أمن تكنولوجيا المعلومات في نظام معلومات حوكمة بيانات الدولة هيئة الإحصاءات في ليتوانيا

Marijus Bernotas
Senior developer
State Data Governance Information System division
Statistics Lithuania

الإحصاءات الرسمية وحوكمة بيانات الدولة

في 1 يناير 2023، أصبحت الإحصاءات الليتوانية هيئة بيانات حكومية.

وفقا للمادة 5، الجزء 1 من قانون الإحصاءات الرسمية وإدارة بيانات الدولة في جمهورية ليتوانيا، وكالة البيانات الحكومية هي مؤسسة حكومية في جمهورية ليتوانيا تشارك في صياغة سياسة الدولة ليس فقط في مجال إدارة الإحصاءات الرسمية الموكلة إلى وزير المالية، ولكن أيضًا في مجال إدارة البيانات الحكومية.

الاحتياجات والتوقعات

تقدم منظمتنا ما يلي:

- مؤشرات مهمة لبلدنا وتحليل مختلف البيانات
- Data solutions للمنظمات الحكومية والعلمية والصحية
- أدوات إدارة الأزمات، بما في ذلك الأدوات المتصلة بـ COVID-19
- Open data
- البيانات لل eurostat
- بيئات تكنولوجيا المعلومات للمنظمات الحكومية والأوساط العلمية لإجراء تحليلاتها الخاصة باستخدام البيانات المدمجة في نظامنا.

قسم حوكمة بيانات الدولة

يتعلق نجاح نظام معلومات حوكمة بيانات الدولة بهذه العناصر الأساسية الثلاثة:

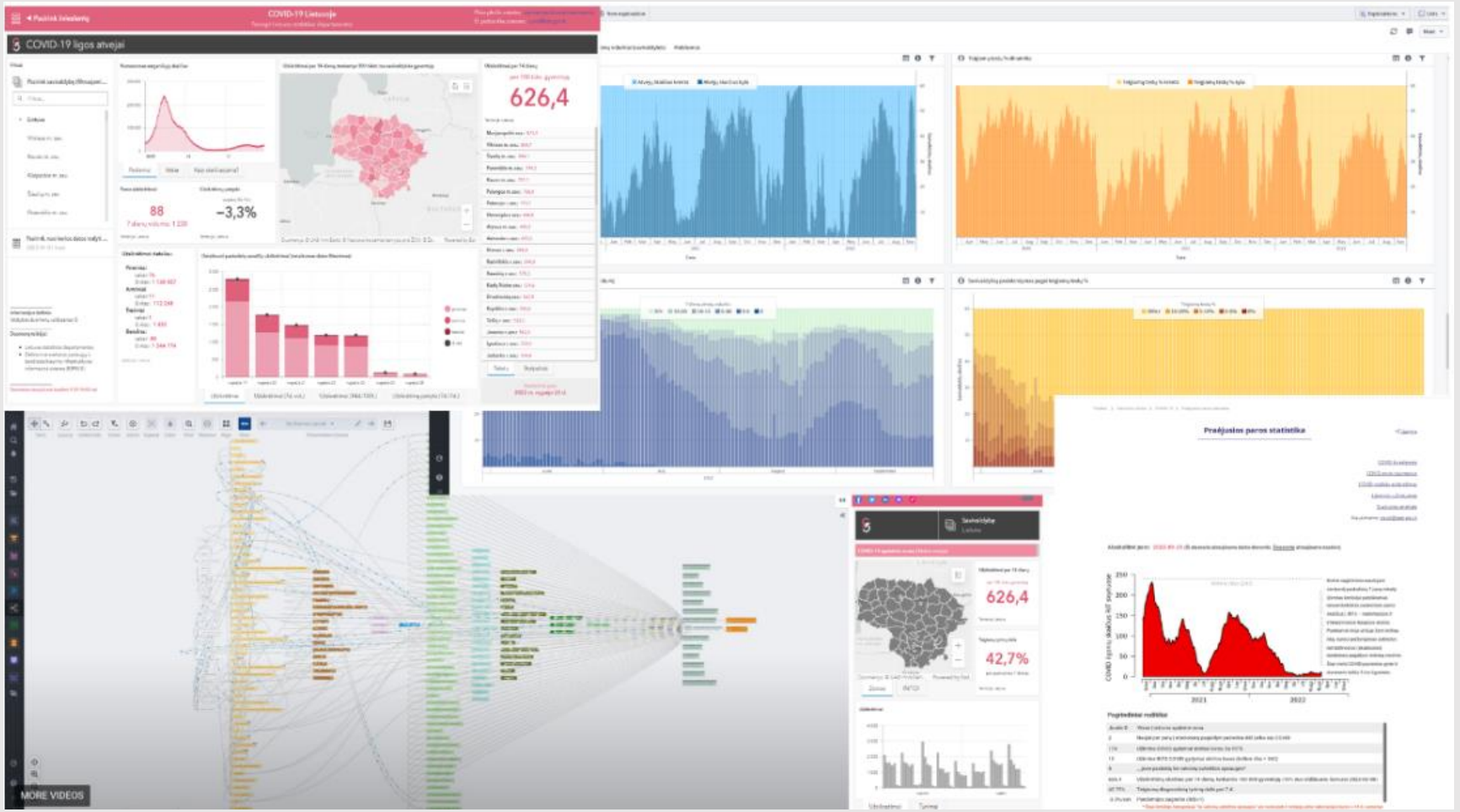
- التنظيمات القانونية
- Technical solutions
- الخبرة/الكفاءات

