



Date: 14/04/2025
Our ref: 01/FOI/25/014233/D

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/25/014233/D

I write in connection with your request for information dated 17/02/2025, received by Greater Manchester Police (GMP) for the following information:

1. *A copy of the Force's DPIA for the use of the Auror Retail Crime Intelligence Platform.*
2. *A copy of the standard operating procedure and/or policy regarding the Force's use of the Auror Retail Crime Intelligence Platform.*
3. *Number of your Force's Police Officers that are registered users of the Auror Retail Crime Intelligence Platform.*

Result of Searches

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP. However, I am not obliged to supply you with all the information held as exemptions apply.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because this information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies.

*Some of the information you have requested is exempt from disclosure by virtue of the following exemptions: **Section 31(1)(a)(b) – Law Enforcement** and **Section 40 – Personal Information***

Where reactions occur in the attached Data Protection Impact Assessment (DPIA) and are annotated with “S31”, this is because that information would, or would be likely to, prejudice the prevention or detection of crime and the apprehension of offenders. Section 31 is a qualified and prejudice-based exemption and as such, subject to a harm and public interest test.

S31(1) - Evidence of Harm

A Freedom of Information Act request is not a private transaction. Both the request itself and any information disclosed, are considered suitable for open publication. This is because under the Act, any information disclosed is released into the wider public domain, effectively to the world, not just to an individual.

Whilst not questioning the motives of the applicant, providing any further information relating to specific law enforcement operations and intelligence gathering tactics used by Greater Manchester Police would reveal our operational capability, which would be of intelligence value to criminals.

Disclosure of tactical options at the police's disposal, including those used to prevent, detect and investigate crimes against the retail sector, will mean that those people who are committing crimes and pose a risk to the public, would be able to formulate ways to circumvent or overwhelm GMP. If disclosed the tactics used by GMP will become less effective and will mean that the police are not able to detect and prevent crime, apprehend, or prosecute offenders or to administer justice for the wider community.

There is always a duty of care to the public and GMP has a clear responsibility to ensure the prevention or detection of crime, and the apprehension or prosecution of offenders is always delivered. There are several tactics available to GMP to ensure the effective delivery of operational law enforcement. In this case, specialist policing activity is required to undertake fair investigations where it may be necessary to progress a range of reasonable lines of enquiry.

As such, the disclosure of any further information which would hinder the forces law enforcement functions cannot be in the public interest.

Public Interest Test

Factors favouring disclosure for S31 - Where public funds are being spent, there is a public interest in accountability and justifying the use of public money. Disclosure of the requested information would enable the public to assess whether the force has appropriately taken steps to help reduce and detect retail crime. Release would enhance public debate as to whether the force is appropriately and effectively engaging with the threat posed by criminals to businesses, workers and customers in the retail sector.

Factors against disclosure for S31 - Disclosure that reveals our operational capabilities would compromise law enforcement tactics. Criminals could use the information to target areas of perceived weakness assuming that their activities are less likely to be detected. It may be used by criminals who are intent on pursuing their criminal activity, to identify and exploit the limitations of these resources.

To release information relating to operational capacity and capability utilised for the prevention, detection and investigation of retail crime would have a detrimental effect on our policing capabilities. Therefore, to mitigate any risks, disclosure of this information needs to be protected, to ensure that those with intent to do so cannot manipulate it or undermine its purpose in any way.

Any disclosure of information which would compromise law enforcement tactics and thus lead to more crime being committed by reducing the opportunity for the prevention and detection of crime, would therefore increase the risk to public safety, which is not in the public interest.

Balancing Test

Law enforcement is of paramount importance and GMP service will not disclose information if to do so would undermine its purpose and place the safety of people at risk. Whilst there is a public interest in the transparency of using public money in policing appropriately and effectively engaging with the threat posed by criminals, there is a very strong public interest in safeguarding the integrity of police investigations and operations in this area.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of law enforcement, this will only be overridden in exceptional circumstances. Any disclosure which hinders our capability and assists criminals cannot be in the public interest.

It is for these reasons that I have determined that the balance test favours non-disclosure of the requested information.

Section 40(2) represents information that identifies a living individual. Where reactions occur in the attached Data Protection Impact Assessment (DPIA) and are annotated with "S40", this is because that information is information that identifies a living individual. To disclose this information would breach the principles of the Data Protection Act 2018. Personal data is defined by Section 1 of the Data Protection Act 1998 and means data that relates to an individual who can be identified directly or indirectly from that data.

Section 40 is an absolute exemption and there is no requirement to conduct a public interest test for such data.

1. Please see a redacted copy of the DPIA attached.
2. No information is held by GMP. No such policy or operating procedure exists.
3. No information is held by GMP. GMP do not keep a record of registered users of Auror.

Greater Manchester Police

Data Protection Impact Assessment

Name of project/initiative: Auror Intelligence Platform



DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of the envisaged processing operations on the protection of personal data.

It is a checklist against Information Governance compliance and is a risk management process that enables Greater Manchester Police to anticipate and address likely impacts of new initiatives, to provide assurance of confidentiality, integrity, availability, data subject rights, IT security and data quality issues related to the project. ,

This assessment **should be completed at the project planning stage** of any major project involving the use of personal data or if you are making a significant change to an existing process.

Notes on completion:

Please answer all questions in Section 1. Should all questions be answered "No" there is no requirement to complete Section 2. In such instances please send the completed assessment to Information Compliance and Records Management Unit (ICRMU) via email to: [REDACTED] S40

If any answer in Section 1 is "Yes" please continue to complete Section 2 and send the completed assessment to the ICRMU as above.

Any queries during completion should be directed to the ICRMU. It follows the process set out in our DPIA guidance and this document should be read along with the guidance.

Any changes to original assessment must be notified to the ICRMU as above. Once all changes are completed, the final completed assessment must also be emailed to the ICRMU as above.

The ICRMU will ensure the Data Protection Officer comments on this assessment before final sign off.

VERSION CONTROL FOR THIS DPIA

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)
V0.1	14/05/24	Initial draft	[REDACTED]
V0.2	12/07/24	ICRMU review	[REDACTED]
V0.3	17/09/24	ICRMU further clarification	[REDACTED]
V0.4	18/11/24	DPO review	[REDACTED]
V0.5	29/11/24	ICRMU updates following clarification provided by CC	[REDACTED]
V0.6	29/11/24	DPO 2 nd review	[REDACTED]
V1	02/01/25	DPO further review and sign off	[REDACTED]

S40

Overview

Project/System/ Initiative	Auror Intelligence Platform					
Information Asset Owner	[REDACTED] S40					
Department/location	FIB					
Select one of these options	New system / process	x	Change to existing system / process		New use of existing data set	

Explain broadly what the project aims to achieve/what benefits would it deliver.

What would be the consequences of not processing/sharing the data?

You may find it helpful to refer or link to other documents, such as a project proposal

Project Aim:

GMP use of Auror intelligence platform.

Auror is a Software-as-a-Service (SaaS) "Platform" that is designed to help retailers' "Customers" reduce crime in their stores and keep people safe. [REDACTED]

S31

The Platform processes data (including personal information) about security and safety events for the purpose of:

- Facilitating a coordinated approach that targets offenders, crime and anti-social behaviour.
- Facilitating the collection and exchange of relevant information
- Supporting the private exclusion of individuals to prevent known troublemakers from committing repeated offences.
- Providing anonymised statistical and crime trend data to ensure businesses are prepared against potential criminal activity.

Auror's Customers are Data Controllers of all data inputted into the platform. Auror is a Data Processor and therefore can only use data for the purposes agreed with Data Controllers. Auror cannot share data with third parties without written permission from the original controller.

The Customers on the Platform have all contracted with Auror (including confidentiality provisions) to ensure that all data transfer will take place via the Platform. Data will therefore not be shared outside of the secure environment.

UK Police Chief Officers are Data Controllers of data within their own forces' possession and require a purpose and lawful basis for sharing information with a non-competent authority (Auror Customers).

Necessity:

Customers rely on the Platform to collate information about retail crime and other similar events to provide them, and the other Users in their chosen community, with intelligence that assists with the prevention of crime and the protection of people and assets. The ability to share information with UK Police enables more effective collaboration between police and retail, enabling better outcomes, and increasing safety in stores and the local community. Police access would support the NPCC Retail Crime Action Plan, whereby local policing teams are encouraged to work with retailers to identify those offenders who cause the most harm and develop joint action plans to target their offending.

S31

S31

[REDACTED]
[REDACTED]
[REDACTED] Auror is one of these third-party

companies.

Proportionality:

The Platform creates a controlled data sharing framework which provides a safe and consistent means of data sharing between Customers and UK Police. The Event submission form has been designed based on the principle of data minimisation. Only personal data required for the purpose of retail crime intelligence reporting and prevention is captured and processed by the Platform.

SECTION 1:

DPIA Screening Questions: If the answer to all of the questions below is 'No', a full DPIA is not required. In such instances just complete this page and submit the document to the Data Protection Officer / ICRMU for review and approval.

If the answer to any of the questions below is "Yes", a full DPIA should be completed. Submit the completed questionnaire to the ICRMU for review and Data Protection Officer approval.

Does the change initiative involve any of the following:		Yes	No
1.	Use systematic and extensive profiling or automated decision-making to make significant decisions about people? <i>Includes evaluation or scoring of individuals</i>		x
2.	Process special category data or criminal offence data on a large scale? <i>Special category data includes: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; data concerning health; data concerning a person's sex life or sexual orientation)</i>	x	
3.	Systematically monitor a publicly accessible place on a large scale? <i>Includes CCTV and other surveillance systems</i>		x
4.	Use new technologies? <i>Includes innovative technological or organisational solutions</i>	x	
5.	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? <i>Whether or not this is on a large scale</i>		x
6.	Carry out profiling on a large scale? <i>Even if this does not involve automated decision-making</i>	x	
7.	Process biometric or genetic data? <i>Whether or not this is on a large scale</i>		x
8.	Combine, compare or match data from multiple sources?	x	
9.	Process personal data without providing a Privacy Notice directly to the individual? <i>Even if the lawful basis for processing suggests a Privacy Notice is not required</i>	x	
10.	Process personal data in a way which involves tracking an individual's online or offline location or behaviour?		x
11.	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?		x
12.	Process personal data which could result in a risk of physical harm in the event of a security breach?		x
13.	Does the scale of the project alone justify completion of a DPIA for quality assurance purposes?	x	

Conclusion:	Yes	No
Is there an intention to complete a DPIA?	x	

If all answers above are No there is no requirement to continue to Section 2. Please email the assessment to the ICRMU via email to: [REDACTED] S40

If any answers above are Yes please continue to complete Section 2 below before emailing the assessment to the ICRMU as above.

SECTION 2: Please refer to the guidance notes on completing a DPIA

Step 1: Identify the need for a DPIA	
1.0 Summarise why you identified the need for a DPIA S31	The Auror platform is designed to process data about individuals involved in retail criminality. This includes criminal offence data on a large scale due to the high volume of incidents. [REDACTED] [REDACTED]
Step 2: Describe the processing	
2.1 How will data be collected or obtained and how will the data be used? S31	Auror Customer Data is collected and owned by Auror Customers [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
2.2 Will you be sharing data with anyone? <i>You might find it useful to use a flow diagram or another way of describing data flows</i> S31	Data flow as follows: Data Capture - [REDACTED] [REDACTED]

S31	Data Storage - Personal data is stored within Snowflake, Auror's data warehouse tool that is used as a central repository to host data from various systems within Auror. This includes sources such as the Platform transaction database, [REDACTED], and the product analytics data. Data Processing - Data is processed within the Auror Platform, hosted on Microsoft Azure Data Sharing - The Auror Platform is a multi-tenanted environment that shares "Platform Insights" across all Customers in a particular geography to assist in identifying repeat activities and organised retail crime. (see additional detail in 2.3) Data Deletion - Once the retention period has lapsed, all personal information is hard deleted from the Auror Platform database, including any backups.
2.3 How will the data be transferred? <i>i.e. Physical data (paper format)</i> - collected/hand delivered in person - postal (i.e sent via special delivery, double enveloped). <i>i.e. Electronic data</i> - via secure system (i.e Egress – secure email). - Files/disc/pen drives (encrypted – password protected) Please refer to Government Security Classifications (GSC) Policy & Procedure S31	Auror Customers will share data with UK Police via the electronic Platform and UK Police have the ability to share relevant offender information with Auror Customers via the Platform. As data controllers, Auror Customers have the ability to turn off data sharing with UK Police if they choose. Customer data cannot be shared to third parties without written permission from the original controller. Auror receives written confirmation that a retailer opts-in to data sharing with police. Retailers can withdraw from data sharing via a written request and an Auror Administrator would update data sharing permissions in the platform accordingly. In terms of cross-retailer data sharing, the Platform is a multi-tenanted environment that compiles "Platform Insights" across all Customers in a particular geography to assist in identifying repeat activities and organised retail crime. Platform Insights include the number of events an offender has been involved in, the total value of those events and when the offender was last active. Platform Insights do not show the details of what other retailers have entered about those Events, such as the nature of those Events, where they occurred geographically or what items were stolen. UK Police have the ability to share relevant offender information with Auror Customer via the Platform by [REDACTED]. The relevant Auror Customer will update the Person Profile based on the information included within the comment, for example naming an unknown individual. All Auror Customers who have Events linked to the Person Profile in question will have visibility of the update. Auror Customers who do not have Events linked to the Person Profile will not have access to the update. This limits access to information shared by UK Police to Auror Customers that have a purpose for receiving this information. There are no international data transfer considerations as data will not be shared outside of the UK.
2.4 How will the data be stored? <i>i.e. physical data – locked away in draw/cupboard</i> <i>electronic data – stored on a secure network/server with logon/password credential, files/disc/Pen drive encrypted.</i>	Auror Customer data is hosted in a secure, multi-tenanted environment provided by Microsoft Azure. Auror processes UK data within a UK-based server. Users access the Platform via a secure web portal and/or mobile application. Personal data is stored within Snowflake, Auror's data warehouse tool that is used as a central repository to host data from various systems within Auror. This includes sources such as the Platform

Please refer to Government Security Classifications (GSC) Policy & Procedure S31	transaction database, [REDACTED], and the product analytics data. The Platform is fully hosted in the cloud with Microsoft Azure. As a global data storage provider, Microsoft has developed strong privacy and security processes and controls and has provided assurances within its own Online Services Terms in respect of compliance with global privacy and security regulations. Microsoft Azure's data centres are SOC 1/SSAE 16/ISAE 3402, SOC 2, and ISO 27001/27002/27018 compliant. Auror does not share customer data, including personal data, with any other third-party processors
2.5 What will be the retention of the data? <i>i.e. will data be retained as per MOPI (see link) or other retention schedules / statutory requirements that are applicable to the data?</i>	Auror retains data in line with each of its customer's data retention policy (most companies hold for 7 years to ensure alignment with broader company policies and statute of limitations etc).
2.6 How will the data be deleted/disposed of? <i>i.e. those parties/partners processing/sharing data with, do they have their own disposal policy?</i> <i>Will information be returned back to the data controller (GMP) for destruction?</i> <i>Will data be disposed of inline with Government Security Classifications (GSC) Policy & Procedure</i>	Once the retention period has lapsed, all personal information is "hard deleted" (removed from the database in its entirety), including any backups. Statistical data (trend analysis etc) is stored separately and will be retained at an aggregate level only and is anonymised. By deleting the primary information that includes PII, it is not possible for this data to be re-identified, as it no longer exists. Some examples of this kind of data are below: Number of incidents involving violence Number of incidents attributed to a repeat offenders Number of new offenders Number of incidents per store
2.7 What types of processing identified as likely high risk are involved? <i>Please see link to ICO website explaining what constitutes high risk processing</i> S31	Innovative technology: [REDACTED] The use of AI has been designed with the guardrails of Auror's Responsible AI Framework. There are also numerous safeguards in place, for instance: - No person of interest within Auror who has been recorded as younger than 18 years of age will be included in this process. - Only results with a high confidence will be surfaced as possible matches within the Auror platform. - Only results with a high image quality will surface as possible matches within the Auror platform. - If someone is incorrectly linked in Auror, they can be unlinked. - A person's identity must still be verified through formal investigation by loss prevention teams and/or Police for each reported event, and preceding and enforcement or legal proceedings. Data Matching:

S31	Auror's intelligence platform combines data captured from multiple sources to create a single, aggregated profile for an offender, demonstrating the scale of their offending [REDACTED] Invisible Processing: Auror allows store colleagues to capture retail crime events without the knowledge of the data subject. This allows store colleagues to capture retail crime intelligence in a safe manner. Data processing on a large scale: Auror enables the capture of retail crime events at high volume. However, the principle of data minimisation is applied throughout the data capture process. The Platform captures only relevant and necessary fields of personal data.
2.8 What types of data subject will be involved? <i>i.e. offenders, victims, GMP employees, children, vulnerable adults etc</i>	Persons suspected of having committed or being about to commit a criminal offence. Persons convicted of a criminal offence Witnesses or other persons with information about offences
2.9 What category of personal data will be processed, basic personal identifiers (name, d.o.b, address etc) or will it also include special category or criminal offence data? <i>Special Category Data refers to:</i> - personal data revealing racial or ethnic origin; - personal data revealing political opinions; - personal data revealing religious or philosophical beliefs; - personal data revealing trade union membership; - genetic data; - biometric data (where used for identification purposes); - data concerning health; - data concerning a person's sex life; and - data concerning a person's sexual orientation.	The Platform is designed to facilitate the processing of only the personal information needed to manage crimes and other security events. The Customer ultimately decides the level of personal information they are willing to use the Platform to process. Personal information may include - People Details (where available): including image, name, DOB, age, address, mobile phone number, ID details, gender, height, build, distinguishing features, and behaviour. Note: The Platform does not ask the user to enter an individual's skin colour or ethnicity as these are often classified as "sensitive information" and can create additional risk around racial bias or profiling. - Vehicle Details: registration plate, colour, make, model. - Evidence: images, videos (CCTV), receipts, witness statements. - Other Details: Details of any witnesses, law enforcement information (including crime reference number) and officer details. Note: The Platform enables Users to crop and obscure any images of innocent bystanders to ensure that they are not identifiable in the information captured and shared by the Users on the Platform.
2.10 How much data will you be collecting, using and how often? How many individuals are affected? <i>Provide figures if known and timescales (i.e. monthly, once etc)</i>	Customers are encouraged to report all events that occur, this could be more than 5000 data subjects. The volume of data will increase dependent on the number of customers that use the platform. Police will have daily access to the platform and all the data contained with it for which consent has been given to share.

2.11 How long do you expect this initiative to last?	Open ended
2.12 What geographical area does it cover? <i>i.e. the whole of Greater Manchester, one District, etc?</i>	UK Police users have access to the Intel module as standard and will be able to view and access all crimes reported and personal data associated with those crimes nationwide. The data can be defined to a specific location which would allow for local area policing. Intelligence relating to cross border offending in GMP and other forces is accessible.
2.13 How much control will the data subject have over the data being processed? Would the data subject expect you to use their data in this way?	Data processing is taking place without the knowledge of data subjects. Personal data belonging to data subjects is processed for the purpose of building retail crime intelligence to better facilitate the identification, apprehension and prosecution of offenders. Consulting data subjects on data processing would impede this purpose. Society would reasonably expect intelligence sharing to take place for law enforcement purposes.
2.14 GMP require a cyber security assessment to be completed; Please provide an email address and full company name; <i>We require your participation in our third-party security risk management programme. This process gives us assurance that our suppliers have implemented an appropriate level of security controls to protect themselves, and us, from cyber incidents.</i> How? <i>GMP use Risk Ledger to manage this process. Risk Ledger is a third-party platform that allows suppliers to complete one comprehensive security assessment which can be shared with any other client who requires an assessment - not only does this save organisations a lot of time, but helps to speed up their sales cycles. We are committed to making this process as pain free as possible for our suppliers, and Risk Ledger helps us to do that. Risk Ledger has strict data privacy and security policies, which can be found in their Terms and Conditions and Privacy Policy. For further information on Risk Ledger please look at Risk Ledger's FAQs.</i> What next? <i>The third party will receive an email from the email address [REDACTED] asking them to sign up to their platform and complete an assessment. Once submitted, we will have visibility of the results. GMP might raise discussions with them within the platform once we begin our review.</i>	[REDACTED] S40 [REDACTED] [REDACTED] S40

If you have any questions about the process please message [REDACTED] S40 •	
2.15 Are there any current issues of public concern that you should factor in? <i>i.e. this could include the impact on the public or where there is no impact then state the benefit on the public</i>	Benefits to society and general public: Local communities will benefit from being able to enjoy safer environments in which to shop, live, work and commute. Providing intelligence on retail crime helps police identify, apprehend and prosecute repeat offenders. Our data shows that repeat offenders are four times more likely to display aggression or violence, therefore by helping the police tackle these worst offenders, Auror is improving safety within retail stores and the community. Disadvantages to society and general public: There is the potential risk that personal data of non-offending members of the public are captured and stored in the platform. To mitigate this risk the platform has built-in redaction software to ensure no other members of the public, employees or contractor data is visible. Collateral intrusion is reduced to a minimum and with regards to video visual data collection focused only on those involved and only for the minimum duration necessary.
2.16 What is the intended effect on data subjects who's personal data you are processing?	Benefits to data subjects (suspects/victims): The ability to capture and share retail crime intelligence provides store and security colleagues (victims) with greater ability to remain safe in the workplace. Having access to information on a person's previous behaviour and threat level allows store and security colleagues to adapt their behaviour e.g. not approaching a person known to be violent. Identifying problematic behaviour in suspects can lead to rehabilitation and community support. Disadvantages to data subjects (suspects/victims): The Platform prevents any form of racial bias or profiling by not allowing users to enter an individual's skin colour or ethnicity. However, retailers and police are able to use Auror to profile data subjects based on their behaviour, e.g. create blacklists or top offender lists. These lists could be used to implement preventative measures against the data subjects, e.g. preventing from entering stores.
Step 3: Consultation process	
3.1 Describe when and how you will seek the data subject's views or justify why it's not appropriate to do so. What information will you give data subjects; is the processing covered either by GMP's (see link below) or another organisation's privacy notice? https://www.gmp.police.uk/hyg/fpngmp/privacy-notice/ <i>If not you may be required to complete a privacy notice (PN) (template of PN obtainable from ICRMU)</i>	Data processing is taking place without the knowledge of data subjects. Personal data belonging to data subjects is processed for the purpose of building retail crime intelligence to better facilitate the identification, apprehension, and prosecution of offenders. Consulting data subjects on data processing would impede this purpose.

S40

3.2 Who else do you need to involve within GMP, or in the case of partners, their organisation? Do you plan to consult other subject matter experts? <i>i.e.</i> • Info. Compliance & Record Mgt Unit - ICRMU (Data Protection) – [REDACTED] • Information Security Team – ([REDACTED]) • The Information Services Branch and systems administrators who will provide access to GMP system(s) • Vetting unit – if having access to GMP systems/premises etc? • Procurement / HR / Legal Services?	Info. Compliance & Record Mgt Unit - ICRMU (Data Protection) aware and will be consulted throughout. Head of FCMU has been consulted with regards platform access for Initial Investigation Officers. Information services and HR will be consulted with regards control of access to the platform. [REDACTED] has been consulted regarding the need for this to go via a project board. Digital management team Auror and Auror customers supportive of UK police access.
3.3 Do you need to ask the other parties/partner/processors to assist/comply? <i>i.e is this arrangement governed by a contract / Data Processing Agreement / Information Sharing Agreement / IT Systems Access Agreement / Memorandum of Understanding</i> <i>Legislation / policy & procedures</i> <i>Reviews?</i>	An Information Sharing Agreement is to be considered along with potential Memorandum Of Understanding /Standard Operating Procedure. The ISA is relevant for police and other customers (retailers) sharing data across the Auror platform. There is currently no contract in place with Auror. Auror will be contracting with GMP as part of an SaaS solution.
Step 4: Assess necessity and proportionality	
4.1 What is your lawful basis for processing? Is the processing subject to a statutory act/legislation?	This processing is in line with the Law Enforcement purposes of the Data Protection Act 2018: CHAPTER 1 Scope 29 Processing to which this Part applies (1) This Part applies to— (a) the processing by a competent authority of personal data wholly or partly by automated means, and (b) the processing by a competent authority otherwise than by automated means of personal data which forms part of a filing system or is intended to form part of a filing system. (2) Any reference in this Part to the processing of personal data is to processing to which this Part applies. (3) For the meaning of “competent authority”, see section 30. 31 “The law enforcement purposes” For the purposes of this Part, “the law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Further to above, the processing is in line with the following Schedule 8 conditions: Statutory etc purposes 1 This condition is met if the processing—

	(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) is necessary for reasons of substantial public interest. Administration of justice 2 This condition is met if the processing is necessary for the administration of justice.
4.2 Is there another way to achieve the same outcome? <i>Can the data be anonymised or pseudonymised in any way</i>	The Platform has been carefully designed to assist Customers apply a data minimisation approach to retail crime reporting and prevention. The Platform captures only relevant and necessary fields of personal data, determined as a result of a robust design process which included input from global law enforcement agencies and major retailers. The Platform also controls the fields of personal data the customer can capture on the Platform, to ensure that it is relevant and appropriate. While a select number of text fields are required to allow users to capture incidents accurately, these are limited and pre-populated options are preferred.
4.3 How will you prevent function creep? <i>i.e the gradual widening of the use of the intended purposes to which the data was originally collected/processed for.</i>	The use of the Auror Platform will be governed by the same rules as the use of any other police system. Police employees will use Auror in a way that follows the relevant Police policies. MOU will be considered for inclusion. Permission to access the platform will be granted and monitored by the Retail Crime lead. User activity on the platform is fully auditable and an audit report can be provided by Auror. An audit report on a user's activity includes: • User search terms and browse parameters a user sets to filter results • User activity (i.e. page views) On request, a monthly report can be produced by Auror and shared with police forces showing who has access to the Auror platform.
4.4 How will you ensure data quality and data minimisation?	The Platform has been carefully designed to assist Customers apply a data minimisation approach to retail crime reporting and prevention. The Platform captures only relevant and necessary fields of personal data, determined as a result of a robust design process which included input from global law enforcement agencies and major retailers. The Platform also controls the fields of personal data the customer can capture on the Platform, to ensure that it is relevant and appropriate. While a select number of text fields are required to allow users to capture incidents accurately, these are limited and pre-populated options are preferred.

	A training input will be provided to all users.
4.5 How will you help to support the data subject rights? <i>i.e. GMP's data being processed will be supported by GMP's Information Compliance & Record Mgt Unit.</i>	Auror has built safeguards into the Platform that control the way information can be processed by its Users. All Users must agree to Terms of Use that limit access to the Platform and the ways in which they can use the Platform. Unlawful data processing such as racial profiling or sharing information about minors is not facilitated by the Platform. Auror operate a review and retention policy in relation to data stored on the Platform. GMP will draft an ISA supported by the Information and Compliance Unit. GMP will support in the event of a data breach or with any subject access requests that may include the data involved in the Auror system
4.6 Will the sharing of data involve any international transfers and how will you safeguard such transfers? <i>Consider if sharing data where in the world that data will be hosted/stored, i.e. UK, EU or further afield?</i>	There are no international data transfer considerations as data will not be shared outside of the EU.

Step 5 - Identify privacy and related risks and identify measures to reduce each risk.

*This DPIA assesses compliance and privacy risks for individuals, such as damage caused by inaccurate data, risk of ID theft following a security breach, or upset caused by not upholding rights or due to unnecessary privacy intrusion. Business risks should be recorded outside of this DPIA in the usual way. This assessment needs to reflect the likelihood and severity of risk **primarily for individuals** and if any residual high risks remain that cannot be reduced to an acceptable level, the ICO must be consulted. If you are uncertain how to identify or rate a risk, please seek advice from the DPO, an Information Governance lead or risk specialist.*

Risk Ref.	Description of Risk <i>Note: is this a risk to individuals, a compliance risk or an organisational risk?</i>	Likelihood, Severity and Overall risk	Solution(s)	Result – Eliminated, reduced or accepted	Measure approved?	Person responsible for risk
01	Lawfulness, fairness and transparency: Auror's Customers could capture data and processing in a way that is not fair or lawful such as engaging in racial profiling or sharing information about minors.	Likelihood: Possible Severity: Significant Overall Risk: Medium	As a responsible custodian of personal information, Auror has built safeguards into the Platform that control the way information can be processed by its Users. All Users must agree to Terms of Use that limit access to the Platform and the ways in which they can use the Platform. Unlawful data processing such as racial profiling or sharing information about minors is not facilitated by the Platform.	Reduced	Yes	Auror
02	Purpose limitation: Auror's Customers use Auror for the purpose of gathering, using, and sharing information about events and retail crime lawfully and respectfully. There is a risk that Customers will use data stored on the Platform for other purposes.	Likelihood: Possible Severity: Significant Overall Risk: Medium	The Platform stores and processes personal information on behalf of Customers and according to the instructions of Customers. Auror is a data processor, which means it does not use or disclose personal information uploaded by our Users for its own purposes. The Customers on the Platform have all contracted with Auror (including confidentiality provisions) to ensure that all data transfer will take place via the Platform. Data will therefore not be shared outside of the secure environment.	Reduced	Yes	Auror Auror Customer GMP

			GMP will set clear guidelines/SOP for use of the system and Platform will only be accessed for policing purposes.			
03	Minimisation Data types are captured and stored on the Platform that are not required for the purpose	Likelihood: Possible Severity: Significant Overall Risk: Medium	The Platform has been carefully designed to assist Customers to apply a data minimisation approach to retail crime reporting and prevention. The Platform captures only relevant and necessary fields of personal data, determined as a result of a robust design process which included input from major retailers and law enforcement agencies. The Platform also controls the fields of personal data the Customer can capture on the Platform, to ensure that it is relevant and appropriate. While a small number of free text fields are needed to allow users to capture incidents accurately, these are limited. The Platform enables Users to crop and obscure any images of innocent bystanders to ensure that they are not identifiable in the information captured and shared by the Users on the Platform.	Reduced	Yes	
04	Accuracy Incorrect data is stored and processed on the Platform.	Likelihood: Possible Severity: Significant Overall Risk: Medium	Auror enables Customers to update any information stored on the Platform if it is deemed to be inaccurate	Reduced	Yes	Auror Auror Customer GMP
05	Retention Data is retained data beyond the Customer's retention period.	Likelihood: Possible Severity: Significant	Auror retains data in line with each of its Customer's data retention policies. Once the retention period has lapsed, all personal information is "hard deleted" (removed from the database in	Reduced	Yes	

		Overall Risk: Medium	its entirety), including any backups. Statistical data (trend analysis etc) is stored separately and will be retained at an aggregate level only. By deleting the primary information that includes PII, it is not possible for this data to be re-identified, as it no longer exists.			
06	Security There is a risk that Users use the platform in a non-compliant way.	Likelihood: Possible Severity: Significant Overall Risk: Medium	Auror takes all reasonable steps to keep all Customer data, including personal information, safe and secure. All information in transit to and from Auror is encrypted using SSL 256-bit encryption. Transport Layer Security (TLS/SSL) is used to protect the transfer of information to our hosted servers. The Platform is also securely encrypted and Microsoft Azure complies with industry-leading security policies and standards, including SOC 1/SSAE 16/ISAE 3402, SOC 2, and ISO 27001/27002. Microsoft sets out all its security features in detail here. Auror also have policies, procedures, and contracts that ensure the people who use the Platform play their part in keeping data secure. All use of the Platform is logged and can be audited by Users to ensure that the personal information it contains is not misused. In the incident of a breach, Auror makes an assurance that it will identify and notify the customer of any data breaches it its agreement with the customers. All users will be provided with training on use of the platform.	Reduced	Yes	Auror Auror Customers GMP

07	Data Subject Rights Data subjects are not specifically informed regarding the processing of their personal data for onward prevention or use by a non-police, law enforcement agency/ commercial company.	Likelihood: Possible Severity: Minimal Overall Risk: Low	Auror supports Customer's obligations by allowing individuals to make privacy requests in relation to their own data (for example, to access, correct, delete or object to the processing of their data) through Auror's website, but will always direct these requests to the customer for processing. Where the customer receives a privacy request, the Platform will make compliance simple by allowing the customer to quickly locate personal data about the requester and either correct it, delete it, or provide a copy of it to the requester	Eliminated	Yes	Auror
----	---	--	---	------------	-----	-------

Step 6: Sign off and record outcomes

Item	Name / date	Notes
DPO advice provided by:	S40	DPO should advise on compliance, Step 5 measures and whether processing can proceed
Summary of DPO advice: Happy for processing to proceed, but care should be taken to monitor the use of this new technology which effectively uses AI to “data match” characteristics across multiple data sets to create a profile of an offender. As profiling by the police and retailers to make a list of “top offenders” could occur, checks should be made to ensure that racial profiling does not inadvertently take place. In addition, the anonymised data that is used for statistical purposes and trend analysis should be checked to ensure that it is truly anonymised and no individuals can be indirectly identified as a result. An ISA between GMP and participating retailers will need to be formulated once the contract with Auror has been signed. GMP will be using Auror’s services as a SaaS, and Information Security are part of the project board overseeing its development and roll out.		
This DPIA will be kept under review by:	Force Intelligence Bureau.	The GMP SPOC is responsible for reviewing this DPIA should there be any future changes. Any review/changes should be completed in consultation with the DPO