Police ICT Company
National Enabling Programmes

Data Protection Impact Assessment

Delivery of the National Management Centre and Identity Access Management and Productivity Services

Programme DPIA

Version: 1.1
Date: 2 May 2019
Author: S40 Personal Information

Status: Official

VERSION HISTORY

Version Number	Changes since last version	Status	Date	Author(s)
0.1	First draft	Draft	11 February 2019	S40 Personal Information
0.2	Updates to reflect feedback following technical review	Draft	21 February 2019	S40 Personal Information
0.3	Updates to reflect feedback from Deloitte, BT and further NEP technical review in light of supplier comments	Draft	11 March 2019	S40 Personal Information
0.4	Updates to reflect comments and amendments following review by S40 Personal Information , and other responses to earlier queries	Draft	16 April 2019	S40 Personal Information
0.5	Minor updates to address outstanding comments	Draft	18 April 2019	S40 Personal Information
0.6	Further mark-up from S40 Personal Information	Draft	23 April 2019	S40 Personal Information
0.7	Minor edits/tidy up following S40 Personal Information final review	Draft	28 April 2019	S40 Personal Information
1.0	Version 0.7 uplifted – Enclosure B(1) embedded and contents page updated	Final	28 April 19	S40 Personal Information
1.1	Appendix added	Final for sharing with forces	2 May 2019	S40 Personal Information

CONTENTS

Step 1: Identify the need for a DPIA

Initial screening questions

In accordance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), a data protection impact assessment ("**DPIA**") is required when the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35 of the GDPR).

The data controller may also in this case need to consider Part 3 of the Data Protection Act 2018 ("**DPA 2018**") which applies to processing by competent authorities for law enforcement purposes. s64, Part 3 of the DPA 2018 requires a DPIA to be carried out where the processing is "*likely to result in a high risk to the rights and freedoms of individuals*".

The following nine criteria[1] should be considered to determine whether a DPIA is required, namely where the processing in question entails:

1. Evaluation or scoring
2. Automated-decision making with legal or similar effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract"

If two or more of these criteria are met then a DPIA should be carried out. In some cases a DPIA should be carried out when only 1 criterion is met.

The Information Commissioner's Office has also published a list of ten types of processing that automatically require a DPIA[2]:

1. Use of innovative technology
2. Use of profiling or special category data to decide on access to services
3. Profiling of individuals on a large scale
4. Processing of biometric data
5. Processing of genetic data
6. Matching of data or combining of datasets from different sources
7. Collection of personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')

[1] This list is taken from the Article 29 Working Party's Guidelines on DPIAs.
[2] See here for further details on the ICO's guidance relating to DPIAs.

8. Tracking of individuals' location or behaviour
9. Profiling of children or targeting marketing or online services at them
10. Processing data that might endanger the individual's physical health or safety in the event of a security breach

These criteria are considered in more detail in the next section.

The following documents are also referred to later in this DPIA; each one is embedded below for ease of reference:

A. NEP Initial Privacy Impact Assessment v1.0 dated February 2018

S31 Law Enforcement

20180218_NEP_Initi
al_PIA_v1.pdf

B. (1) NEP Update for Suppliers of Policing PowerPoint Presentation dated 19 November 2018 To be provided upon request and circulated separately due to very large file size. (2) NEP IAM and PS LLD – Volume 1 – Introduction – V6.0

S31 Law Enforcement

C. Office 365 for Policing – National SIRO Risk Decisions v2.0 dated 15 June 2018

S31 Law Enforcement

Explain broadly what the 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. Summarise why you identified the need for a DPIA.

PROJECT AIMS AND BENEFITS What

is NEP?

The National Enabling Programmes ("**NEP**") aim to deliver a hybrid cloud/on premises IT solution to UK Police Forces in line with the UK Policing Vision 2025. NEP will deliver a variety of productivity services (including various Microsoft products), an Identity and Access Management capability and a National Management Centre (Cyber Security Operations Centre) centralising information security monitoring capabilities.

The move to a cloud based environment means that police information and user credentials will be stored on infrastructure provided by Microsoft and Amazon Web Services which may present privacy concerns. The significant improvement in user monitoring capabilities may also present some privacy concerns.

This DPIA has been written to assess the NEP's consideration of privacy based risks and issues. In particular it

assesses the Security and Risk Management (SRM) process to understand how privacy has been integrated into the NEP solution.

Background

In general, UK Police Forces rely on Microsoft productivity tools, Sailpoint IdentityNow and on-premises IT infrastructure to conduct their day-to-day tasks (up to GSC Official security classification, including Official information which is sensitive and must be handled accordingly). Each Police Force implements their IT solutions differently as they act as independent organisations where the procurement of IT is concerned. This has led to a non-homogenous IT estate deployed across UK policing. One of the effects of this is that security of the Police IT estate is extremely difficult to implement and assure.

The approach to Cyber Risk management and the application of security controls therefore differs from one force to another and includes mitigation of risk with the use of security technologies, people and processes within the respective police force. The understanding of risks also differs between organisations, likewise the level of risk appetite.

The impact on system and information security also affects the protection of the privacy of Police Officers, Police employees, victims of crime, witnesses, suspects in investigations, convicted offenders, general public and any other parties involved in Police work. Despite the lack of consistent security implemented across the UK Police IT estate it should be noted that information security and privacy are embedded in Police cultures and behaviours; there is also clear guidance given in the Management of Police Information (MOPI) policy which Police Forces adhere to.

