

- As competent authorities, the police lawfully process data under Part 3, Chapter 2, Section 35 of the DPA 2018 where it is necessary for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Fair Processing:

Each Police force will have its own comprehensive privacy notice. This is supplemented by the NPCC privacy notice.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

NBCS

- The information shared by NBCS will be that which was originally obtained for the prevention of crime, disruption and deterrent of criminal and nuisance behaviour.
- Sharing this information with a third party, in this case NBCS members or the police or other law enforcement bodies, will not result in the information being processed in any manner contradictory to the original purpose. The processing enhances the ability of police forces and widens the policing community and resources.

Police

Purpose limitation for policing may be attained through; limited access to the data; provisions and testing. Further; the data flow diagram and a full understanding of the processing is clear to all parties and controlled at all stages; the purpose is stringent; the data processed and examples of resulting outcomes should be shared with NPCC and relevant parties within the senior management of all parties for understanding.

The expected benefits to the NPCC, policing and the victim, should be stipulated before sharing and absolute.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

NBCS achieves this principle by:

- minimising the personal data it holds and processes;
- de-identifying the data, whenever business processes allows;
- formally reviewing the adequacy and relevant of personal data annually, adjusting where it finds that personal data is not relevant or is not adequate and this is captured in the data asset register;
- only sharing data with organisations to whom it is relevant and ensuring that the minimal amount of data should be share for the purposes set out in this DPIA.

Police

Police forces achieve this principle by following the National Decision Making Model in regard to proportionality to ensure only the minimal amount of personal data necessary is shared with NBCS to achieve the purpose; moreover this information will only be shared in limited circumstances, where a repeat offender has been reported to a police force and a record of the crime instance made on a police crime management system.

The 3rd Data Protection principle and compliance for law enforcement processing, where the police process personal data for a law enforcement purpose (DPA Section 31) compliance with the DPA third principle (DPA Section 37) is achieved as follows:

- The police will limit any disclosure of personal data to NBCS to that which is relevant and not excessive to the law enforcement purpose and will ensure the personal data is adequate. This will be achieved through manual review of the personal data involved.
- A similar process will be adopted for any personal data disclosed to the police when it is uploaded onto police systems.
- The processing of specific data has to be relevant, necessary and proportionate. Non-relevant data is removed, redacted and/or anonymised and includes justification for the absolute benefit of victims.
- Quality is maintained through; control of incoming data, avoidance of duplication; explicit initial requirements; data integrity and ethics enforced; data cleansing; auditable data flow; testing and data quality consultation assured and controlled.
- Review, inspection and audit should ensure standards are maintained. Any audit reporting should be shared with Information Management Teams within the police and relevant representatives of senior management.

Principle 4: Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

NBCS achieves this principle by:

- Maintaining processes that assure the quality of personal data shared with NBCS, advising the source when NBCS finds that data to be inaccurate or of poor quality;
- Maintaining processes that keep personal data up to date.
- Making it easy for data subjects to ask for their personal data to be rectified or erased, when legally permissible.
- Erasing or rectify data that is found to be inaccurate or out of date with 72 hours of discovery.

Police forces are subject to additional requirements of the fourth Data Protection principle (Section 38 of the DPA 2018) to ensure greater accountability for accuracy of any data processed for law enforcement purposes.
The 4th principle compliance for law enforcement processing for the police service, where the police process personal data for a law enforcement purpose (DPA Section 31) compliance with the DPA third principle (DPA Section 38) is achieved as follows:

- The police have in place processes to review the accuracy of personal data held on police systems and update or correct it where necessary to do so.

These processes are applied to personal data that is disclosed data or received.

- Police processes also ensure that clarity over the status of a data subject as an offender (alleged or otherwise), convicted person, victim (alleged or otherwise) or witness.
- Personal data will not be amended where it is required for evidential purposes or where it is an accurate record of an inaccurate or untrue allegation.
- Subject rights applications regarding accuracy will be processed in accordance with the DPA.

The following should be undertaken; checks against original requirements; identification of inaccurate/less reliable data sources are acted upon or at least taken into consideration/cleansed by all parties. Manual checks take place.

Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

NBCS achieves this principle by:

- Data held on the system will be automatically deleted at the end of a 25 month period.
- Reviewing its use of personal data and destroy information when it no longer supports the define purpose for processing it.

Police forces will follow the guidelines in the Management of Police Information (MoPI) for the retention, review and disposal of data processed for law enforcement purposes. A detailed breakdown is available through the NPCC Schedule on Review, Retention and Destruction. The police will fully considered and abide by this guidance.

