Tunbridge Wells SAFE TOWN Partnership

Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The Tunbridge Wells Business Crime Reduction Partnership has been established to assist members of the business community in the area, who are vulnerable to theft, intimidation and assault, anti-social behaviour and other criminal activity by customers or anti-social elements. The members join together to share and exchange information about the activities of suspects, whether identified or not; to take steps to alert other members to the presence of those potential risks; to exclude potential offenders from their business premises; to arrest them or to take such other action either jointly or singly, to prevent theft, violence and anti-social behaviour and to protect their assets and staff.

Members will be encouraged to identify offenders by name, if known, or by description, and to communicate information about those persons, their movements and their associates, where it is suspected or believed that the intention and presence of those persons is or may be unlawful.

The need for a PIA has been identified because new information of criminal behaviour will be collected about individuals and disclosed to the members and partners who are organisations and people who have not previously had routine access to the information. The information will also be used to assist the Board of Management to make decisions and subsequently take action against individuals that could have a significant impact on them in the form of exclusion notices.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Where a criminal offence has been committed against a member, that member, apart from any notification to police, should complete an incident report and forward it to the Partnership Co-ordinator of the partnership.

The Partnership Co-ordinator will assess that information for accuracy and relevance before making a decision as to whether the information should be retained or disposed of forthwith. If the offender is unknown but the incident has been dealt with by police, the Partnership Co-ordinator will request the offender's details to be disclosed by the police using the appropriate policy and paperwork. If the information is to be retained, a decision will be made as to whether it is to be made available to members to assist in the prevention and detection of crime and the prosecution of offenders, or whether it is to be retained for a defined period of time to ensure that any future offending behaviour by that person may be linked and further action taken in light of that.

Where personal data is to be made available to members, it will be by electronic means through a database system designed for that purpose and operated exclusively by the partnership for that purpose.

The number of persons affected by this will vary depending on levels of criminal activity and other local conditions. All personal or sensitive personal data will only be processed in accordance with the data protection principles set out in the Act.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Consultation has taken place internally with the board of management/directors who are local business members of the partnership and other persons co-opted as board members, as well as the broader membership to ensure that they are fully aware of the nature of the work of the partnership, their duties in respect of oversight of the work of the Partnership Co-ordinator and the liabilities which may be incurred in the event of any failure.

Externally, the Partnership Co-ordinator is in regular communication with the police, who are supportive of the work of the partnership and who have access to partnership data for the purposes of the prevention and detection of crime and the prosecution of offenders, and who also provide the partnership with selected information to assist in that purpose. The partnership has an information sharing agreement with Kent Police which sets out in detail what data the police will provide to the partnership, who it may be circulated to, its retention period and other restrictions, permissions or reviews.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Targeting or identification of offenders, suspects or persons of interest	Incorrect identification of persons of interest and circulation of information	Failure to properly validate information	Breaches of DPA, reputational damage

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Incorrect processing or circulation of data relating to individuals	Ensure ALL information is properly and thoroughly checked before consideration is given to circulation to members	The risk is reduced considerably	Provided the intelligence related to each potential offender is subject to proper review and analysis before it is considered for circulation, then the subsequent response is proportionate to the risk and is a legitimate aim of the partnership

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
Incorrect processing or circulation of data relating to individuals	1. Correct assessment by the Partnership Co-ordinator 2. Oversight of the Partnership Co-ordinator by a nominated board member or director (the data protection officer)	The board of management/directors of the partnership

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Appoint a Data Protection Officer from within the Board	11 July 2017	BoM

OUTCOME: Jack Smith appointed as DP Officer 11/7/17

Contact point for future privacy concerns
The Partnership Co-ordinator is the initial contact point for the partnership. They will bring any privacy concerns or subject access requests to the immediate attention of the board or designated board member.

July 2017

July 2017

Annex three

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?
The project is designed to assist member businesses to reduce the considerable risk of crime, violence and anti-social behaviour on their businesses, their staff and customers, and to reduce the economic harm which is caused by such behaviour.

How will you tell individuals about the use of their personal data?
Where it is possible, offenders will be informed that their data will be retained by the partnership for specified periods for the purposes of the prevention and detection of crime and the prosecution of offenders. Offenders will receive written notice when the partnership has made a decision to exclude them from the premises of members following an incident or series of incidents

Do you need to amend your privacy notices? No

Have you established which conditions for processing apply?

Section 29 (1) of Part IV of the Data Protection Act (DPA) states that:
Personal data processed for any of the following purposes:

(a) the prevention or detection of crime;
(b) the apprehension or prosecution of offenders

are exempt from the first Data Protection Principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and Section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

1. Data processing must be carried out in accordance with Schedule 2 of the DPA *Conditions relevant for purposes of the first principle: processing of any personal data;* this will generally relate to purposes under 5(a) or (d) or 6(1) of Schedule 2.