The National Enabling Programmes Solution

The National Police Chiefs Council ("**NPCC**") has set a UK Policing Vision 2025 to have all 48 Police Forces in the UK digitally enabled and cloud ready. To enable this vision, the National Police Technology Council ("**NPTC**"), with sponsorship from the NPCC and the Association of Police and Crime Commissioners ("**APCC**"), has secured initial funding from the Police Transformation Fund ("**PTF**") to establish three national solutions as part of the NEP initiative:

- A Security Operations Centre ("**SOC**") - to deliver a nationally coordinated monitoring, response and remediation capability in order to protect all UK Police Forces from cyber threats.
- An Identity Access Management ("**IAM**") platform - to enable user access to local, regional and national information, network and applications including cloud services in an efficient and effective manner.
- Productivity Services – to establish a national and standardised technology platform that complements the Public Contact vision from the Digital Policing Portfolio and delivers productivity benefits such as: collaborative production of documents, spreadsheets and presentations (amongst other examples); and the storage and management of these files, email and file-sharing. A key aim is to remove barriers to operational efficiency and to enable joint working, as well as digital engagement with the public.

These three national solutions are major programmes of work. They have received both top-down support from the NPCC, APCC and the Home Office, and bottom-up support from the policing technology leadership community in recognition of the need for technology to enable significant strategic changes in the working methods of the UK Police Force. This will remove existing obstacles to efficient information sharing and cross-force communication and will deliver more efficient and collaborative ways of working between Police Forces and their partners.

It should be noted that the NEP is not mandated to make UK Police Forces compliant with data privacy legislation. That said, this programme intends to provide robust security around all information in the system with privacy built in to both the assessment of risk and application of necessary and proportionate controls.

This will improve a Police Force's ability to mitigate privacy risks. The security framework which the NEP has used to identify risks can also be re-used by Forces to assess risks on other technology projects.

The programme will deliver the productivity tools detailed in Table 1 through the implementation of Microsoft cloud services deployed in a hybrid configuration in Police Forces.

Component(s)	Description
Exchange Online	Online or hybrid infrastructure and software for the delivery of Email, Calendar & Tasks to any enabled device or via a web client
Office 365 ProPlus	Latest version of tools including Word, Excel, PowerPoint, Publisher, Access to support core productivity tasks such as document creation, editing and sharing
Groups and Teams	Modern conversation experience for working groups that supports forces when teams need to collaborate. Also creates an Office 365 "membership" which carries across to other products in the Office 365 family
Skype for Business	Instant messaging, voice and video conferencing and screen sharing tool supporting both internal and external federated communication
SharePoint Online	Web portal for collaboration including document management, team sites, intranet hosting and workflow and smart form routing
OneDrive for Business	Cloud file storage accessible from any enabled device and fully integrated with the other 365 components
Yammer	Enterprise Social Networking to connect the individuals working within an organization based on shared communities of interest
Delve	Advanced search tooling which surfaces internal recommended shared content to a user from across Office 365
Intune	Mobile device management, mobile application management, and PC management capabilities from the cloud
Microsoft Flow	Cloud only, trigger based application for automating workflows between products within O365
Microsoft Planner	A planning application used for collaborating on tasks and actions between users

Microsoft Power Apps	A specific tool to allow users to build their own applications to exploit data stored within O365 products such as SharePoint

Table 1: Productivity Tools delivered by NEP

These productivity tools will be secured using the Microsoft security components and an Identity and Access Management solution (SailPoint IdentityNow) detailed in Table 2. Security controls designed specifically for the NEP solution will also be implemented as part of the delivery of the NEP solution. As part of the monitoring solution to be implemented in each force a more modern and proportionate approach will be implemented for the end user monitoring. This solution includes IBM tools also listed in the table below.

Component(s)	aka	Description
Privileged Identity Management	**PIM**	Stronger control of privileged roles, e.g. elevation of IT admin privileges only when required, on-demand.
Azure Identity Protection	**IdP**	Utilises data analysis from Azure AD to generate reports and alerts that can detect potential vulnerabilities, automate responses to suspicious events and support incident investigation
Identity Governance (SailPoint)	**-**	Identity provisioning, certification (including access reviews), access management (including roles and role management), reporting and governance
Exchange Online Protection	**EOP**	Email filtering service to protect against spam and malware, including features to safeguard the force from messaging-policy violations
Data Loss Prevention	**DLP**	Data Loss prevention policies applied to outbound mail from an Exchange Online hosted mailbox
Advanced Threat Protection	**ATP**	Cloud-based email filtering that helps protect against unknown malware and viruses by providing robust zero-day protection, and safeguards against harmful links in real-time
Azure Information Protection	**AIP**	Allows a force to classify, label, and protect its documents and emails. RMS enables rights management for content outside Office 365 (e.g. on premises file servers)
Cloud App Security	**CAS**	Security protection for cloud applications — both approved and unapproved — for deeper visibility, comprehensive controls and enhanced protection against cloud security issues
IBM Resilient	**-**	A tool to manage incidents related to any cyber vulnerability identified.
IBM QRadar	**-**	Tools used to collect event logs for centralised monitoring. The tool will be tuned to provide a necessary and proportionate approach to event collection.

Table 2: Security components delivered by NEP

"Security by Design" is a process which builds from the comprehensive Cyber Risk Assessment undertaken by NEP. The *"Security by Design"* process provides a mechanism to ensure that all identified risks have mitigation steps in place to reduce the risk to within risk management tolerances or to remove the risk in its entirety. *"Security by Design"* has been a key principle in the development of the NEP designs and the consideration of privacy has been an inherent part of the process. The deployment of the NEP solution across UK Police Forces will deliver significant productivity benefits to Police Forces whilst improving the overall Cyber Security maturity of a force. The development of the cyber risk management position of an organisation is assessed against the National Institute of Standards for Technology's (NIST's) Cybersecurity Framework, providing a baseline for a Police Force. A re-assessment is undertaken once the NEP has completed delivery where an overall improvement can be demonstrated from the integration of the Blueprint NEP Design set. The inclusion of the integrated security elements (including the NMC, IAM solution

and Security Model) will significantly improve the security of Police information and therefore the ability of UK Police Forces to protect the privacy of all of its stakeholders.