Principle 6: Security And Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

NBCS achieves this principle by:

- Establishing an effective information security policy framework, which aligns with ISO27001.
- Designing processes with 'privacy by design' in mind.
- Maintaining procedures that:
  a) Identify assets, which impact personal data.
  b) Map data flows of personal data.
  c) Risk assess assets and data flows.
  d) Identify owners of assets, risks and data.
  e) Control the disposal of personal data.
  f) Manage the transfer and sharing of personal data.
  g) Seek assurance from our third-party partners.

h) Put in place information sharing agreements, so that we all have a common understanding of the use and protection of personal data.
i) Manage information security incidents, learning from them to prevent reoccurrence and reporting to the ICO when required.
j) Establish clear roles and responsibilities for all staff, so that they understand what is expected of them and who to contact for support.
k) Effectively manage joiners, movers and leavers within the organisation.
l) Provide our staff with training and supervision, so that they can confidently handle personal information and systems that process it.

- NBCS will also ensure only software accredited to ISO27001 will be used for the processing of data.

Police forces will ensure that appropriate technical and operational measures are in place to maintain the security and confidentiality of data they process.

Principle 7: Accountability

NBCS

For the purpose of the agreement the NBCS holds the position as Data Controller. NBCS has robust service contracts and ISAs with every member. NBCS has also conducted its own Legitimate Interest Assessment and DPIA in relation to these processes.

Police

The NPCC is a non-statutory entity that is a collaboration between Chief Constables under the terms of the NPCC s22a Collaboration Agreement. In relation to the carrying out of their collaborative functions for the NPCC or responsibilities under the s22a agreement, it is understood that each individual Chief Constable/Commissioner is the Controller[1] for their own force's data with the NPCC Business/Retail Crime lead (Assistant Commissioner Paul Betts) acting as Lead Controller for purpose of this agreement.

Additional information in regard to:

Subject Rights: *which subject rights applicable to this processing, how are they managed, who is responsible for what, who is the main contact for data subjects.*

Subject Rights requests will be managed by each individual force, following the procedures they already have in place.

NBCS subject rights are exercised via enquiries@nationalbusinesscrimesolution.com

[1] Controller for the purpose of the MoU is as Article 4(7) of the UK General Data Protection Regulation

Third Party Processors: *are any third party processors involved, do you have data processing agreements/contracts in place that cover how subject rights/breaches will be managed.* NBCS data is hosted by Amazon Web Services (AWS) and the software is supplied by Zinc Systems. Servers are based in UK.
International Transfer: *what additional safeguards are being used for this processing.* There are no intented transfers outside of the United Kingdom. Data will remain within the UK at all times, on UK servers.

Parts 6-7 should be completed by the business area / subject matter expert, in conjunction with the DP professional

6. Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1) Unfair and unlawful sharing/processing.	2	3	6
2) User error, misuse, data corruption, loss of service.	2	3	6
3) Onward processing deemed to be beyond the original purpose of collection.	1	3	3
4) Too many data categories or types are processed with NBCS and members.	1	2	2
5) Incorrect data items/categories obtained and provided to NBCS and members.	2	3	6
6) Retention by all parties is beyond its use/usefulness, and therefore unlawfully held.	1	2	2
7) Technical and organisational measures are not in place.	2	3	6
8) The Zinc System is not security accredited or secure.	2	3	6
9) Unauthorised access to NBCS records by unauthorised persons.	2	3	6
10) Passwords are maliciously or accidentally disclosed.	2	3	6
11) Insecure infrastructure or premises; is subject to a cyber attack; the information is held or used in an insecure environment.	2	3	6
12) Insecure transmission of data to and from NBCS and its members; misdirection of email traffic through incorrect addressing.	2	3	6
13) Data subjects rights derogated and of being informed re further processing.	1	2	2
14) Information can be damaged/inappropriately deleted; the integrity of the information is jeopardized; the information is inaccessible to those who should have access to it; or the information is not shared when it could be; users are inadequately trained; there is a disproportionate impact on certain groups.	2	3	6

7. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Fair and Lawful; It is not lawful or fair to process or share this data with NBCS and unknown members/third parties. User error, misuse, data corruption, loss of service.	A legally binding Information Sharing Agreement (ISA) is in place and signed by legal authorities on behalf of NPCC and NBCS. NBCS and all forces Privacy Notices and policies indicate that disclosure/processing can take place for such purposes; who, when, where, what, why and how. Documented user training on the system/software; dedicated contact within the member businesses; regular penetration testing; regular patch updates; data saved on servers which can then be restored; use of reputable support company; support company ISO27001 compliant; software hosted on UK based servers.	Reduced	Low	