مثال - COVID-19 dashboards and reports

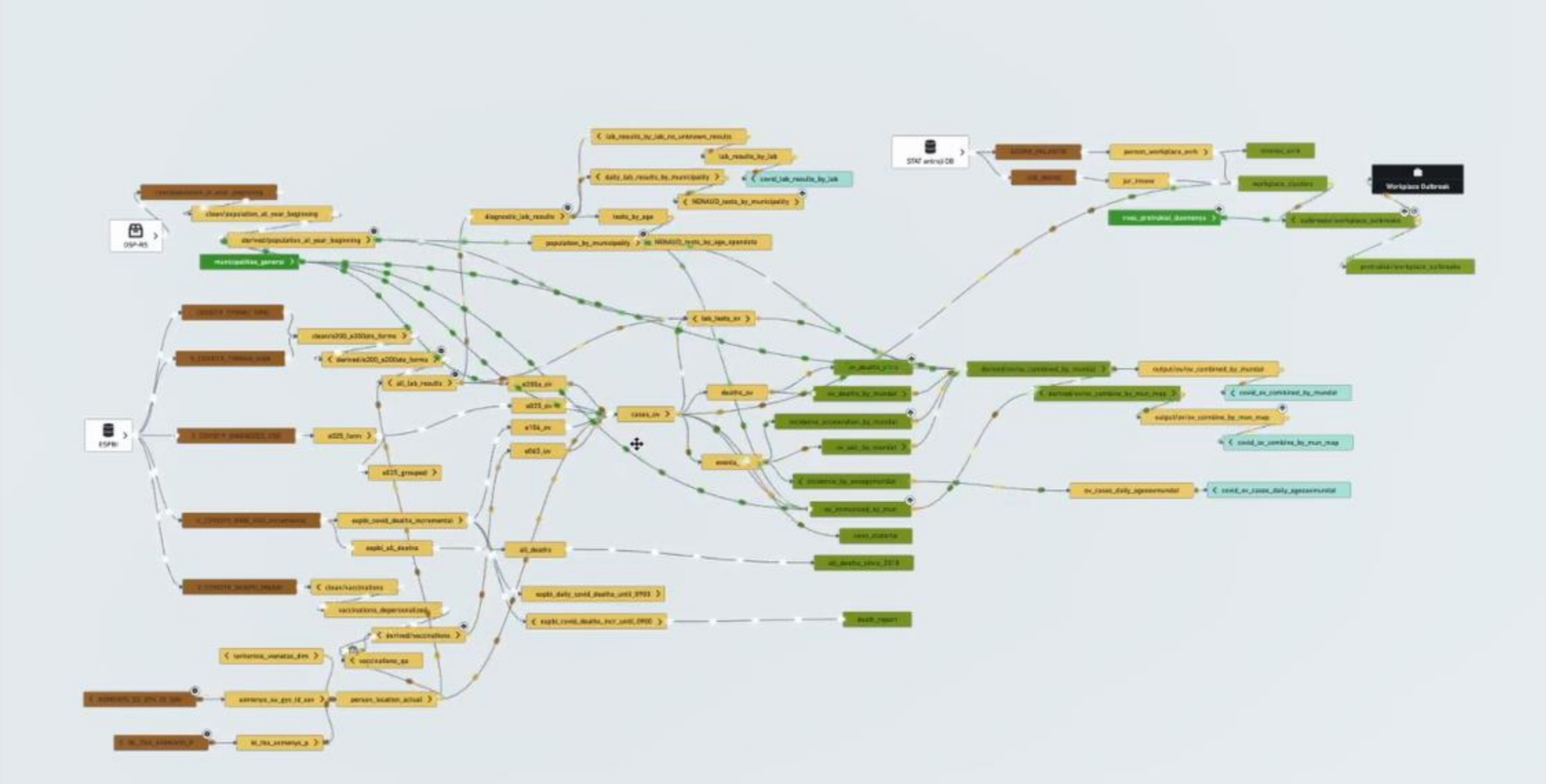
- Internal dashboards
- External dashboards

https://osp.stat.gov.lt/covid-dashboards

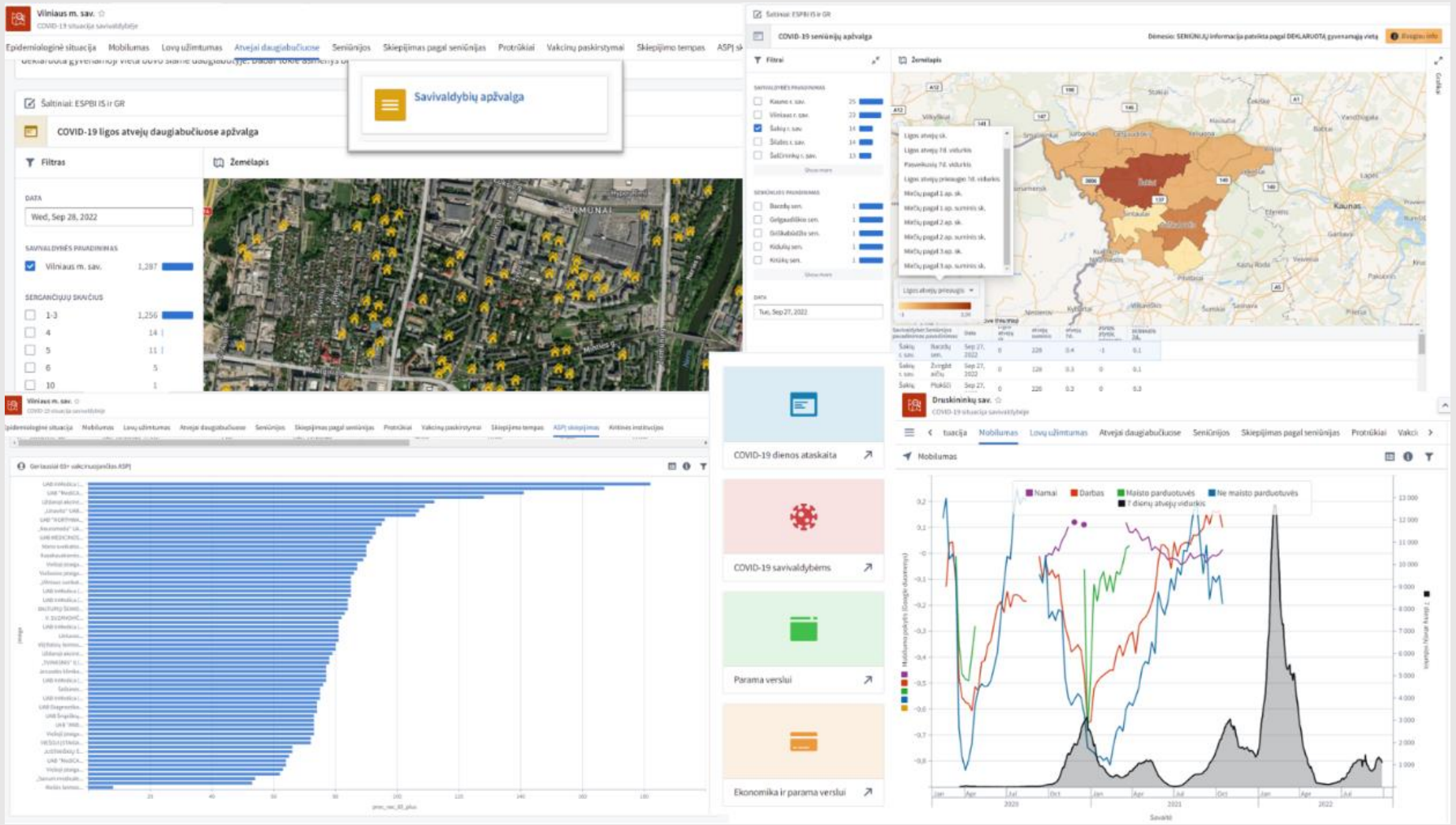
- Compatibile with mobile devices
- Daily report



مثال – COVID-19 data pipeline



مثال – internal dasbhoards for municipalities



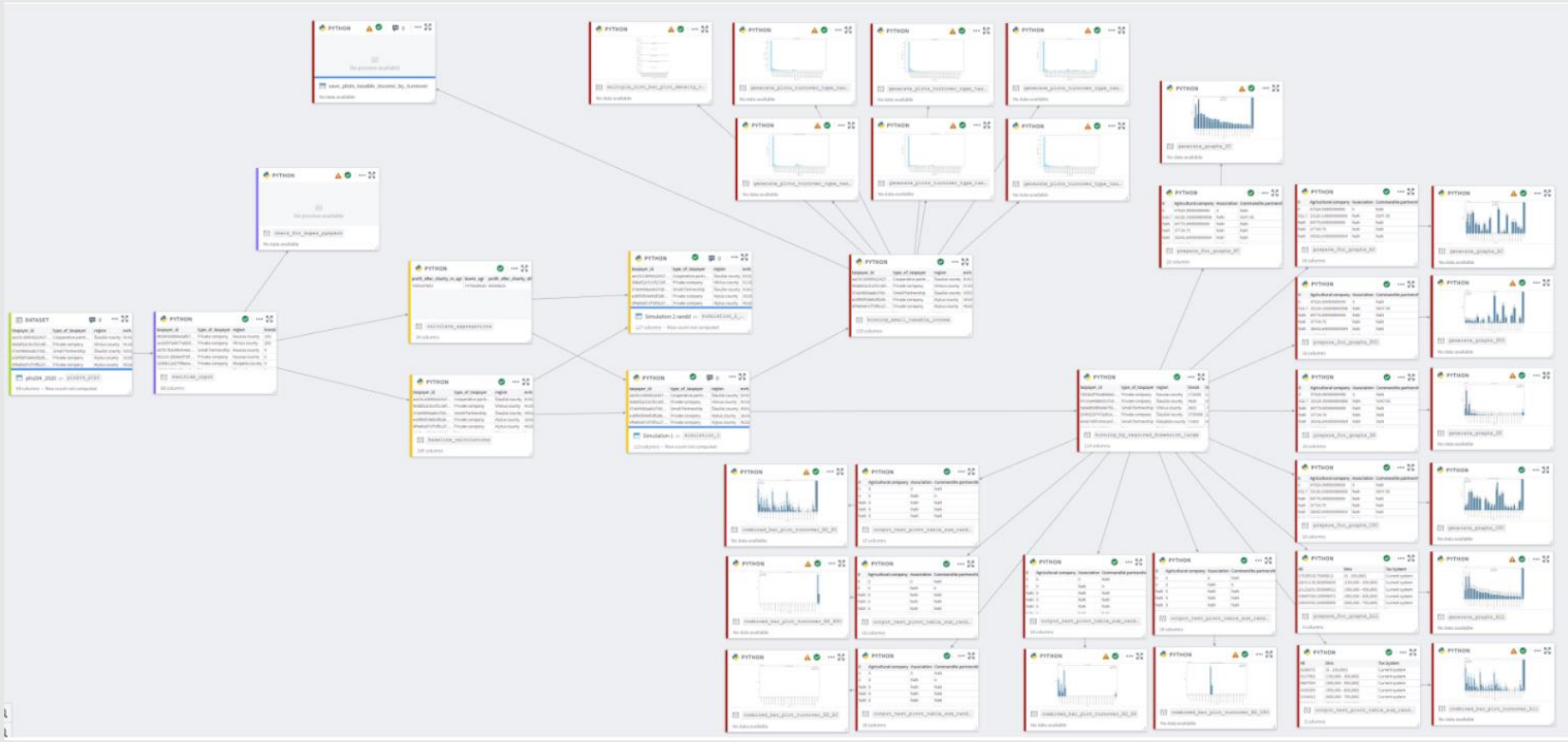
الاقتصاد والأعمال في لتوانيا – مثال (the dashboard)

- دمج البيانات الواردة من مختلف المؤسسات وإعداد المؤشرات
- Internal dashboards
- Public application
  - https://osp.stat.gov.lt/ev-dashboards

مثال - وحدات تحليلية لتقييم البيئة الخاضعة للضريبة للأفراد العاملين لحسابهم الخاص والشركات الصغيرة.

يوفر نظام المعلومات لدينا البيئات، حيث
و Rيمكن استخدام رمز
لإجراء تحليل Python
مختلف للبيانات.

Apache Spark is used as a main database engine.



السياق الأمني في نظام معلومات حوكمة البيانات في الدولة

- في العامين الماضيين، تم إنشاء نظام إيكولوجي راسخ وعامل لبيانات الدولة، مع التكامل مع أكثر من 40 نظامًا/موارد معلومات حكومية.
- وسيتم إدماج ما يقرب من 300 نظام/موارد إضافية في السنوات القادمة.
- يطور قسمنا أيضًا تطبيقات داخلية للبيانات التشغيلية و external public dashboards
- في الوقت الحالي، يوجد في نظام المعلومات لدينا ما يقرب من 2000 حساب للمستخدمين الداخليين والخارجيين، مع عدد من الأدوار والمسؤوليات
- Our developers and analysts use *git* repositories, code workbooks, various analysis tools. We use **Palantir Foundry** platform, which allows us to us Python and R programming languages, GIT repositories, Apache Spark data engine.

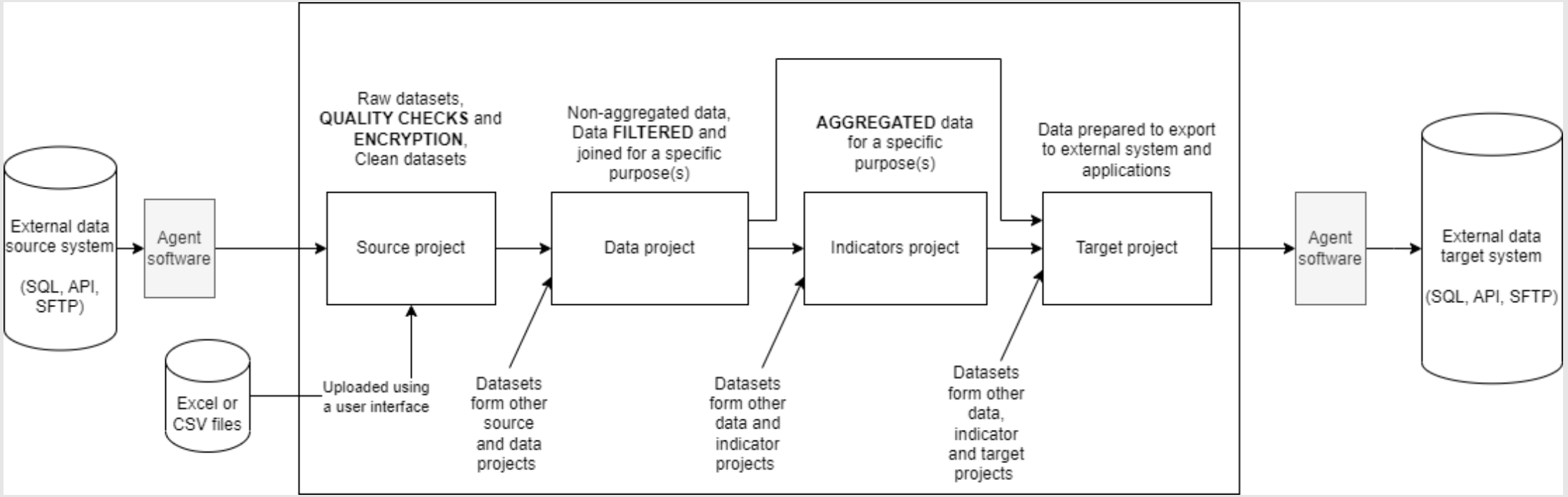
السياق الأمني في نظام معلومات حوكمة البيانات في الولاية