WHY A DPIA IS NECESSARY FOR THE NEP:

In February 2018 the NEP carried out a privacy impact assessment ("**PIA**") for the programme; some of the text in that PIA is replicated in this DPIA, updated as necessary to reflect (a) the passage of time since the PIA was completed and (b) changes in the way the NEP is being delivered. The PIA was carried out before the GDPR and the DPA 2018 came into force. When determining whether a PIA should be carried out the forces followed the then-current guidance in the ICO's Conducting Privacy Impact Assessments Code of Practice and it was determined that a PIA was required. That guidance was issued before the GDPR and DPA 2018 came into force.

Following the introduction of the GDPR and DPA 2018 and the guidance of both the ICO and the Article 29 Working Party, the following criteria have been considered in the context of the NEP.

Does the Project involve at least two of the following criteria?

1. Evaluation or scoring

   Yes - the NEP solution seeks to increase the ability to analyse and evaluate data across force boundaries, to enable easier facilitation of information sharing internally, and externally across forces and partners.

2. Automated-decision making with legal or similar effect

   Yes – Forces can choose from a catalogue of business change, utilising some if not all of the products included in the NEP Blueprint. Some of the scenarios will provide automation to decision making and processes that will influence an investigation or policing action. These actions could lead to legal outputs.

3. Systematic monitoring

Yes. **S31 Law Enforcement**

4. Sensitive data or data of a highly personal nature

Yes. The NEP solutions will process a significant amount of sensitive personal data and data relating to criminal activities and convictions. **S31 Law Enforcement**

5. Data processed on a large scale

   Yes. The NEP solutions will be used by police forces across the UK for a variety of purposes but primarily the management of unstructured data.

6. Matching or combining datasets

In the future, yes. Each Force will have its own tenant where they process their own data. **S31 Law Enforcement**

7. Data concerning vulnerable data subjects

   Yes. The system will hold information about children, victims and other vulnerable individuals. The products used to provide a solution will only hold unstructured data sets. It is not the intention for NEP to replace core policing systems functionality.

8. Innovative use or applying new technological or technological solutions

   Yes. The NEP is an innovative programme and solution. It will enable significant strategic changes in the working methods of UK police forces and will remove existing obstacles to efficient information sharing and cross-force communication, delivering more efficient and collaborative ways of working between Police Forces and their partners.

9. The processing in itself "prevents data subjects from exercising a right or using a service or a contract"

   No.

As more than one of the above criteria are met, a DPIA must be carried out.

The Information Commissioner's Office has published a list of ten types of processing that automatically require a DPIA. Does the Project involve any of the following types of processing?

1. Use of innovative technology

   Yes. The NEP is an innovative programme and solution. It will enable significant strategic changes in the working methods of UK police forces and will remove existing obstacles to efficient information sharing and cross-force communication, delivering more efficient and collaborative ways of working between Police Forces and their partners. The NEP programme has implemented and completed a full risk assessment of the known Police Assets against the latest threat assessment. This provided an inherent risk position to start a technical design process working to a principle of *"Security by Design"*.

2. Use of profiling or special category data to decide on access to services

   Yes. The Identity Access Management solution will profile the use of HR system roles that will provision access to services based on Role based Access controls. The NEP Blueprint design will deliver Joiner, Mover and Leaver processes which will provide the foundation for the access to systems and information.

3. Profiling of individuals on a large scale

   Yes – each force/other tenant will have a capability to identify what systems are being used to access information and data. The final phases of the NMC development will likely deliver the functionality

to undertake behavioural analysis. This is still to be scoped and determined as functionality to implement.

4. Processing of biometric data

   Yes - the designs will allow for users to sign on using biometric data (facial recognition). More traditional biometric data could also be shared within policing (finger prints etc) using the NEP solution.

5. Processing of genetic data

   Yes. The solution includes the Business Intelligence desktop capability which will allow a user to access genetic data sets for analysis. This functionality will require additional services outside the remit of NEP but some forces do have the capability.

6. Matching of data or combining of datasets from different sources

   In the future, yes. The NMC will have the capability to combine datasets to determine threats from Cyber Adversaries collectively for national policing.

7. Collection of personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')

   Yes – for example where data is collected as part of a police investigation.

8. Tracking of individuals' location or behaviour No

9. Profiling of children or targeting marketing or online services at them

   No. There is no use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making.

10. Processing data that might endanger the individual's physical health or safety in the event of a security breach

    Yes – for example if operational policing data relating to a live investigation is lost or stolen. However the controls put in place to mitigate risk as part of the *"Security by Design"* process mitigate the risk to an acceptable tolerance. The controls are collective and provide a defence in depth position to minimise and where possible prevent any data exfiltration.

As the NEP meets at least one of the ICO's types of processing that automatically require a DPIA, a DPIA is required.

Other factors which were considered as pertinent to the decision to undertake this DPIA are:

- The NEP solution will compel individuals to provide information about themselves, including police officers, staff and contractors. This is however limited to user login credentials only.
- Information about individuals may be disclosed to or processed by organisations or people who have not previously had routine access to the information – for example user credentials and information will be disclosed to the cloud service provider, which has not previously had routine access. Police information will be stored in the cloud service provider's infrastructure.
- Information about individuals is being used in a way it is not currently used. Information about employees' work will be monitored in all UK police forces. This may not currently be the case in all forces.
- The NEP involves using new technology and delivery methodology that means the privacy

implications need to be carefully considered – e.g. migrating systems to the cloud. Furthermore, new user monitoring technologies may be perceived as being privacy intrusive – many police forces do not currently have comprehensive user monitoring capabilities. It should be noted that the minimum set of monitoring points are included in the Blueprint. This totals 13 monitoring points as a minimal viable set of events. This should be balanced with the control it provides in mitigating Cyber Adversary risk and risks associated with this.

- Actions may be taken against employees as a result of monitoring their work activities, for example when major security and/or data breaches are identified. Such actions could potentially have a significant impact on those employees.
- The information being processed includes criminal records, data on children, data on disabilities and potentially health records. Victim and witness information may also be stored on this system.
- The NEP involves multiple organisations, including numerous law enforcement agencies and private sector suppliers.

It is recognised that the NEP gives rise to some significant data protection questions, particularly in the context of data security and migration to the cloud. Whilst not insurmountable, it is acknowledged that it is important to give due consideration to these questions at an early stage, and to keep them under review as the solution develops. The approach to design and risk management provides a robust advancement in the controls for data protection, with full governance in place to provide auditability of who is accessing data and information. Encryption is applied through policy providing safeguards in the event of malicious or nonmalicious data breaches.

Step 2: Describe the processing

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?

Enclosures B (1) (the NEP Update for Suppliers of Policing PowerPoint Presentation dated 19 November 2018), and B(2) (the NEP IAM and PS Low Level Design document), both embedded in Step 1 above, contain a detailed overview of the NEP solution, including technical architecture diagrams and supporting text to show how and where data will be collected, used and stored, and where the data originates from. We have not replicated the totality of Enclosures B(1) and B(2) here, due to their scale, but have copied two of the key slides below. For further details, please refer directly to Enclosures B(1) and B(2).

As described under the heading of "Identity of data controllers" below, this DPIA focuses on the privacy risks being presented by the deployment of the NEP solutions from a central perspective. The Blueprint design provides a solution which will be locally owned and operated by the host force. Each force has committed to deliver the solution to the Blueprint and therefore the data flows are provided in the detailed design Volume set. As the data which will be processed and stored originates from forces and other tenants at a local level, forces may wish to include a more detailed analysis of the end-to-end data flows from their specific, local perspective in Appendix A to this DPIA.

As the NEP provides a Blueprint design which is common to all forces/tenants, this DPIA has been completed once centrally, but will then be reviewed and validated by forces locally when they come to access and utilise the NEP solutions for the processing of personal data. Forces each have the opportunity to consider any additional, different or local privacy risks when reviewing this DPIA and completing their own validation checks. Again, to assist forces across the country, the NEP has sought to standardise the format for the DPIA, and has included at Appendix A space for individual forces to reflect on any additional or different local risks and mitigation strategies. Should any force believe that there are errors or omissions in the main body of this DPIA (i.e. all sections other than Appendix A), then these queries should be referred to the NEP, which will in any event keep this DPIA under regular review as the programme advances.

The data which will be processed via the NEP solutions originates from UK police forces. In general terms, NEP does not substantially change the nature or scope of the personal data which forces routinely collect or process, it simply provides an improved, consistent and more secure solution which forces can use to store and access personal data. With that said, once the National Monitoring Centre is established, security data sets ***will*** be combined in one location for the monitoring points included in the Blueprint. Each force tenant will also hold the logs as part of the Azure Advanced Threat Protection in line with the design configuration.

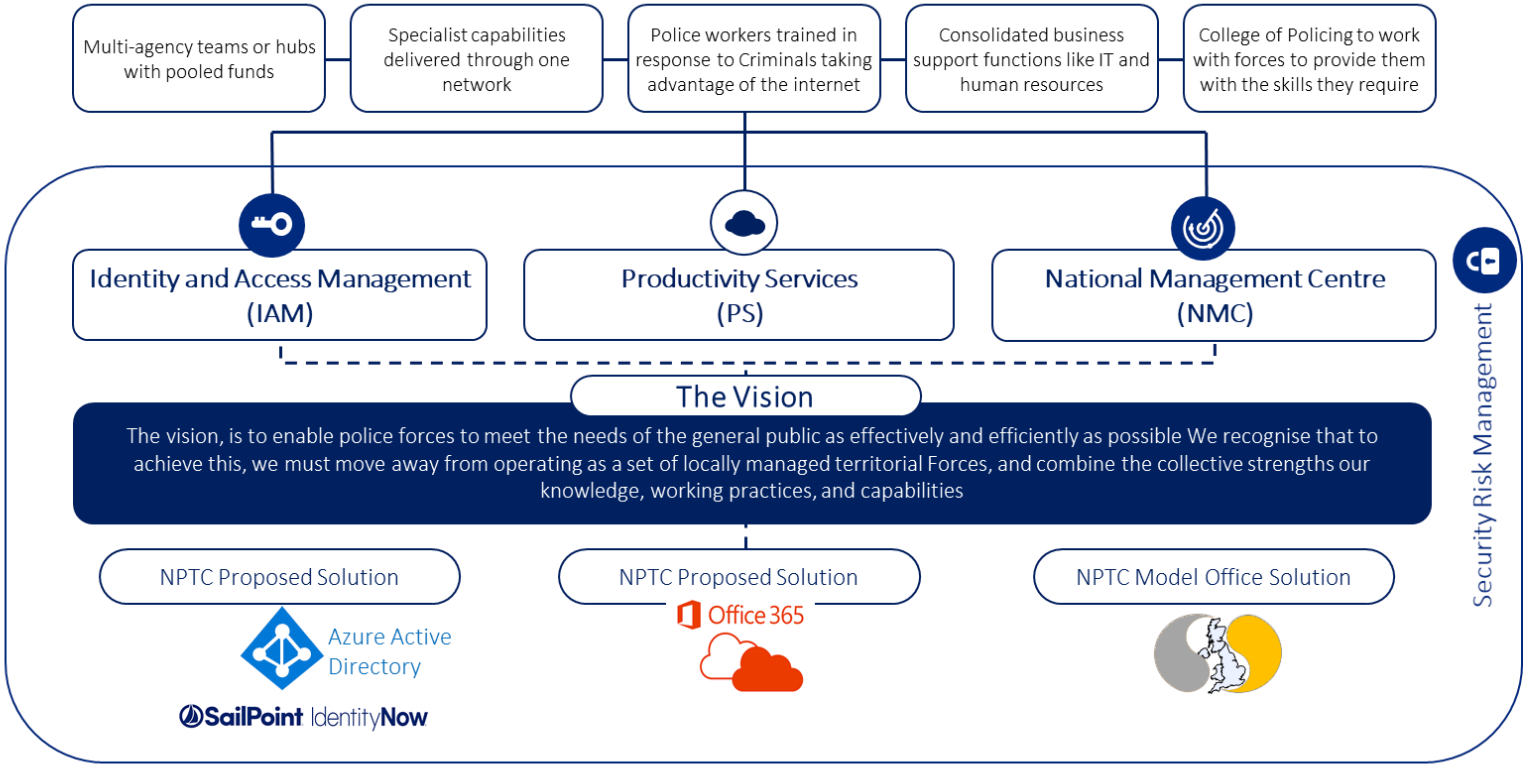
As the NEP solutions will entail the processing of policing datasets, this of course elevates the risk of the processing activities. In this case, the processing is not high risk because the risk has inherently changed, but because data is being processed in a new way and new people will have access to it – for example, there is likely to be replication of data in multiple locations as forces share certain data. The key mitigating factor for this risk centres on the introduction of IAM, meaning that data controllers will have control over who has access to what. These privacy risks are considered in more detail later in this DPIA.

NEP Solution

Microsoft technologies were chosen for the NEP, due to their potential to meet programme compliance needs. SailPoint IdentityNow will be used for identity governance.

Core Programme Principles:

1. Cloud is "good"
2. Police adoption of GSC
3. Common blueprint design



S31 Law Enforcement

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?

Identity of the data controllers

This DPIA focuses on the privacy risks being presented by the deployment of the NEP solutions from a central perspective. For the avoidance of doubt, the NEP is not itself a data controller. It has no separate legal personality, has no ability to enter into contracts, does not employ any individuals and – by its very nature – is intended to exist for a relatively short period of time, until the National Enabling Programmes have been delivered and passed into "business as usual" functions within UK policing. This DPIA has therefore been conducted by the Police ICT Company, which is intended in due course to take ownership of the output of the NEP.

Each police force will be its own data controller for the personal data which it collects and processes using the NEP solution. Each police force is therefore its own data controller for the purposes of its use of the NEP solution. This DPIA does not replace the specific risk assessments which each individual force must undertake when considering use of the NEP solution. Only those organisations themselves can assess their own specific data protection risks, based on their specific circumstances – Appendix A has been included in this DPIA to provide forces with space to augment the content of the main body of this DPIA with any specific risks identified at an individual force level. It is intended and expected that this DPIA will enable all forces to focus their attentions particularly on the issues which are local to them and their engagement with the NEP solution. The privacy risks from a central perspective are considered in the main body of this DPIA.

The types and categories of personal data

The types and categories of personal data processed by the NEP solution will depend on the content of the information inputted into the system by forces/tenants. The NEP solution could be used by data controllers (i.e. forces and other tenants) to process personal data including:

- Personal details (e.g. name, address, email address, telephone number, car registration number, national insurance number, passport, driving licences)
- System usage details
- Family, lifestyle and social circumstances
- Education and training details
- Employment details
- Online identifiers (e.g. internet protocol addresses, cookies identifiers)
- Financial details (e.g. bank account details)
- Criminal records, offences (including alleged offences) and criminal proceedings, outcomes and sentences
- Legal proceedings
- Data on children
- Special categories of personal data, including data on disabilities, health records, religious or philosophical beliefs, trade union membership
- Victim and witness information

It is important to stress that the above list is not exhaustive, and that by the nature of the NEP solution and the scope of the IT systems with which it interfaces, the categories of personal data which may be processed via the NEP solution is very wide.

Collection and recipients of personal data

The NEP solution will process and store vast quantities of data – it will be used by police forces across the UK for storing personal data. It is likely that the number of individuals whose personal data will be stored and/or processed using the NEP solution exceeds 1,000,000.

How information stored on the NEP is requested will depend on the particular information. Information may be requested in different ways, under different statutory powers, and for different purposes. Certain information will be voluntarily provided to Police Forces by the public (e.g. when individuals make firearms applications).

The power to request information comes in the main from the Police Acts and other pieces of legislation which enable police officers or police staff to carry out their duties, e.g. Police and Criminal Evidence Act 1984 (PACE), Criminal Procedure and Investigations Act 1996 (CPIA), etc. together with common law powers. The Police Act 1996, section 30(1) gives police force members all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the chief officer can delegate certain powers to police staff. This ensures a consistent approach by the police forces in their legitimate data gathering objectives.

The collection of data is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. The College of Policing has published the Information Management Authorised Professional Practice[2] (APP) to assist forces with their data collection and recording responsibilities.

How is information stored?

As can be seen in the Design Architecture diagram above, the NEP will store information using a hybrid cloud solution. Certain information will continue to be stored locally by forces on their existing IT infrastructure, whilst other unstructured information (e.g. emails, files etc) will be stored in the cloud.

Numerous security features are present at each level of the network topography; these are outlined in more detail in Enclosure B. Furthermore, on 20 March 2017 Commissioner Dyson, the National SIRO for Policing, chaired a meeting with stakeholders from across policing to determine the National Policing Information Risk Appetite in respect of the Police use of Microsoft Office 365 and Azure Active directory.
Nineteen national risks were considered along with the mitigations (if any) available to reduce those risks. The document included at Enclosure C (Office 365 for Policing – National SIRO Risk Decisions) sets out the summary risks and the steps required to mitigate them, reflecting the decisions made during the meeting.

Use of personal data

Information stored on the NEP solution will be used in a variety of ways, including policing and safeguarding

[2] https://www.app.college.police.uk/app-content/information-management/management-of-policeinformation/collection-and-recording/

purposes (for example, where information being processed relates to a criminal investigation). The way in which the information is used will depend on the nature of the data and the purpose for which it was collected.

(a) Information used for a policing purpose:

The Code of Practice on the Management of Police Information[3] ("**MOPI**") sets out at 2.2.2 that the police purposes are defined as: protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law. Any such information used for a policing purpose will be processed in accordance with the DPA 2018.

(b) Information used for a non-policing purpose:

Information used for any purpose other than a policing purpose (see point (a) above) will be deemed to be used for a non-policing purpose. This includes, without limitation, processing of employee data by employer data controllers. Any information used for a non-policing purpose will be processed in accordance with the GDPR and the DPA 2018 and under the relevant statutory powers relating to that particular information and the purpose for which it is being processed. Personal data will be processed in compliance with the relevant conditions set out at Article 6 and 9 (if appropriate) of the GDPR and in Schedule 1 (as appropriate) of the DPA 2018.

How is information reviewed, retained and deleted?

The Controller (i.e. the individual police force) for a particular piece of data will be responsible for reviewing, retaining and deleting that information in accordance with its own internal code of practice, the GDPR and DPA 2018. The NEP solution will allow the relevant Controller to manage its data in this way with a baseline configuration provided as part of the Blueprint implementation.

The retention periods and principles set out in the MOPI guidelines (see in particular 4.5 – 4.6 of the Code of Practice on the Management of Police Information[4]) will apply to data stored on the NEP solution. A base configuration is provided that can be extended to meet the needs of MOPI and other legislation. If these guidelines and legislative requirements change then the base configuration will also need to change.

Who determines how and why the personal data is processed?

Each Controller (i.e. the individual police force) determines how and why the personal data is processed.

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)?

[3] http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf
[4] http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

Relationship with individuals

The personal data which will be processed using the NEP solution includes data relating to police officers, employees, contractors and suppliers. It also includes information relating to live policing matters. By way of example only, information which is contained within emails which are stored in the Azure cloud hosting environment, and information relating to service requests (e.g. when individuals apply for firearms licences or make an individual rights request under the GDPR) will be processed utilising the NEP solution.

The relationship with individuals therefore varies depending on the processing in question. In some cases, the relationship will be one of employer to employee, in others it is customer to supplier and in others (i.e. live policing matters) it will be Police force to victim, witness, suspect or convicted criminal in relation to offences or suspected offences.

NEP solution technology

The use of cloud technology in and of itself is far from novel. Cloud is used for data processing activities by many organisations across a range of sectors in the UK and globally. It is also used specifically in a number of instances by UK policing. For example, Microsoft's Azure platform is used by a number of police forces to host a "Public Engagement" solution, which enables members of the public to engage directly with the police when reporting incidents or intelligence.

The NEP solution is intended to take advantage of the enhanced security features which modern technology working practices can provide. The National SIRO Risk Decisions document included at Enclosure C sets out some of the risks and mitigation strategies which have been considered in the context of making greater use of certain cloud technologies within the NEP solution. Fundamentally, however, it is entirely expected that the NEP solution will improve security and reduce the risk of security flaws.

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?

The purposes and benefits of the processing are described in Step 1 above, and in more detail in the NEP Update for Suppliers of Policing PowerPoint Presentation dated 19 November 2018 at Enclosure B.

Step 3: 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?

This DPIA is being completed centrally, from the perspective of the NEP as the delivery vehicle for the various technology solutions which the NEP entails. As the data controllers for the personal data which will be input to the NEP solution are police forces nationally, the NEP (and the Police ICT Company) has engaged with force representatives to ascertain their views and ensure that, wherever possible, their concerns are also reflected in this DPIA. Furthermore, forces also have the opportunity to review, validate and augment this DPIA by populating Appendix A, having considered the privacy risks in more detail from a force perspective.

In producing this DPIA, input has been sought (and provided) by various stakeholders within NEP, the Police ICT Company and externally, including:

- NEP Commercial Lead
- NEP Programme Director
- NEP CTO
- NEP Technical Lead
- Police ICT Company CEO
- Police ICT Company DPO
- Local force DPO and technical/implementation representatives, including the two pilot forces (Kent and Essex) and Sussex

Furthermore, we have also consulted two key data processors within the NEP ecosystem, BT and Deloitte, to seek their assistance in completing this DPIA. Both suppliers provided their feedback following a review of draft v0.2 of this DPIA. Their comments were then reviewed by the NEP and Police ICT Company, and the document was further updated to take account of the feedback received.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? 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?

Lawful basis for processing

The lawful bases for processing information via the NEP solutions are in fact no different to the lawful bases for the processing which forces currently undertake. These lawful bases vary depending on the processing activity in question. For example, in the case of processing employee data, this processing is necessary for the performance of a contract, for compliance with a legal obligation and/or for the controller's legitimate interests. In the case of processing personal data to consider and (if appropriate) approve an individual's firearms application, the processing will be necessary for compliance with a legal obligation to which the controller is subject.

Compliance by processors

The two key data processors in the NEP solution ecosystem are BT and Deloitte. Each of these was appointed following a competitive procurement process and each has in place a robust contract which includes clauses addressing the requirements of the GDPR and DPA 2018 (in particular, ensuring compliance with Article 28 of the GDPR). The clauses included in both contracts are based on and substantially similar to the Crown Commercial Service's standard data protection clauses[5].

International data transfers

International data transfers are controlled by way of contracts with all data processors. By way of example, in the BT and Deloitte contracts, the suppliers (acting as data processors) are prohibited from transferring personal data outside of the EU unless the prior written consent of the Authority has been obtained and certain other conditions are fulfilled. It is not intended that any processing of personal data outside the EU will occur through use of the functionality being provided as part of the NEP solution.

Step 5: 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**
Lawful, fair and transparent – there is an increased risk of unlawful access due to increased data availability across multiple forces	Possible	Significant	Low
Purpose limitation – there is an increased risk of data being used for an additional purpose	Possible	Significant	Low
Accuracy – an increased risk of inaccuracy due to duplication, combination and increased access and ability to share data	Possible	Significant	Medium

[5] Available here: https://www.gov.uk/government/publications/procurement-policy-note-0218-changes-to-dataprotection-legislation-general-data-protection-regulation

Storage limitation - an increased risk due to duplication and sharing (different data retention schedules applied depending on the data type and data controller)	Probable	Significant	Medium
Integrity and confidentiality – there is still risk to the integrity and confidentiality of data. The 31 police information assets and associated inherent risks in those assets become the risk of the NEP. This also applies to the email system	Remote	Significant	Low
Consent – there is a risk that the management of consent (capture and removal) is not fully supported within the NEP solution	Possible	Significant	Low
Right to information – there is an increased risk of lack of transparent processing as the individual data controllers do not correctly adapt their privacy policies to address the additional processing undertaken within the NEP	Possible	Minimum	Low
Access – there is an increased risk that sharing and the combination of data leads to the creation of additional personal data that is not then easily collected and collated by the original data controller in order to fulfil a DSAR or information rights request	Probable	Significant	Low
Rectification – there is an increased risk that sharing and combination of data leads to the creation of additional personal data that is not then easily corrected	Probable	Significant	Medium
Erasure – there is an increased risk that sharing and combination of data leads to the creation of additional personal data that is then not easily deleted	Probable	Significant	Low
Restriction of processing – there is an increased risk that restriction of data processing in one force is not then adhered to by another	Remote	Significant	Low
Profiling – there is an increased risk of unlawful profiling as more people will now have access to the data	Remote	Significant	Low

Step 6: Identify measures to reduce risk

Risk	Option to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Lawful, fair and transparent – there is an increased risk of unlawful access due to increased data availability across multiple forces	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk.	Reduced to an acceptable level	Residual risk lower than prior to NEP solution roll out	
Purpose limitation – there is an increased risk of data being used for an additional purpose	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk.	Reduced to an acceptable level	Residual risk lower than prior to NEP solution roll out	
Accuracy – an increased risk of inaccuracy due to duplication, combination and increased access and ability to share data	Mitigated by staff training and strict access controls. Individual data controllers will have the ability to control with which organisations they share data	Reduced to an acceptable level	Data accuracy is a perennial risk, but the residual risk here is no higher than prior to NEP solution roll out	
Storage limitation - an increased risk due to duplication and sharing (different data retention schedules applied depending on the data type and data controller)	Mitigated by staff training and strict access controls. Individual data controllers will have the ability to control with which organisations they share data	Reduced to an acceptable level	Residual risk no higher than prior to NEP solution roll out	

Integrity and confidentiality – there is still risk to the integrity and confidentiality of data. The 31 police information assets and associated inherent risks in those assets become the risk of the NEP. This also applies to the email system	Mitigated by the Security Risk Management (SRM) process used during the NEP development	Reduced to an acceptable level	Residual risk lower than prior to NEP solution roll out	

Consent – there is a risk that the management of consent (capture and removal) is not fully supported within the NEP solution	Mitigated by staff training and ability for forces to continue to operate consent management functionality which they currently utilise. Risk is also mitigated by the fact that consent is not the prevailing lawful basis relied upon for processing of personal data via NEP	Reduced to an acceptable level	Residual risk no higher than prior to NEP solution roll out	
Right to information – there is an increased risk of lack of transparent processing as the individual data controllers do not correctly adapt their privacy policies to address the additional processing undertaken within the NEP	Mitigated by ensuring the data sharing and processing agreements (articles 26 & 28) include a requirement for the forces to update their Privacy Notices appropriately	Reduced to an acceptable level	Reduced to an acceptable level	

Access – there is an increased risk that sharing and the combination of data leads to the creation of additional personal data that is not then easily collected and collated by the original data controller in order to fulfil a DSAR or information rights request	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk. Also mitigated by the terms of data processing and sharing agreements.	Reduced to an acceptable level	Reduced to an acceptable level	
Rectification – there is an increased risk that sharing and combination of data leads to the creation of additional personal data that is not then easily corrected	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk. Also mitigated by the terms of data processing and sharing agreements.	Reduced to an acceptable level	Reduced to an acceptable level	
Erasure – there is an increased risk that sharing and combination of data leads to the creation of additional personal data that is then not easily deleted	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk. Also mitigated by the terms of data processing and sharing agreements.	Reduced to an acceptable level	Reduced to an acceptable level	
Restriction of processing – there is an increased risk that restriction of data processing in one force is not then adhered to by another	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk. Also mitigated by the terms of data processing and sharing agreements.	Reduced to an acceptable level	Reduced to an acceptable level	