Purpose Limitation; The onward processing to a non-law enforcement organisations for non-law enforcement purposes, is deemed to be beyond the original purpose of collection.	This is mitigated through; correct lawful bases, limited access to the data; provisions and testing. Further; the data flow diagram and process map, and a full understanding of the processing is clear and controlled at all stages; the purpose is stringent; the data processed and resulting outcome is shared with Information Governance/Compliance (IG/C) Teams and relevant parties within senior management for understanding, responsibility and ownership. The legally binding ISA, Privacy Notices and policies state the purpose and limitations therein of the expected processing.	Reduced	Low	
Data Minimisation; The risk is that too many data categories or types are processed and shared with NBCS and members.	The processing of specific data is relevant, necessary and proportionate. Non-relevant data is removed, redacted and/or anonymised and includes justification for the absolute benefit of victims. Data quality is maintained through; control of incoming data, avoidance of duplication; explicit initial requirements; data integrity and ethics enforced; data cleansing; auditable data flow; testing and data quality consultation assured through IG/C Teams and controlled through operational officers. Review, inspection and audit will ensure standards are maintained. Any audit reporting should be shared with IG/C Teams and relevant representatives of senior management.	Reduced	Low	

Accuracy; Incorrect data items and categories are reported to police and obtained from victims, then supplied to NBCS and members.	The following will be undertaken; checks against original requirements; use of prescribed data entry template; documented user training for system/software entry; dedicated contact within the member businesses; all forces to advise NBCS in writing, who will then amend/delete data; identification of inaccurate/less reliable data sources are acted upon or at least taken into consideration/cleansed by all parties. Manual checks take place.	Reduced	Low	
Retention; The data is retained by police forces, NBCS and members beyond its use and/or usefulness, and therefore, is unlawfully held.	The NPCC Schedule on Review, Retention and Destruction of the data used are fully considered and abided by, from a policing perspective. NBCS and it's members confirm and it is documented within the ISA and Data Protection Policy that the obtained police data is held for a maximum of 25 months, unless, on a case-by-case basis, it is needed to be retained for injunction or other legal reasons.	Reduced	Low	

Security; Technical and organisational measures are not in place to protect data and/or individuals. The Zinc System, web based or software is not security accredited and considered to be unsafe to store police data. Unauthorised access to NBCS records by unauthorised persons. Passwords are maliciously or accidentally disclosed. The system is hosted on an insecure infrastructure or premises; is subject to a cyber attack; the information is held or used in an insecure	Technical and organisational measures are place to protect data across the police estate, with full time Information Security (InfoSec) Teams, subject to penetration testing, and preventative measures regarding the access to systems by way of firewalls and a series of approved security measures both in the digital estate of the police service network (PSN). The Zinc System is a secure platform, with an individual username and password policy; regular penetration testing and; regular patch management/updates undertaken. Username and password required for access; complex usernames used for access; minimum 8-character passwords, numbers and symbol required; dedicated contact within the member business. Zinc Systems hold ISO27001 accreditation and undertakes penetration testing. Email transfer will be to secure email accounts only and held on Zinc Systems which cannot be removed, copied or reused by members.	Reduced	Low	

environment; insecure transmission of data to and from NBCS and its members; misdirection of email traffic through incorrect addressing.				

Data Subject Right; Data subjects cannot exercise their rights and are not specifically informed regarding the processing of their victim/personal data for onward prevention or use by a non-police, law enforcement agency/commercial company. Unjustified refusal of service to the data subject. The information is being used unfairly or without transparency to data subjects. The information cannot be amended, erased, restricted, objected to or accessed on the Zinc System.	Police Privacy Notices are easily available and transparent, for the public and victims to see and understand how, who, where, when, why and what processing is undertaken by the police. All police websites include pages on "how to request police information" under a number of pieces of legislation, including how to request personal information. Any discovery of personal data breaches or losses of information will instigate a pause in processing. This pause should also instigate a review of the undertaking with the responsible police business area, IG/C Team, NPCC and NBCS. Member internal process; NBCS do not prevent entry to any individuals onto a member premises. NBCS will consider the publication of the ISA or consider indicating the use of open and transparent use of social media to advertise the relationship. The Zinc System allows or early removal, amendments, extension of storage.	Reduced	Low	

Other risks; The information can be damaged or inappropriately deleted; the integrity of the information is jeopardized; the information is inaccessible to those who should have access to it; or the information is not shared when it could be; users are inadequately trained; there is a disproportionate impact on certain groups.	Audit and review functions are fully undertaken. Records of changes to information obtained are routinely assessed. Access audits are automatically and manual checked.	Reduced	Low	
All NBCS members are not documented and are not known to all police forces, sharing police information.	All NBCS members are indicated to all police forces.			
The data processing contract between	The full contract between NBCS and Zinc Systems is held on behalf of all forces by the NPCC.			

NBCS and Zinc Systems is not held and are not known to all police forces, where police information is being held and processed.				

Part 8 should be completed by the business area / subject matter expert

8. Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA