An effective approach to subversion, how does the municipality of Leiden do it?

In tackling organised crime and related subversion activities, municipalities play a prominent role. They have a strong information position; criminals need the facilities of municipalities, for example, to launder money and run their subversion business. These include buying, building and operating real estate, starting up hospitality establishments, applying for compulsory permits and so on. In doing so, they leave information with the municipality. But how does a municipality turn this valuable information into actionable intelligence within the applicable laws and regulations using i2's analysis and visualisation software, among others? We asked Freek Edeling, Information Coordinator/Project Manager of the Subversion Team at the municipality of Leiden.

DataExpert

The challenge

Dutch municipalities have a wealth of data at their disposal. However, for fear of privacy breaches, it is often not yet used to its full potential. The General Data Protection Requirement (GDPR) in particular creates a challenge to actually being allowed to convert the available data into useful and valuable intelligence. Because flat data from different sources, does not make intelligence. However, there are opportunities, in accordance with the applicable laws and regulations, to use the data to tackle subversion. This does mean that there must be a solid privacy protocol in place and the work processes must be followed very carefully.

Freek: *“The whole challenge is to obtain and process information weighted and as minimised as possible. In a way that you can justify in front of a judge or the Dutch Data Protection Authority”.*

Once the authority is able to use applicable data, the next challenge is to efficiently make the data transparent.

The solution: a roadmap

The solution according to Freek is to work with a roadmap drawn up in accordance with the privacy protocol drafted by the municipality of Leiden to tackle subversion. *“It is incredibly important to create a clear roadmap in which the steps, searches, rationales and findings are recorded as well as possible (visually) with supporting software programs such as i2. And in which (privacy) checks are carried out at different stages.”*

The roadmap

As described, the municipality of Leiden works with its own roadmap, based on the Ministry of Justice and Security's model privacy protocol. Below, we explain the working process step by step.

Step 1: identification

Logically, the first step in an investigation into subversion is to follow up signs of potential subversion activities. How and by whom a signal is picked up varies. First of all, municipalities generally know who the key players are in the criminal circuit of their own municipality. Especially if a subversion picture has been drawn up by the RIEC (Regional Information and Expertise Centres).

Within the municipality of Leiden, work has been done to train all employees to learn to recognise signs of subversion. This is a way for them to create awareness. If a colleague in the Licences Department then notices, for example, that an application to remodel a restaurant is being submitted for the fifth time in one year, they will alert the Subversion Team. In addition, other signals may come from, for example, an anonymous crime report, from the police or integral checks.

Step 2: signal assessment

The next step is to assess whether this signal falls under the responsibility of the Subversion Team or whether it belongs to another department. This is determined based on three criteria:

1. Is it a signal of subversion?
2. Does it involve a power of the municipality?
3. Does it take place within the territory of the municipality?

If the second or third question is answered 'no', the signal may need to be handled by a party outside the municipality. For example, if the signal is related to a violation of environmental legislation (without a subversion element), the Environmental Service will be notified.

Step 3: estimating the severity of the signal

If the signal can indeed be picked up by the Subversion Team of the municipality of Leiden, the first searches are carried out. These searches are designed to enrich the signal with other information and thus also estimate whether the signal is ‘severe’ enough for follow-up. To comply with GDPR regulations, in this phase the analysts only have the possibility to query open sources such as cadastral information (who owns the property), the WOZ (Valuation of Immovable Property) and the KvK (Chamber of Commerce). The analysts approach these sources from the already existing GIS data system. The first search can be used to answer questions such as:

- What property does the subject have and how is it financed?
- What companies is the subject involved in?

With this information, a good initial weighting can be performed.

Step 4: interim Privacy Check

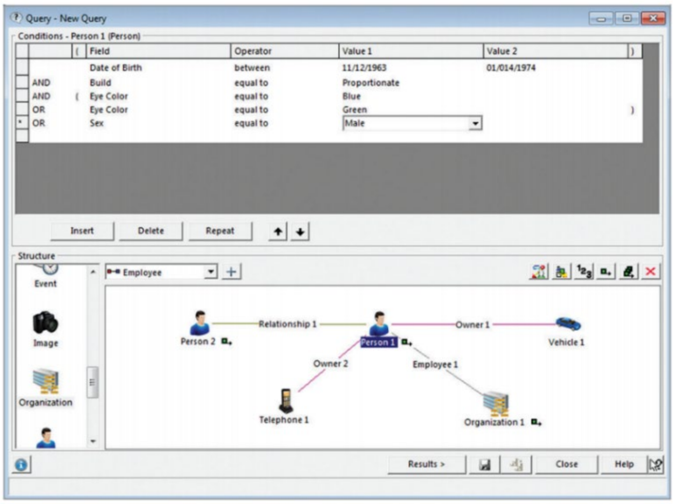
Whether the investigation continues, including using valuable closed sources, will be decided by the weighing team of the municipality of Leiden. The weighing team includes a lawyer, the privacy officer, programme manager, BIBOB (Public Administration Probity Screening) coordinator and a senior policy officer from the Security Team. This group of specialists determines whether the signal is severe enough to continue the investigation.

Step 5: source investigation

Once the weighing team agrees to continue the investigation, the Subversion Team can start adding more data to their investigation. Some of the data that can be added to the survey is in i2 iBase VIK.

This i2 iBase VIK is the Leiden Security Information Exchange. i2 iBase VIK is powered by an SQL database of basic registrations where data may not be enriched or modified. The information is identical to the data in the source file. Importing the data into i2 iBase is automated using the Scheduler option in i2 iBase.

i2 iBase allows the analyst to use queries to select useful information. These queries can be created by the analyst using a visual query option in the tool. No SQL knowledge is needed to query the database. According to Freek, you have to learn and get a feel which queries work best. You need to understand municipal processes to ask the right questions. The results of the previously mentioned queries within i2 iBase VIK, can then be added to a new investigation database. This creates a separate investigation database for each signal/case.



Query - New Query

Conditions - Person 1 (Person)

	(	Field	Operator	Value 1	Value 2	)
		Date of Birth	between	11/12/1963	01/014/1974	
AND		Build	equal to	Proportionate		
AND	(	Eye Color	equal to	Blue		
OR		Eye Color	equal to	Green		)
OR		Sex	equal to	Male		

Figure 1: Visual query example

In addition to the data exported from i2 iBase VIK, information from other sources such as permit applications, Enforcement Team registrations and so on is also added to the investigation database.

The selected investigation data is then visualised and analysed in i2 Analyst's Notebook. This way, a good and clear picture can be drawn of who the key players are, who has a connection with whom and in what time period certain activities took place.

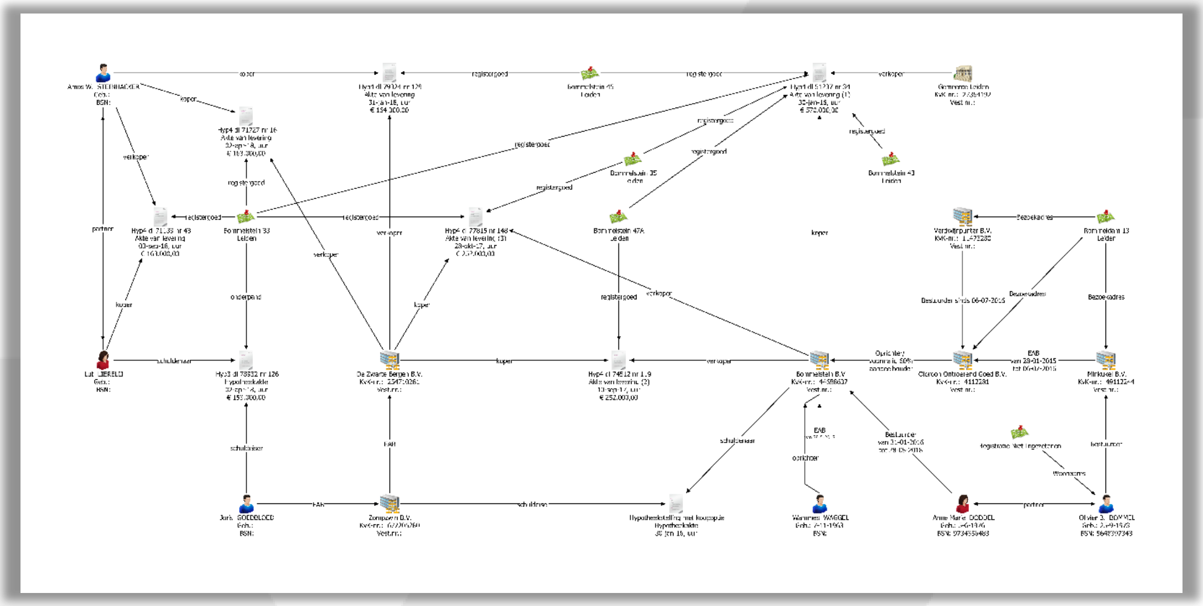


Figure 2: i2 Analyst's notebook diagram example

Step 6: weighting the findings

After completing the source investigation, consideration is given to whether the findings should be shared with other internal and external parties. This may include the police, the environmental services, the HEIT and/or the RIEC. This step also includes checking whether the investigation has been conducted in compliance with privacy laws.

If it turns out to be a case requiring deeper investigation in collaboration with partners such as the police, an action plan is drawn up and action is taken.

Freek: *"The nice thing is, all the steps you take in the investigation are also immediately logged within i2 iBase and i2 Analyst's Notebook".* Upon completion of an investigation, the database and analysis results are stored, archived and destroyed for the purpose of data minimisation and in compliance with the GDPR.

The outcome of the roadmap

"We now have a method that works well for our team and our municipality. Where I can look myself in the mirror and think: I have conducted a thorough and responsible investigation, which can be tested against the GDPR", Edeling notes.

Through the roadmap and the deployment of i2 software, the municipality of Leiden is able to realise a complete picture. Freek: *"You can of course make data comprehensible in all sorts of ways, such as with a mind map program or a bunch of Excel sheets, but i2 iBase and i2 Analyst's Notebook just works a lot better. It is beautiful software that is also used by many of our partners".*

By using i2 software, the municipality of Leiden can also easily share results with external parties if required. Indeed, in the investigation world, i2 software is a global standard when it comes to analysis and visualisation programs.

The future

"The process is in place, so now it is a matter of exploring how i2 iBase VIK can be expanded further by adding more data to the SQL database. For instance, you could add the municipal case system and funding data from the Land Registry", says Freek. Freek also thinks that all of a municipality's data should actually be in a data warehouse. That way, everyone can use same facility and the same data; with restrictions where necessary, of course. Data-driven work is valuable for everyone. Gathering everything together manually thus becomes a thing of the past.

Freek also mentions the importance of collaboration now, but certainly also in the future: *"If you were allowed to combine the information from the police and FIOD with your investigation, for example, you would get an even more complete picture".* Collaboration between municipalities should also be part of the future. Unlike the municipality of Leiden, some municipalities do not have sufficient capacity or budget to adopt such an approach. By pooling capacity together (with covenants, of course), you could get a lot more done in, for example, the fight against subversion.

Conclusion

Freek: *"The Approach to Subversion with i2 iBase is not just an application you use to make a diagram. It is the complete picture: the data, the knowledge and experience present, the work process and the software".* By sharing his experiences, Freek wants to inspire fellow municipalities to think about establishing such a work process. Within their own capabilities, of course. *"This is the only way we can really combat subversion properly",* says Edeling.

DataExpert is at your service

Just like at the municipality of Leiden, DataExpert's experts are happy to help you improve your information position and set up an appropriate work process. Besides the i2 analysis software used by the municipality of Leiden, we also offer OSINT tooling for gathering data from open sources, among other things. We also provide training to educate employees in the use of the tooling and our consultants are happy to help you figure out how the work process could be set up in your municipality.

Please contact us via:

P: +31 (0)318 543173

E: info@dataexpert.nl

W: www.dataexpert.nl