

Lumi Drug Scan

Brief Privacy Analysis

30 June 2020

1. Project summary: Lumi Drug Scan

1.1 Brief description of the project

a) *Describe your existing systems and the main changes that are proposed*

Workshops with frontline police have identified the need for an improved method to rapidly indicate whether a seized suspected drug sample is in fact a drug. NZ Police intercept ~10,000 suspected drug samples per year. The options currently available to Police (e.g. field colour tests, Raman devices at central hubs or laboratory analysis) are often cumbersome, expensive and inconvenient.

The Lumi Drug Scan project is developing a service for frontline police that will allow them to test suspected drug samples in the field in real-time. This service enables samples to be screened using a near-infrared (N-IR) hand-held device (called TactiScan) with the data being analysed automatically by machine-learning drug detection models hosted in the cloud. A mobile phone app connects the device to the cloud and provides functionality for Police to record metadata about the sample and to receive an in-app notification of the result. A report will also be emailed to the officer confirming the analysis. Real-time screening results will provide evidence that supports and improves decision making. This will reduce time processing the first stages of drug seizures and supports early intervention and diversion of drug users into non-judicial pathways.

The service will be trialled by Police in a 6-month pilot, involving selected staff from 5 districts. During the pilot Police will screen seized samples and assess the value generated from having access to real-time results. Samples screened during the pilot will be submitted to ESR for laboratory analysis to enable the reliability of the drug detection algorithms will be assessed.

b) *Describe the purpose of the change, including any projected benefits to your organisation or to the individuals affected*

Lumi testing is intended to provide rapid screening results to support frontline police to make decisions about how to proceed with a case when intercepting suspected drug samples. It delivers scientific results to the officer out in the field in real-time.

A number of benefits are anticipated from Lumi testing:

- Officer decision making in the field will have the benefit of being informed by evidence. This, in combination with the officer's experience and the circumstances of the event, will provide more confidence in decision making, reducing the time and effort in progressing a case.

- Early access to screening results will support opportunities to direct drug users down alternative pathways. Drug use is increasingly seen as a health issue, best supported by providing addiction services, rehabilitation and counselling. A distributed network of screening devices accessible by police in the field enables the capture of a broad set of data. This will enable collection of a data set that represents the occurrence and variety of drugs circulating in the community. This rich data set will support improved response and prevention activities to reduce the harm caused by drug use.

c) *Identify the main stakeholders or entities involved, and their role in the project.*

Lumi drug scan has been developed by ESR in collaboration with NZ Police. ESR and Police are the key stakeholders, with interest in the outcomes enabled by this analysis.

1.2 Personal information that the project will involve

In the table below, describe:

- *the personal information that will be collected, used and/or disclosed*
- *the source of the information*
- *the purpose of the information for your project.*

Note: "Personal information" is any information about an identifiable living person. However, a person doesn't have to be named in the information to be identifiable.

Type of personal Information	Source of Information	Purpose of information for the project
Identification details of the Officer using the service (name and email address)	Police Active Directory will provide user details through to the Lumi database when a user logs in	User name is collected and stored to enable sample information and results to be collated by user (and presented back to the user)
Location of the event recorded by GPS coordinates	The app captures the latitude and longitude coordinates at the time a sample is screened	The location of where a sample is tested is presented with the results of the particular test. Collated location data allows the distribution of testing to be presented and reviewed. This data will also enable the mapping of trends.

2. Privacy assessment

2.1 Areas that are risky for privacy

Some types of projects are commonly known to create privacy risks. If the project involves one or more of these risk areas, it's likely that a PIA will be valuable.

Use this checklist to identify and record whether your proposal raises certain privacy risks. Delete any that do not apply.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Information management generally			
A substantial change to an existing policy, process or system that involves personal information <i>Example: New legislation or policy that makes it compulsory to collect or disclose information</i>		✓	Police will use existing processes that enable them to search for and seize suspected drug samples.
Any practice or activity that is listed on a risk register kept by your organisation <i>Example: Practices or activities listed on your office's privacy risk register or health and safety register</i>	✓		A new risk assessment analysis has been completed covering the field use of the Lumi drug scan service
Collection			
A new collection of personal information <i>Example: Collecting information about individuals' location</i>	✓		Collecting the GPS coordinates from where a suspected drug sample is seized is a new collection of information, as well as the name and email address of officers.
A new way of collecting personal information <i>Example: Collecting information online rather than on paper forms</i>	✓		Data will be collected in the field using a mobile app.
Storage, security and retention			
A change in the way personal information is stored or secured <i>Example: Storing information in the cloud</i>	✓		Data collected will be stored securely in a dedicated Azure database. A security risk analysis has been completed for the data journey and storage into this database.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
<p>A change to how sensitive information is managed</p> <p>Example: Moving health or financial records to a new database</p>		✓	ESR is applying existing data management, security and access protocols to Lumi data.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
<p>Transferring personal information offshore or using a third-party contractor</p> <p>Example: Outsourcing the payroll function or storing information in the cloud</p>	✓		Lumi data will be stored in Azure using their Australian data centres.
<p>A decision to keep personal information for longer than you have previously</p> <p>Example: Changing IT backups to be kept for 10 years when you previously only stored them for 7</p>		✓	Data storage will be subject to existing standards for the management of ESR's forensic records.

Use or disclosure

<p>A new use or disclosure of personal information that is already held</p> <p>Example: Sharing information with other parties in a new way</p>		✓	ESR and Police will not share Lumi data with any other party unless by prior agreement. An example of a situation where ESR and Police may seek to share Lumi data is via a summary of information included in a report or publication.
<p>Sharing or matching personal information held by different organisations or currently held in different datasets</p> <p>Example: Combining information with other information held on public registers, or sharing information to enable organisations to provide services jointly</p>	✓		Police will provide the name and email address of officers logging in to the service. This will enable users to see results for samples they have tested and for results in the databases to be stored by user. Requirements for data reuse are the same as data sharing described above – only permissible with prior approval of ESR and Police.

Individuals' access to their information

A change in policy that results in people having less access to information that you hold about them <i>Example: Archiving documents after 6 months into a facility from which they can't be easily retrieved</i>		✓	ESR has drafted a Lumi Privacy Policy to describe the collection, storage and opportunities to access Lumi data.
---	--	---	--

Identifying individuals

Establishing a new way of identifying individuals <i>Example: A unique identifier, a biometric, or an online identity system</i>		✓	No new person identifiers will be created by or used in the system. No information about the individuals found in possession of suspected drug samples is collected and these individuals will not be able to be identified using Lumi data.
--	--	---	--

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
New intrusions on individuals' property, person or activities			
Introducing a new system for searching individuals' property, persons or premises <i>Example: A phone company adopts a new policy of searching data in old phones that are handed in</i>		✓	Police will use existing legislation that provides grounds for warrantless search and the seizure of suspected drug samples. Lumi testing will occur after a sample has been seized based on an officer's good cause to suspect that a sample is a controlled drug.
Surveillance, tracking or monitoring of movements, behaviour or communications <i>Example: Installing a new CCTV system</i>		✓	GPS data of sample testing locations will only be used for the purposes of trend analysis, via a dashboard that presents number of scans and locations.
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information <i>Example: Changing the location of the reception desk, where people may discuss personal details</i>		✓	No changes to Police or ESR physical spaces are anticipated.
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them <i>Example: Adding a new medical condition to the requirements of a pilot's license</i>		✓	No new regulatory requirements are anticipated.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space		✓	Nothing else.

2.2 Initial risk assessment

If you answered “Yes” to any of the questions above, use the table below to give a rating – either **Low (L)**, **Medium (M)**, or **High (H)** – for each of the aspects of the project set out in the first column.

For risks that you’ve identified as Medium or High, indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

If you answered “No” to all the questions in 2.1 above, move on to section 3 below.

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled	L	Officer information will be recorded to identify the person undertaking the screening of a suspected drug samples. GPS coordinates will be recorded of the location of each sample tested. All data will be encrypted and held securely, with policies in place to manage the access and use of the data.
Sensitivity of the information (eg health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive	L	No personal information from individuals found in possession of suspected drug samples is recorded.

<p>Significance of the changes</p> <p>L – Only minor change to existing functions/activities</p> <p>M – Substantial change to existing functions/activities; or a new initiative</p> <p>H – Major overhaul of existing functions/activities; or a new initiative that's significantly different</p>	L	Lumi becomes part of an existing Police process for seizing suspected drug samples.
<p>Interaction with others</p> <p>L – No interaction with other agencies</p> <p>M – Interaction with one or two other agencies</p> <p>H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction</p>	M	<p>Results obtained from Lumi testing will form part of the information used by Police to determine appropriate next steps when progressing an investigation that involves a suspected drug sample. Results from Lumi testing for a specific case may be made available by Police to other parties associated with that case, including health services, defence or prosecution lawyers, and the judiciary. Lumi testing results are not intended for use in court where the identity of the suspected drug sample is in question.</p> <p>Sharing or publication of trend information from Lumi testing may be approved by Police and ESR, where all identifying information has been removed.</p>
<p>Public impact</p> <p>L – Minimal impact on the organisation and clients</p> <p>M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern</p> <p>H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely</p>	M	<p>Members of the public who interact with Police in relation to the possession of suspected drug samples will see Lumi testing being undertaken and will see the results of the analysis.</p> <p>The real-time provision of screening results has the potential to support the decision making that an officer undertakes when progressing a case, and the interactions they have with members of the public.</p>

3. Summary of privacy impact

The privacy impact for this project has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	✓
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	
High – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	

3.1 Reasons for the privacy impact rating

Briefly summarise your reasons for the rating you gave above.

The privacy impact for this project has been rated as having a **Low Risk**. The rating of low has been selected because, firstly, only limited data is collected or stored by the app. The only personal data recorded is name and email address of a Police user who is accessing the app to test a sample. It is common practice for an officer to record their personal details as part of chain of custody and evidence recording procedures and therefore this is an accepted aspect of current workflows. The only location data recorded is the GPS coordinates of the location that a sample was tested. This data is only captured when a sample is tested and no other location information is stored during use of the app or by any background processes. Again, recording the location that a sample is collected from is common practice when samples are collected for subsequent testing.

Secondly, the solution has developed strong data storage, security and access protocols. All data captured by the app is encrypted during transfer and when stored in the database. An independent security audit has been completed describing the security layers incorporated into the functionality of the app and the cloud service where the data is processed and stored. ESR has implemented system and data management best practice recommendations from the independent review. Data management access and use processes in place across ESR's existing forensic science processes are in place.

4. Recommendation

A full privacy impact assessment is not required

A full privacy impact assessment is not needed as there are no significant risks associated with collecting, handling or processing the personal information used in Lumi. The summary of the privacy impact assessment is low, and although new data (in the form of GPS coordinates) is being captured, there are sufficient safeguards around the collection, handling, processing and storage of that information.