Data Protection Impact Assessment Report

Project Information	
Project Name (and or number)	Business Intelligence Tool (Qlik Sense)
Business Area/s Affected	Improvement & Change
Information Asset Owner	Head of Improvement & Change
Senior Responsible Officer	[redacted]
Project Manager	[redacted]
Data Protection Officer	[redacted]

Document Ownership	
Author(s)	[redacted]
Document Owner	[redacted] – Data Protection Officer (DPO)

Document Review Information			
Document Location			
Quality Reviewers	**Name**	**Role**	**Sections Reviewed**
	[redacted]	ISO	Whole document
	[redacted]	RM	Whole document
	[redacted]	DPO	Whole document
Version History	**Version Date**	**Requestor of Change**	**Summary of Change(s)**
0.1			Initial Draft
1.0	09/10/2019		Signed off by DPO
1.3	28/01/2020		Audit capacity; workstream owners; user categories; appendix A (commissioning/publication process); ACL records (CCU); roles descriptions and vetting levels; Cat C intel
1.4	30/01/2020	[redacted]	Review and approval by ISO, RM and DPO
1.5	04/04/2022	[redacted]	All links updated; All sections updated to reflect change in practice; commissioning and publication processes & governance to be updated;

			IAO and data type appendix to be updated/moved externally?
1.6	24/05/2022	[redacted]	Review and approval by DPO
1.7	24/05/2022	[redacted]	Review and approval by IAO

Distribution List		
Name	**Department/Organisation**	**Project Role**

Introduction

The **Data Protection Impact Assessment (DPIA)** process is not only a legal requirement, as explained in Appendix B, it is also an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective considerations where solutions can be more costly or delay implementation. A DPIA, can also identify whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way Wiltshire police use individual's personal data. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour, and their personal communications.

When carried out early the DPIA process can provide the following benefits:

- meet legal requirements
- avoid loss of trust and reputation
- identity management and privacy principles
- avoid disproportionate or unnecessary use of personal data
- avoid unnecessary costs
- avoid inadequate solutions
- support a communications strategy.

Who is responsible for carrying out a DPIA?

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Information Asset Owner (IAO) for a project and is produced as part of the project proposal; however, this activity can be delegated to an appropriate person such as the Project Manager/Lead. When a new project/initiative involving the processing of personal information is being considered the IAO or Project Manager will contact the DPO to arrange a meeting with relevant parties to discuss the proposal. At this stage it may be identified that it is necessary to undertake an information security assessment.

The DPIA will require authorisation by:

- Information Asset Owner and Senior Responsible Officer
- Data Protection Officer
- Senior Information Risk Officer – where the DPIA has identified 'high' residual risks and referral to the Information Commissioner is required.

Data Protection Impact Assessment Report

1. Outline of the project, objectives and benefits

The project will deliver a corporate rollout of a Business Intelligence tool to improve the ability to display and analyse business intelligence for the purposes of improving service delivery to the Public.

Objectives

- To provide real time access for all staff to enable them to have the right information available to them to make the right decision at the right time
- To embed advanced analytics to support the identification of risk and to better direct resources before risk becomes a reality
- To deliver efficiencies and savings across the Constabulary in how information is managed, reported, and analysed

2. Describe the intended use of personal data:

a) Describe the nature of the processing:

Information Governance

- There are several flow charts describing the Information Governance attached in Annex A; these cover the following processes:
  - Commissioning new work: Requestors will fill out a SharePoint form describing their requirements; IAOs will gatekeep the request and escalate any information governance issues where required; updates will be recorded in the SharePoint list (with the request form data) and, if approved will move the request into the development backlog; changes which are not deemed significant (compared to the original request) may not need IAO approval to sign-off.
  - Developing new work: Developers will work with the customer(s) and IAOs to either produce iterative (where testers are risk assessed and approved by IAOs), or IAO-approved products; IAOs have governance over use of testers, app content and audiences; Information governance is managed through the Qlik Sense IAO who can escalate risks where required.
  - New data connections: Where a request requires a new connection to a Force data source, the IAO(s) for that source will be consulted and a ticket raised with ICT only when their written approval is given; IAOs may wish to place limitations on Developers; these will be recorded in both the project brief (that initiated the need for a new connection) and against information held against that data source by the Developers.
  - Data validation reviews: Developers will use triggers to determine whether a data validation review is required; where a review identifies errors, these will be discussed with the relevant IAOs, and they will determine whether to unpublish or caveat the app(s) in question while remedial work takes place (a new commission); Developers will be responsible for reporting potential data inaccuracies that may trigger a data validation review; Trigger events include:
    - Changes to the data source (that may affect one/more apps)

- Where definitions/methodologies changes
- On request from IAO (Qlik Sense or source system), DPO, or any other Information Governance authority

Data Sources

- Data is extracted from various sources as defined below:
  - Flat files (e.g. Excel workbooks, .csv/.txt files etc.) stored directly (not SharePoint) on Wiltshire Police servers. Files can only be accessed where the Qlik Sense account [redacted] has been granted access by ICT. The only files currently accessed in this fashion are those owned by Improvement & Change for the purposes of using with Qlik Sense, these are stored on the following Wiltshire Servers: [redacted] and [redacted]
  - Flat Files and Lists stored within Wiltshire Police SharePoint. Files and lists can only be accessed where the Qlik Sense account has been granted access by the SharePoint Administrator of the site where the data is stored.
  - Existing Wiltshire Police databases via Open Data Base Connectivity / Object Linking and Embedding, Database (ODBC/OLEDB) and stored in Qlik Sense. ODBC / OLEDB provide direct access to all tables and fields within these source systems. Databases can only be accessed by Qlik Sense once a connection has been approved by the IAO and ICT, and then created by ICT. Once this connection has been approved, Qlik Sense will have 'read all' access to the data contained within that data source. Data will be stored within Qlik Sense files, which are be hosted on Wiltshire Police servers.

Licencing

- Data will not be accessible outside of the Wiltshire Police network and requires a [Qlik Sense] Professional or User licence to use; all users of the Wiltshire Police network can automatically acquire a licence if they are a member of the "_All Police Staff" or "_All Police Officers" AD Groups:
  - 30 Professional Licences are available for use by the Force; these licences are granted by adding users to the following AD Groups [redacted] and [redacted]. These licences enable users to:
    - Access the Qlik Sense Hub (where all user-facing apps are accessed)
    - Create and edit personal Sheets within published apps.
  - [Qlik Sense] Developers are granted further access, via membership of the [redacted] or [redacted] AG Groups (these users will be referenced as "Developers" where applicable in this document). This enables these users to:
    - Edit and publish apps.
    - Access the Qlik Management Console (QMC; where tasks and security are managed).
    - Access the Wiltshire Police Servers [redacted] and [redacted] where I&C (Improvement & Change) flat files are stored along with all data extracted and transformed from Force data sources.
    - Directly access all data within Force data sources Qlik Sense has a

connection to.

- Professional Licences are allocated to all members of the Developer, Business Intelligence Teams, and Qlik Sense administrators in ICT, and may be granted to authorised users, if deemed appropriate, by the Information Asset Owner.
- 1970 Qlik Sense Standard licences are available for anyone with access to the Wiltshire Police network and is a member of either the "_All Police Staff" or "_All Police Officers" AD Groups. These licenses are automatically allocated by Qlik Sense following the user attempting to access Qlik Sense.
- By default, Standard License users are only able to view Qlik Sense data that has been published by the Developer and where the data has not been further restricted.
- Standard License users may be granted access to more sensitive or restricted data by any one of the following means:
    - Via ICT adding them to the relevant AD Groups after receiving authorisation from the Information Asset owners of Qlik Sense and the original data source.
    - Via the QMC, for the purposes of supporting and validating development of applications within Qlik Sense, by Developers. This access will only be temporary and should not be used for any other purpose. These users will be authorised by the Information Asset owners of Qlik Sense and the original data source.
    - Utilising "Section Access," Qlik Sense Developers can create apps with additional security features, limiting only named users to access part, or all, of the data within an app. These apps will use either named access, or role/team/department-based groups as defined by the most recent data extract from the Force's ERP (Enterprise Resource Planning) database. Rules for which groups can access which data will be authorised by the Information Asset owners of Qlik Sense and the original data source.

System Security

- The system security will be subject to the same security afforded to the Wiltshire Police Network. Access to Qlik Sense will be subject to role-based permissions via the application of individual licences being applied to workstreams of applications and by assigning permissions to AD Groups. Stream owners will have access to app(s) which will detail the AD Groups and their members who have access to their streams as well as how recently each user has accessed each/any app. The Developers will manage the distribution of business relevant information, restricting access to certain data sets authorised users only.

Data restrictions and limitations

- Where required, Developers will cleanse the data as it is loaded into Qlik Sense and present it to users via self-service apps. This cleansing will take one or more of the following means at either the behest of the original IAO(s), or the Developer themselves (as part of ensuring apps only contain the data they require to meet the agreed needs of the user):
    - Exclusion of specific data fields (default for all Standard Licence Users)
    - Anonymisation of data (default for Category C Intelligence)

    - Exclusion of entire records (default for all Standard Licence Users)
    - Exclusion of all associated records (default for all Standard Licence Users)

- Qlik Sense users will have read-only access to their own personal data relating to their role/duties via Qlik Sense apps created by Developers. Unless authorised, users will only be able to see their own information, and the information of the people below them in their line management chain, as defined by the most recent data extract from the Force's ERP database.

- Category C Intelligence (Lawful sharing permitted with conditions) will have the Summary box anonymised but *may* be made available to Intelligence staff (or other approved users) only after consultation with the relevant IAOs.
- The data stored in Qlik Sense will be moment in time data collected from other databases and flat files unless otherwise authorised by the Information Asset owners of Qlik Sense and the original data source. External, or publicly held data will be the most recently available version of such data.
- For data available to Standard License users, data retention will be rolling 6 years from the start of the current month, or in line with the source data base from which the data is extracted from, whichever is shortest (any records deleted from the source system will be deleted from the Qlik Sense files/applications).
- Developers and other designated Professional License users (currently Business Intelligence Support Officers only) will have access to any data stored in the source systems (including restricted and sensitive) via Qlik Sense apps for the purposes of Statutory Reporting and Freedom of Information requests only. These apps will use Section Access to limit users to only those named by the Qlik Sense IAO as being approved. The apps containing this data will be accessible through a combination of restricted Streams and/or Section Access security permission applied either for named users, or users holding named roles (as per the most recent data download from the Force's Establishment database).
- To maintain compliance with the Force Records Retention Schedule, data files (.qvd) and applications (.qvf) which have been inactive for 6 months will get archived, then reviewed and deleted by the Developers after a further 6 months (12 months total), unless it is confirmed the data will legitimately be required later. Where uncertainty remains, applications may be saved empty of data but with the script intact so it can be reloaded with fresh data.

Data Processing

The nature of the processing is what you plan to do with the personal data.