Profiling – there is an increased risk of unlawful profiling as more people will now have access to the data	Mitigated by staff training and strict access controls. IAM implementation across the NEP reduces the risk. Also mitigated by the terms of data processing and sharing agreements.	Reduced to an acceptable level	Residual risk lower than prior to NEP solution roll out	

Step 7: 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:

I have considered the details set out in this DPIA and the accompanying documents and conclude that the risks associated with the processing activities described in this DPIA have been considered and understood, and that appropriate privacy solutions and risk management strategies have been deployed to manage the risks which do exist. Subject to the recommended actions/next steps set out below, I am satisfied, from my Police ICT Company DPO perspective, that:

- the safeguards being deployed to protect against the risks to the rights and freedoms of data subjects described in this DPIA are proportionate and appropriate; and
- there are no residual high risks to the rights and freedoms of natural persons, and so no need to consult the ICO pursuant to Article 36 GDPR.

Please note that this advice is provided to the Police ICT Company and National Enabling Programmes only. Whilst this document will be shared with forces, each force is required to consider the privacy impact, risks and mitigations for its own account. It is not expected that there will be great variances from one force to the next, as the NEP solutions are common to all, the technical design is consistent for all and the risk mitigation strategies are also consistent for all. Nonetheless, should forces feel that any local risks have not been adequately covered in this DPIA, they are advised to address these in Appendix A. Any queries should be raised with the NEP in the first instance.

Recommended actions/next steps

1. As forces and other tenants are transitioned into using the NEP solution in a live environment, they (acting as data controllers) will need to undertake their own impact assessments (in this case by way of populating Appendix A of this DPIA, which streamlines the documentation and makes it more coherent and consistent. It also avoids forces having to repeat large sections of the front end of this DPIA). This is acknowledged in a number of places, but for the avoidance of any doubt I would advise that Appendix A to this DPIA is completed by each data controller/force prior to them using the NEP solution for the processing of personal data.

    - **Suggested action: commence work to complete Appendix A to this DPIA, with NEP to complete a draft template which forces can then review, validate, adapt and amend as appropriate prior to them utilising the NEP solution. Whilst this should be concluded as soon as possible, as a number of stakeholders will need to be engaged and this is not a straight-forward process, an absolute deadline for completing the draft template Appendix A should be by the end of April 2019.**

2. One risk of particular concern (albeit one which is capable of mitigation) is the potential lack of transparency for data subjects about how the NEP solution will process personal data, how staff activities are being monitored and so on. The privacy solution being deployed to address this risk is to ensure that forces update their privacy notices as appropriate. However, this in turn presents a further risk – i.e. that individual forces adopt different approaches to amending their privacy notices, provide differing levels of detail and so on, introducing in effect a “postcode lottery” as to the level of transparent information provided to data subjects about the processing of their data. I would therefore advise that the NEP works collaboratively with the Police ICT Company and force representatives (e.g. Kent and Essex as the pilot forces) to create a template update to privacy notices for sharing with all forces. Not only will this mitigate the privacy risks which have been identified, it will also reduce duplication of effort and so reduce costs (noting, nonetheless, that individual forces will still be responsible for ensuring that the privacy notice updates accurately and comprehensively address their local processing activities). Furthermore, this DPIA could be published (whether internally within forces/tenants and/or nationally on the relevant website(s)),

which would have the effect of further managing and reducing these risks. If this DPIA is to be published, then this point should be added to Step Six of the DPIA as a further privacy/risk management solution.

- **Suggested action: NEP and Police ICT Company to consider whether or not to publish the DPIA and work together with force representatives (e.g. Kent and Essex as the pilot forces) to create a template update to privacy notices for sharing with all forces. I would suggest that this position is considered, and a decision reached, by the end of April 2019. Any template updates to privacy notices, and any publication of this DPIA, should be completed by no later than 30 June 2019.**

3. Given the very dynamic nature of the NEP solution and the pace of digital change within policing at present, I would advise that this DPIA is kept under regular review.

    - **Suggested action: NEP and Police ICT Company to keep this DPIA under regular review. The first such review should be completed by no later than 30 September 2019 or, if sooner, the time of the next NEP design refresh.**

4. Whilst I am satisfied that there are no residual high risks to the rights and freedoms of natural persons, and so no need to consult the ICO pursuant to Article 36 GDPR, I would nonetheless advise that the ICO is engaged and asked to review this DPIA on a voluntary basis. Any queries or comments from the ICO should be reflected (as required) in a revised iteration of the DPIA.

    - **Suggested action: draft DPIA to be shared with ICO by no later than 30 April 2019, inviting the ICO's comments and review.**

DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments: N/A – feedback from those parties who were approached has been fed into the body of this DPIA.		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX A: FORCE-SPECIFIC CONSIDERATIONS AND IMPACT ASSESSMENTS

1. Details of any additional information regarding the processing activities
   [Drafting note: forces may wish to consider including their own data flow diagrams here, in particular. If there is nothing to add, please mark "N/A"].
   -

2. Details of any additional consultation activities by the force
   - [Drafting note: if none, please mark "N/A"].

3. Details of any additional risks from a local force perspective
   [Drafting note: please add any additional risks to the table below. If none, please delete table and mark "N/A"].
   -

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

4. Details of any additional risk mitigations from a local force perspective
   [Drafting note: please add any additional risks to the table below. If none, please delete table and mark "N/A"].
   -

Risk	Option to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved

5. Details of any additional DPO advice
   - [Drafting note: if none, please mark "N/A"].