2. Data processing must be carried out in accordance with Schedule 3 of the DPA – *Conditions relevant for purposes of the first principle: processing of sensitive personal data*; this will generally relate to purposes under 3(a) (ii), 5 and 7 (1)(a) and (2) of Schedule 3.

3. Where it is proposed that the matter be referred to police as an offence for their investigation and disposal, purpose 6(a) and 7(1) (a) of Schedule 3 may also be invoked.

4. The processing is in accordance with the conditions set out in The Data Protection (Processing of Sensitive Personal Data) Order, 2000:

> "Personal data processed for any of the following purposes—
> (a) the prevention or detection of crime
>
> (b) the apprehension or prosecution of offenders
>
> are exempt from the first Data Protection Principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection".

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
We are not relying on consent to process data.

If your organisation is subject to the Human Rights Act, you also need to consider:
The partnership is a private body exercising rights of property and is not a public authority as defined by ICO guidance.

Will your actions interfere with the right to privacy under Article 8?
We will not interfere with the rights of the subject under article 8 as we will only process personal or sensitive personal data which has been made publicly available by the subject's own criminal behaviour. We only circulate such data to our members, police or other agencies with whom we have a written ISA and who we have provided such advice and warning to against unauthorised disclosure of the information to minimise the risk of data being misused.

Have you identified the social need and aims of the project?
The social needs and aims of the project are set out in the National Association of Business Crime Partnerships ltd, codes of practice and advice, of which we have a copy. The objectives are to reduce crime, violence and anti-social behaviour against our members in the areas in which we provide that service.

Are your actions a proportionate response to the social need?
Our actions complement those of the police and other agencies. This has become increasingly necessary as police and public resources have been reduced and the focus has moved away from the physical policing and control of management of the areas in which we operate. The absence of police and reduced levels of deterrence, arrest and prosecution have required the local business community to become more pro-active in

providing crime prevention services to its members which helps to provide commercial benefits to the community.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?
We rely on the specified purposes of the prevention and detection of crime and the prosecution of offenders as set out in the preceding section 'Have you established which conditions apply for processing'.

Have you identified potential new purposes as the scope of the project expands?
We do not anticipate extending our purposes beyond those already identified.

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?
The quality of the information presented to the Partnership Co-ordinator may be of variable quality and utility and all data is required to be further assessed before any decision is made as to its further purpose. Where any data does not fulfil the criteria of being fit for purpose, it will not be used. It will not be retained beyond a reasonable period and will then be deleted.

Which personal data could you not use, without compromising the needs of the project?
Any data which is either not sufficient, relevant or useful or which does not meet the standards of the DP principles will not be used and will be deleted.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?
Partnership software has been designed to facilitate the updating of any data contained within its records and also produces an automatic 'bring up' prompts which requires the Partnership Co-ordinator to assess the

data periodically and to make a decision as to whether it should be retained for a further period.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?
Data obtained from members is assessed for its accuracy either from knowledge of the subject, further enquiry of the author, police confirmation, visual evidence (CCTV) or other publicly accessible records.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?
Retention periods are set depending upon the severity and frequency of the offending behaviour. All data is reviewed automatically through the review facility of the partnership database, or by manual examination. Where there is no longer a requirement to retain data to assist in the prevention and detection of crime and the prosecution of offenders, it will be deleted.

Are you procuring software that will allow you to delete information in line with your retention periods?
The partnership database contains a facility to review data, which must be completed in each case. Where data is nor reviewed in line with the 'bring up' prompt, it is automatically deleted.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?
The partnership is able to respond to data access requests in compliance with the DPA either by accessing the database or by accessing paper records. The NABCP Codes of Practice and Advice contains instructions and specimen letters to assist in responding to requests.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
The project does not, and will not, involve marketing.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and

against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?
The partnership database is only accessible to members who have signed the partnership data integrity and membership agreement. There is an audit trail which automatically identifies any person logging on to the restricted areas of the partnership website.

What training and instructions are necessary to ensure that staff know how to operate a new system securely?
Training is given to new staff both on the technical capabilities of the system and on the requirements of the DPA. Members are provided with sufficient information to inform them of the importance of data integrity and the requirement to comply with all partnership rules concerning access to and divulging of, personal or sensitive personal data.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?
The partnership will not transfer any data outside the EEA.

If you will be making transfers, how will you ensure that the data is adequately protected?
Not applicable.