- Data will be collected from: any/all Force databases (to include law enforcement data) and spreadsheets; public websites (e.g. ONS); external "big" data sources (e.g. demographic, geographic, financial, environmental)
- Data will be stored within Qlik Sense applications (.qvf) and data files (.qvd)
- Data will be stored on Wiltshire Police servers
- Up to 2,000 users will have access to the data with four categories of user based on their AD Group membership:
    - ICT – full access to all data, in line with their role as system administrators. Vetted to MV or NPPV 3
    - Developers – full access to source systems/data and read/write capability to Qlik Sense applications Vetted to MV (Police) or NPPV 3

    - Professional Licence Users – up to full read-only access to data in Qlik Sense applications (SC & MV clearance required). Vetted to MV (Police) or NPPV 3
    - Standard Licence Users – read-only access to Qlik Sense applications; access to data only as provided by Developers and only to applications according to their role(s)/AD Group access on a Stream-by-Stream basis, as authorised by the Information Asset owners of Qlik Sense and the original data source. Vetted to minimum of RV or NPPV 2.
- Personal data is shared with the Home Office and NPCC (National Police Chief's Council) for persons involved with crimes in line with current practices, for example, daily hate crime requests which provide name, ethnicity, and date of birth for all victims, suspects, and offenders.
- There are intentions to share data with partners outside Wiltshire Police. Data will only be shared where appropriate information governance is in place. An example of potential data sharing is: "High Frequency Contacts," where data is shared by local councils, housing associations, Criminal Justice, and National Probation Service partners, to identify people who create high demand across multiple agencies and would benefit intervention to reduce their demand.
- General access to Qlik Sense applications is controlled by ICT via membership of AD groups. Published applications are grouped into "Streams" where each stream can be restricted only to users who are members of relevant, role-based AD groups, or by name.
- Wiltshire Police have been using Qlik View since 2012. Qlik Sense is the replacement product which has the same capability as Qlik View plus mapping capabilities.

b) Describe the scope of the processing

- Personal data may come from a variety of sources and would be both staff data and members of the public data, to include both special category and data processed for a law enforcement purpose.
- Any/all data that Wiltshire Police hold on any system could be part of the Qlik Sense database and used to provide business intelligence.
- Published applications containing personal (law enforcement) data will only include data up to six years old unless used for statutory or FOI reporting. Requests for applications containing older data will require approval from the Force's Data Protection Officer and all applicable Information Asset Owners.
- Applications will include:
    - Record-level details of law enforcement data, including personal data of all named persons (including children) where already held on a Wiltshire Police database
    - Record-level establishment data (staff, officers, volunteers, contractors, external resources) where already held on a Wiltshire Police database
- The extent of the processing would be based on user requirements, but every area of the business could benefit from bespoke self-service application data. Examples include:
    - Using data collected from telephony, Record Management and Incident Control databases, call handlers could access any/all the following (including sensitive data but excluding access-controlled data):

        - history of calls from the current [telephone] number
        - users of the current number
        - previous crimes and incidents involving the current number/caller/address/previous users
        - officers dealing with previous calls
    - Users will be able to see any of the following information about themselves, and of the people below them in their line management chain, as defined by the most recent data extract from the Force's ERP database:
        - Sickness history
        - Training history (and current/expired skills)
        - Posting history
        - Current task workload
        - PDR (Professional Development Review) history
        - Development plans
        - Status of current investigations
        - Stop & Search, arrest, scene attendance volumes
        - Complaints
    - Users could access personal data of members of the public (excluding access-controlled records) living/operating within their geographical area (where data is currently already held on a Force system, including:
        - Involvement in Crimes and Incidents, past and current
        - Contact information (addresses and telephone numbers)
        - Vehicles used
        - Risk of causing/being at harm, based on algorithms designed by analysts and following the ALGO-CARE (link1, link2) framework for use of algorithms in Policing (as adopted by the NPCC).
        - Whether they are an outstanding suspect
- Data subjects would be anyone who has had any involvement with Wiltshire Police and their data is recorded on any Wiltshire Police data base.
- This system could interrogate all data held on any Wiltshire Police data base to include special category and law enforcement data.
- By default, data will be collected from the source databases at least daily, overwriting all existing data held within Qlik Sense.
- Qlik Sense may store more data than is presently stored in the original data source, only when authorised by the Information Asset owners of Qlik Sense and the original data source.
- There are some applications which are used to provide look up of legacy data and are the only way that this data is available. Specific differences with most of the analytics based QlikSense apps, is that these will refer to and hold data more than 6 years old. These include:
    - Force Data Search (replaces ColdFusion based application):
        - References data from Niche and Storm. Where access to specific data is controlled by ACL (Access Control List), this security is replaced in this app.
        - The implementation matches that of the original Force Data Search (FDS) application it replaces.

    Audit of specific queries on nominals and cases are also recorded as per the original FDS application it replaces. iPerform (replaces C#/asp application; historic establishment data). Origin (historic establishment data)

c) Describe the context of the processing:

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact:

- The source of the data is from:
  - Wiltshire Police systems (databases and flat files)
  - Partner agencies (e.g. Criminal Justice and Probation services)
  - Provided by, or collected from, staff/members or the public for HR/Policing purposes
- The relationship with individuals is not direct with Qlik Sense as it is originally stored on other systems.
- Qlik Sense is processing data for a secondary purpose; users have control of their data via whichever means they already have control in the source system(s).
- Data processed includes personal data on young and/or vulnerable people
- Data will be used by Criminal Intelligence staff and officers to identify/create/manage cohorts of people known to Wiltshire Police and Partner agencies who we feel may warrant more/different proactive intervention/support. Algorithms will be created which rank persons according to the risk/harm they may cause/be subject to and while this is intended as an internal aide to decision-making, there have been concerns raised across the country regarding such behaviour.
- *The Force Disclosure Unit Operations Manager has confirmed that Qlik Sense data is not admissible for disclosure requests from employees or the public.*

d) Describe the purposes of the processing:

- The purpose of processing this information is to improve intelligence throughout the organisation by linking data sources together via a single reporting tool, providing apps and reports.
- This will reduce the number of systems individuals require to obtain access to permitted information about themselves and their team, or to enable them to do their job more effectively.
- The data is intended to be used for predictive analytical purposes in line with the ALGO-CARE framework as already identified above (use of predictive analytics software will be subject to their own DPIA).
- Qlik Sense data will be used to monitor existing cohorts of people and provide risk-based “scoring” of individuals e.g. RSOs or Outstanding Suspects.
- The data will be used to identify data-quality errors throughout the linked data sources, enabling users to find and correct errors in information, including personal data in a timely fashion. Data quality errors identified in Niche data will be made available to the Data Quality Team for consideration of rectification. For other Force databases, the IAO/database owner or their designated proxies will be given access to apps detailing the data quality errors/anomalies and they will be responsible for taking appropriate action.
- The data will be used to aid in the identification of areas of demand reduction, enabling cost savings and/or efficiencies.

3. Consultation:

a) The following consultation approach and stakeholder groups were incorporated into the consultation process:
- Formal consultation did not take place, for the following reasons:
  - Qlik Sense is a replacement for an already recognised Force system (QlikView).
  - QlikView and Qlik Sense were both fully supported and championed by ELT (Executive Leadership Team) and the OPCC (Office of the Police and Crime Commissioner) (Office of the Police and Crime Commissioner).
  - The additional capabilities of Qlik Sense over QlikView do nothing to change the amount of/way that we handle personal data, other than increasing the number of people in Force who can access data.
  - Qlik Sense and QlikView are already used by several other UK Forces, including Avon & Somerset, Gwent, West Midlands, and Dorset Police.

b) A summary of the stakeholder views are as follows:
- N/A

c) The above stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities.

4. Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair, lawful, and transparent:

- The Lawful basis for the processing of personal data will be dependent on the type of data being processed and the purpose of each individual application. The probable lawful basis for the intended use of Qlik Sense is provided below:

  - Personal data (General Processing; UK GDPR (General Data Protection Regulation)):
    - Article 6 (b) Performance of a contract
    - Article 6 (c) Legal Obligation
    - Article 6 (e) Public Interest / task

  - Special Category data (UK General Processing; GDPR):
    - Article 9, 2(a) Explicit Consent
    - Article 9, 2 (b) Employment Law
    - Article 9, 2 (g) Substantial public interest

  - Criminal data (Law Enforcement Processing – special category and criminal convictions etc data; DPA 2018):
    - *Will meet a condition in Schedule 1, Part 1-4, and have an appropriate policy document in place where required.*

- Criminal data (Law Enforcement Processing – conditions for sensitive processing under Part 3; DPA 2018):
  - *Statutory etc purpose*
  - *Administration of justice*
  - *Protecting individuals' vital interests*
  - *Safeguarding of children and individuals at risk*
  - *Personal data already in the public domain*
  - *Legal Claims*
  - *Preventing Fraud*
  - *Archiving*

- Explain how individuals will be made aware of the processing:
  - The Force Privacy Notice outlines how personal data will be processed by Wiltshire Police, and how they can opt out of its use for scientific research and statistics.

Principle 2: Use of personal data is for a specified, explicit, and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:

a) If collecting personal data for primary use, explain how you have targeted only the information required:
   - Data is not collected for primary use.

b) If re-using personal data for further use, explain how this secondary use is compatible with the original reason you collected it:
   - Qlik Sense will only ever process data for a secondary purpose which is compatible with the primary purpose for which it was collected or for analytical purposes.
   - Qlik Sense is the only practical way in which the Force will be able to provide statutory data to the Home Office and NPCC without purchasing alternative tools.
   - As per the Force Privacy Notice, individuals are advised that we will process personal information for the purposes of “Administration of Justice,” to meet our “Legal Obligations,” and to improve the service we provide the public.

Principle 3: Use of personal data is adequate, relevant, and no more than necessary:

a) Explain how the amount of personal data you intend to use is enough to be understood by the audience, but no more than the minimum needed to achieve your purpose:
   - Qlik Sense will process all personal data recorded in the source databases but, when creating and publishing applications what data is used and displayed for users will be limited to only the data the Developers deem to be appropriate and proportionate, in accordance with the requirements of the user(s) who have commissioned the work. Developers will use their professional judgement in this matter and liaise with the original IAO or the

Force Data Protection Officer where they deem in necessary.

Principle 4: Personal data must be accurate and kept up to date:

a) Explain how accurate recording of data will be achieved and how it will be kept up to date, where necessary:
- All the personal data will be extracted from the source systems, transformed (for formatting purposes) where necessary and presented in a read-only format.
- Personal data presented in Qlik Sense can only be amended by updating the original data source.

b) Explain any mechanisms that will allow you to amend or append data that is found to be inaccurate (i.e.: DQ errors in recording):
- Qlik Sense will have data quality applications, or sheets within applications, which can be used by Wiltshire Police to inform database administrators to manually update the source databases/systems.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

a) Data held in the new IT System – explain how any automated and / or manual capability to delete data will be used to comply with MoPI (Management of Police Information) retention rules or the NPCC Retention Schedule:
- Data is a transformed copy of existing data in source systems, and when data is removed from the source system, the next time the application(s) are updated they will mirror these changes.
- All applications will inform users that the data presented within is only accurate up to the most recent reload timestamp, as well as what data ranges are included.
- Data files (.qvd) and applications (.qvf) which have been inactive for 6 months will get archived, then reviewed and deleted by the Developers after 12 months, unless it is confirmed the data will legitimately be required later. Where uncertainty remains, applications may be saved empty of data but with the script intact so it can be reloaded with fresh data

b) Data held in an unstructured manner (paper, word / excel files etc) - explain how you will use any automated and / or manual capability to delete data in line with MoPI retention rules or the NPCC Retention Schedule:
- Unstructured personal data stored in data files (.qvd) and applications (.qvf) which have been inactive for 6 months will get archived, then reviewed and deleted by the Developers after 12 months, unless it is confirmed the data will legitimately be required later. Where uncertainty remains, applications may be saved empty of data but with the script intact so it can be reloaded with fresh data

Principle 6: Personal data must be protected against unauthorised / unlawful use,

accidental loss, damage, or destruction:

a) Explain any technical security measures that will be put in place to protect the data:
   - Only staff members, in ICT-managed AD groups will be able to access *any* data held by Qlik Sense.
   - Qlik Sense has no permissions to write/delete data from any of the source systems it connects to.
   - Individual/sets of applications will also be further restricted from unauthorised use by limiting access to them via separate security AD groups.
   - Personal data regarding Wiltshire Police establishment will only be available within highly restricted Streams or via use of Section-Access within Qlik Sense applying role-based permissions as per the most recent data extraction from the Force's ERP database.
   - Qlik Sense is not fully auditable to "User Selection Level," it can be audited to show: times and dates of user access; applications accessed (or attempted to access). There are Qlik Sense applications on both the Non-Production (Developers and Analysts) and Production (all users) servers which contain this data.
   - We can turn on "Debug-level" auditing which will enable auditors to review every page and selection made by all users in case of any concerns about user activity, but these are presently turned off due to system performance and storage constraints.
   - When creating new, or making significant changes to apps in Qlik Sense, Developers will work exclusively on the non-Production server. This will limit the number of users who could gain access to personal data whilst apps are in testing/piloting and development.

b) Explain how you will make data users (staff) aware of any security measures or procedures they will need to follow:
   - Developers will be fully trained in the application of security measures within Qlik Sense, specifically how to create security groups for applications, and how to add and remove people from group. This will limit the number/type of people who can access certain applications containing sensitive personal data.
   - Applications will include a cover page reminding them of the Acceptable Use of Force Systems Policy, the date ranges covered by the application, when the file was last reloaded, and what to do following a data breach, including links to the relevant documents & policies.
   - All staff and officers are required to complete the NCALT data protection training which outlines their responsibilities, and the legislation, with respect to data protection.

7. Personal data will be processed in accordance with the individual's data protection rights:

a) Explain, where relevant, how requests from individuals wanting to exercise their rights, will be managed.
   - Individuals will be able to exercise their rights with respect to the source systems (Force databases and flat files) their data is recorded within, in line with existing Force processes, as defined in the Force's privacy notice.

Individuals will not be able to exercise their rights directly with respect to Qlik Sense except that live data files and applications will reflect changes made to the source systems they are reading from the next time they are reloaded.

- Qlik Sense data files and applications which are no longer in use will be archived (restricting access to them to the Developer team only) after 6 months, and will be deleted, or have the personal data recorded within deleted, after 12 months.

8. Personal data will not be transferred outside the UK without guaranteed adequate privacy protections:

a) Confirm whether personal data is being processed outside the UK and if so where:
   - No data will be processed outside the UK

b) If yes to a) above - explain which of the formal / recognised 'adequacy' measures will guarantee privacy protection:

9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & UK GDPR:

a) Explain what (if any) governance documents will be required to support the data processing (e.g.: Information Sharing Agreements, Data Processor contractual clause etc):
   - All staff and officers are required to complete the mandatory College Learn Managing Information (data protection) training which outlines their responsibilities, and the legislation, with respect to data protection.
   - The Force policy on acceptable use of Force systems and policy following a data breach are kept up to date and accessible via the Force's intranet site.
   - Any regular data sharing with external organisations will require an ISA (Information Sharing Agreement) or ensuring the data complies with existing standards as defined by the Force Disclosure Unit.

b) Detail, where known, what governance arrangements will be in place to oversee the processing of personal data in a compliant manner when BAU:

   - Information Asset Owner(s) will be consulted during the development of applications to confirm they authorise the way their data is to be used and they accept any data quality and lawfulness risks. This process is not required where the manner of processing and the audience for the data remain within bounds already authorised.

   - The Developers will maintain a Data Governance/Information Asset Owners List, detailing the below (see Annex B). The purpose of this list is to enable Developers to know what they are permitted to create in Qlik Sense and who for, before they consult with IAOs:
     - Data Source & Type
     - IAO
     - Information Guardian
     - Pre-approved audiences for summary data (inc. caveats)

- Pre-approved audiences for record-level data (inc. caveats)

- Only pre-approved audiences for record-level data will be used for data testing and validation of Qlik Sense apps and data.

- Qlik Sense will not be used for surveillance purposes; Developers will ensure they understand the Code of Practice for Covert Surveillance and Property Interference and if they are in any way uncertain will refer the work to the CAB Manager. The CAB have confirmed that applications that use only Wiltshire Police data confer little to no risk with respect to the Code of Practice for Covert Surveillance and Property Interference. The default position regarding surveillance is that Wiltshire Police Qlik Sense Applications requests for surveillance purposes will require an amendment to this DPIA.

- IAOs, or their designated proxies, will be provided with all data quality reports/information stemming from the application design to enable them to both update the source systems with accurate data, and if necessary, either delay the final publication of an application and/or ensure appropriate warnings are provided with the application with regards to the risk of decisions being made on the back of poor data quality.

- Where a Developer identifies an app as deviating from pre-agreed standards/limitations they will liaise with the IAO (or the designated proxy) to present/describe the deviation and obtain approval before publishing. The standards/limitations for consideration include:

    - New personal data not yet presented via Qlik Sense
    - Users who have not yet seen such data via Qlik Sense
    - New methods of presenting such data that may lend itself to users inferring or making judgement about persons or groups

- Where Professional License Users (other than Developers) wish to publish data, a Developer will review the new data/users and, using their professional judgement, determine whether it needs referring to the IAO.

5. Identifying and assessing risks.

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

The listed 'agreed actions' have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

	Describe the source of the risk, the problem it creates and the potential impact on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible, or probable.	**Severity of harm** Minimal, significant, or severe.	**Risk score** Low, medium, or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium, or high.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]				[redacted]		
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

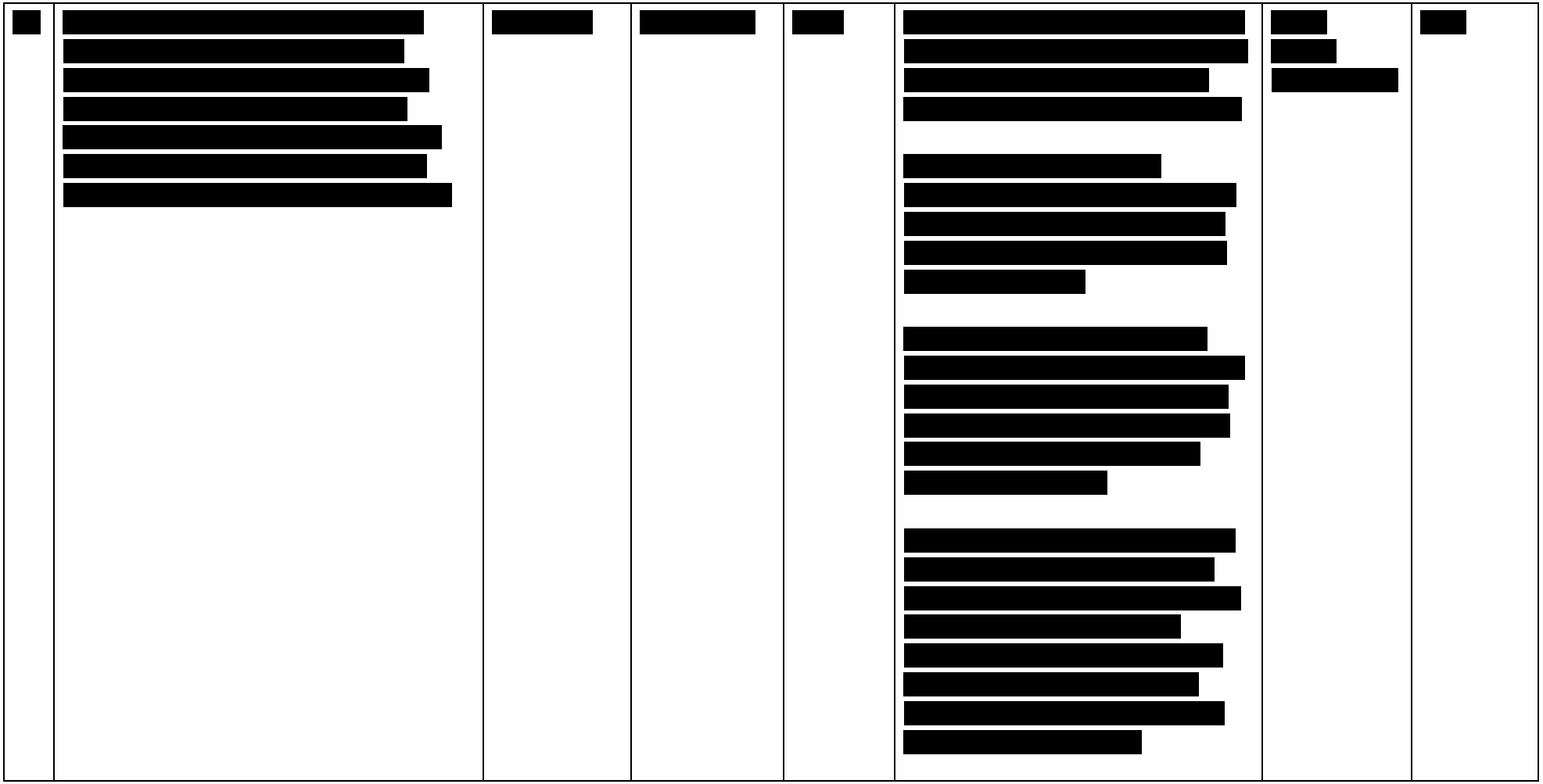
	[redacted]				[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]W

					[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

					[redacted]		

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]



[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

***If you have accepted any of the above risks you must provide a rationale for doing so in the 'Agreed Actions' column.**

6. Authorisation of DPIA:

DPIA copies will be retained by the DPO, Information Asset Owner and within the relevant Project Management records.

- **Approval signatories**

Item	Name / role / date	Notes
Risk Reducing Measures approved by **Information Asset Owner:**	[redacted] Head of Improvement & Change, 2nd April 2020 [redacted] Head of Improvement & Change, 24th May2022	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by **Senior Responsible Officer**:	[redacted] Head of Improvement & Change, 2nd April 2020 [redacted] Head of Improvement & Change, 24th May2022	Acceptance of mitigating actions.
Residual risks approved by **XXXXXX** (in consultation with IAO):	N/A – No residual high risks identified.	If accepting any residual high risk, consult the ICO before going ahead
Data Protection Officer approval of DPIA:	[redacted], DPO, 9th October 2019 [redacted], DPO, 30th March 2020 [redacted] DPO, 24th May 2022	DPO should consider any medium / high residual risks and whether processing can proceed

Summary of DPO advice:
9th October 2019: It is my advice that this processing activity can continue, subject to the agreed mitigating actions being implemented fully.

The DPIA process has identified a number of risks, with the level of some remaining residual risk still presenting as medium after mitigating actions have been identified and agreed.

Much of this DPIA has been written from a theoretical perspective and the proposed processing activities (to include the commissioning process) have not been fully tested due to the limited role out of Qlik Sense to date.

Therefore, this DPIA will need to be reviewed after an initial 6-month period to determine whether the risks identified have changed level (either in severity or likelihood), and also to

assess whether any new risks have identified during the course of the processing activity.

30th March 2020: I am assured by the changes made to this DPIA, specifically the detail provided for the processes that have been agreed and implemented to manage the commissioning of new apps, publication of apps, management of user categories, vetting requirements, and audit capabilities.

It is my advice that this processing activity should continue, subject to the agreed mitigating actions being fully implemented. Any outstanding risks should be considered for recording on the appropriate Local Risk Register, with the IAO being responsible.

However, due to many of the residual risks still being assessed as medium and potential capability for high-risk processing activity, I advise that this DPIA will need to be reviewed in 6 months' time (October 2020).

24th May 2022: I have reviewed the revised DPIA in full, and in particular welcome the clarity that has now been provided regarding the processes for Commissioning New Work, Developing New Work, New Data Connections and Data Validation Reviews (please refer to the process maps in Annex A). I also note the revisions made to the risk section, and that after identifying / agreeing mitigating actions there are two risks remaining with a residual risk level of low.

It is my advice that this processing activity continue, understanding that there is still work on going to address the identified risks. I advise that this DPIA should be reviewed in 12 months time.

- **Residual high risks (complete <u>only</u> if there are any 'high' <u>residual</u> risks):**

Item	**Name / role / date**	**Notes**
DPO advice accepted or overruled by **Senior Information Risk Owner (SIRO):**		If overruling the DPO's advice you should record your rationale below
SIRO Comments:		
Date and name of person referring DPIA to ICO:		As required by law if any high residual risks remain.
Summary of ICO advice:		

- **Accountability – update of 'records of processing':**

Information Management Name / role	Information Asset Register	Special Category Data Policy Document	Notes
			Add dates the records were updated.

- **Review of DPIA:**

Item	Information Management Name / role / date	Frequency	Notes
DPIA will be kept under review by:	[redacted] (IG), Senior Developer	12 months	1st review to be completed after 6 months and annually thereafter.

A. Annexes

Annex A. Qlik Sense Process Maps

This PowerPoint contains maps for the following processes:

- Commissioning new work
- Developing new work
- New data connections
- Data validation reviews
- Managing the backlog of work
- Creating/Updating AD Groups and Stream (security)

These process maps will be reviewed by the Qlik Sense IAO and IG annually.

Annex B. Data Types and Information Asset Owners

This SharePoint list details each Data Type, its data source, Information Asset Owner, Information Guardian (where applicable) and any limitations/rules for its use in Qlik Sense.

The list will be maintained and updated by the Developers during both the commissioning and development processes, and will be reviewed by the Qlik Sense IAO and IG annually.

Annex C. Qlik Sense Streams and Owners

All Qlik Sense Streams are owned by The Qlik Sense Information Asset Owner, this ownership may be shared by one or more Information Asset Owners depending on the original data sources used to create the Qlik Sense Apps within each Stream.

Information Asset Owners will be informed before a new app, or significant change to an existing app, is added to a Stream to ensure proper authorisation is received.

The list of Streams and their [Information Asset] Owners will be recorded in this SharePoint list. The list will be maintained and updated by the Developers during both the commissioning and development process, and will be reviewed and the Qlik Sense IAO and IG annually.

Annex D. Development Backlog

The Qlik Sense Development Request Form automatically fills in the initial fields required within the Development Backlog. Qlik Sense decision-makers then review the data from the form and add to it as required (following the commissioning process detailed in Annex A). Once work has been approved by the relevant Information Asset Owners, the Developers creating a product will refer to the Development Backlog and add further detail where appropriate.

Annex E. Qlik Sense Development Request Form

All requests for new applications, or significant changes to existing applications are recorded here. The request form enables user to self-serve a request, which are then regularly reviewed.

B. Appendices

Appendix A. Definition of Terms

- **Development Backlog** – The list of Qlik Sense applications or amendments (products) not yet started work on. This owned by the Qlik Sense Information Asset Owner.
- **Product** – A Qlik Sense application or amendment.
- **Product Backlog** – A prioritised list of tasks developed from the list of Customer Stories and their pre-requisites which, when completed, will deliver the Product. This may be curated by the Developer working on the Product, or someone better acquainted with the Customer needs. Tasks should be prioritised into “Musts, Shoulds and Coulds,” where all the “Musts” combined should describe the Minimum Viable Product.
- **Customer Story** – A user/customer requirement (experience or activity) within a Product; the customer (or their representative determines the priority of each Story). Each story must include a clear definition of what “Done” looks like.
- **Task** – An activity to be completed by a member of the Delivery Team; Developers determine which Tasks they will undertake in which Sprint, and only tasks deemed “Ready” may be added to a Sprint backlog.

- **Sprint** – A pre-defined period (2-4 weeks) containing a list of tasks (from the Product Backlog) as defined by the Developer to meet the Sprint Goal.
- **Sprint Backlog** – A list of tasks (from the Product Backlog) to complete in a single Sprint; any incomplete tasks are returned to the Product Backlog for a possible later Sprint.
- **Sprint Goal** – A clear objective for each Sprint defined by the Delivery Team.
- **Delivery Team** – The group of people responsible for delivering the Product (in a series of Sprints). Comprised of the following roles (within Wiltshire Police): Product Owner; Developer(s); Scrum Master (optional). If the Product is only being delivered by a single person, then they are responsible for all roles.
- **Product Owner** – Responsible for the Product Backlog; they are the "Voice of the Customer" and are responsible for prioritising, refining, and decomposing the Tasks in the Product Backlog until they are Ready to be added to a Sprint Backlog.
- **Scrum Master** – Servant Leader to the Delivery Team: Serves the Delivery Team by facilitating meetings and maintaining morale; Serves the Product Owner in managing the Product Backlog; Serves the Developers to maintain Agile working practices and removing barriers to completing Tasks; Serves the Organisation by explaining and embedding Agile practices.
- **Definition of "Done"** – Defined by the Customer; what the Customer defines as sufficient to accept the Task as good enough.
- **Definition of "Ready"** – Defined by the Developer; when the task objective is clear *and* the predicted time to deliver is less than the Sprint duration.
- **Minimum Viable Product (MVP)** – The minimum capability of the application. If during development it transpires that the Developer cannot meet the MVP, this is grounds to stop all development.
- **Significant Change** – Any change to an existing application that deviates from the capability as authorised by the Information Asset Owners.
- **Data Source** – The database or flat file the data comes from (e.g. Niche, Storm, First File spreadsheet etc.)
- **Data Type** – A [brief] description of the type of data within the system (e.g. Intelligence, staff data, staff diversity data etc.)
- **Information Asset Owner** – The Force recognised owner of the Data [Type]. In the context of the GDPR, Information Asset Owners are Accountable for the quality, integrity, and protection of their data space. This includes Defining Policies, Creating Trusted Data and Eliminating Redundancies.
- **Information Guardian** – Effectively the deputy for the Information Asset Owner, however, where the Information Asset Owner is accountable for the data, the Information Guardian is responsible for the data. There are six key areas of responsibility: Define the Data; Create Processes and Procedures; Maintain Data Quality; Optimise Workflows; Monitor Data Usage; Ensure Compliance and Security
- **Pre-approved audience for record-level data** – In terms of Qlik Sense: staff within the organisation pre-approved by the Information Asset Owner or Information Guardian to be able to view unverified, record-level data within a Qlik Sense app. Normally staff in the same department as the Information Asset Owner and/or Information Guardian, and regular users of the data. These staff would be the first go-to for Qlik Sense Developers for verification of data within Qlik Sense apps prior to final publication.
- **Pre-approved audience for summary data** – In terms of Qlik Sense: staff within the organisation pre-approved by the Information Asset Owner or Information Guardian to be able to view unverified summary data within a Qlik Sense app. They

are not approved to view record level data, so this would be data like: Crimes per CPT; Staff off sick per Department etc. These staff could be used to verify summary data only.

- **Data Domain** – See Data Source & Data Type.
- **Qlik Sense SMEs (Subject Matter Experts)** – Subject Matter Experts within the Improvement & Change department with respect to the Data [Type].
- **Defining Policies** – As they have a vested interest in the integrity of their data, owners focus on defining policies (for example retention or deletion policies) and standards that ensure the alignment of their data to the GDPR.
- **Creating Trusted Data** – Data ownership is a key ingredient to gain customer trust and achieve measurable business benefits. Poor data could easily result in bad customer experiences and losing customers. When personal data is not reconciled into a data subject 360° view, compliance with data subject access rights, such as rights of portability or rights to be forgotten cannot be fully achieved.
- **Eliminating Redundancies** – As organizations strive to put the appropriate governance framework in place for GDPR, one common frustration is a loss of productivity. This issue stems from multiple teams addressing the same problem either because there is not a clear understanding of data or they are not even aware that the problem has been resolved by another team. Federated ownership eliminates these painful issues.
- **Define The Data** – Define the data and identify assets within their own Data Domains. This ensures there is not conflict with other data elements.
- **Create Processes and Procedures** – Create processes and procedures along with access controls to monitor adherence. This includes establishing internal policies and standards—and enforcing those policies.
- **Maintain Data Quality** – Maintain quality of the data using customer feedback, concerns, questions; internally reporting metrics; evaluating and identifying issues; and coordinating and implementing corrections regularly.
- **Optimise Workflows** – Optimize workflows and communications.
- **Monitor Data Usage** – Monitor data usage to assist teams, share best practice trends in data use, and provide insight into how and where teams can use data to help in day-to-day decision-making.
- **Ensure Compliance and Security** – Ensure compliance and security of the data. Data Stewards are responsible for protecting the data—while providing information on potential risks and offering regulatory guidance.
- **Unverified Data** – In terms of Qlik Sense: apps/pages where data structures have not been verified by (or on behalf of) the Information Asset Owner or Information Guardian.
- **Verified Data** – In terms of Qlik Sense: apps/pages where the data structures have been checked and tested by (or on behalf of) the Information Asset Owner or Information Guardian.
- **Data Structure** – In terms of Qlik Sense: Developers extract, transform and load data from one or more Data Sources into Qlik Sense. Data presented via Qlik Sense *should* be identical to that in the Data Sources, but there are times when it differs, either to "gloss over" Data Quality issues, human error on the part of the Developer(s), or because rules have been agreed with the Information Asset Owner to transform the data into a new format or value.
- **Qlik Sense** – Software/Business Intelligence (BI) tool for aggregating data from multiple Data Sources and presenting it in self-service BI dashboards.

- **Business Intelligence (not the Team) –** A technology-driven process for analysing data and delivering actionable information that helps executives, managers and workers make informed business decisions. As part of the BI process, organisations: collect data from internal IT systems and external sources; prepare it for analysis; run queries against the data; and create data visualisations, BI dashboards, and reports to make the results available to business users for operational decision-making and strategic planning.