- يستوعب نظام المعلومات ويصدر بيانات من عدد كبير من مجموعات البيانات من منظمات أخرى.
- **تساعد حلول معالجة البيانات لدينا المنظمات، مثل البلديات أو المستشفيات، على اتخاذ قرارات تعتمد على البيانات.**
- البيانات من نظامنا منشورة على الويب.
- يتم تحويل العديد من مجموعات البيانات إلى بيانات مفتوحة.
- يتميز أمن المعلومات لدينا أيضًا بمشاريع sandboxحيث يمكن للمنظمات الأخرى إجراء تحليلها الخاص باستخدام البيانات والأدوات المتكاملة المتاحة داخل النظام.

نطاق نظام إدارة أمن المعلومات في قسم حوكمة بيانات الدولة

- هناك حاجة مستمرة إلى حلول أمنية قوية لتكنولوجيا المعلومات لتقليل المخاطر المتعلقة بما يلي:
  - عدد كبير من النظم غير المتجانسة
  - بيانات شخصية وصحية حساسة
  - عدد كبير نسبيا من المشاريع
  - عدد كبير نسبيا من المستخدمين
  - تعقيد معالجة البيانات
  - نفقات تجهيز البيانات بسبب كميات كبيرة من البيانات
  - مخاطر أخرى تتصل بتكنولوجيات المعلومات (web security, viruses, social engineering, physical security, etc.)

data pipelines النموذجي في نظام معلومات حوكمة البيانات في الدولة



القيادة والالتزام في قسمنا

- يلتزم الموظفون في قسمنا بنشاط بتطوير والحفاظ على عمليات آمنة لنظام المعلومات لدينا، لتقديم خدمات عالية الجودة للأطراف المهتمة.
  - لدينا اجتماعات أسبوعية للقسم حيث يناقش كبار المديرين والمتخصصين مواضيع مختلفة، بما في ذلك الموضوعات المتعلقة بأمن النظام وقوته، والتعامل مع المعلومات الشخصية، والموضوعات القانونية.
  - تقوم القيادات الفنية والإدارة في قسمنا جنبًا إلى جنب مع المتخصصين الأمنيين المتفانين بتطوير أمن المعلومات لدينا وتحسينه باستمرار.
  - يعمل شعبنا على تحسين الوعي الأمني بتكنولوجيا المعلومات، من خلال المشاركة في أنشطة التدريب والعمليات المتعلقة بالأمن، وكتابة الوثائق، والإبلاغ عن القضايا الأمنية والمشاركة في المناقشات حول مواضيع أمن تكنولوجيا المعلومات.

القيادة والالتزام في قسمنا

- قسم تكنولوجيا المعلومات لدينا لديه فريق دعم 24/7
- يطلعنا مطور أمن المعلومات ومزود الخدمة بنشاط على المشكلات الأمنية المهمة ويحسن النظام ويحدثه باستمرار. 24/7 الدعم متاح أيضا.
- في الوقت الحالي، لدينا في قسمنا 7 فرق تعقد اجتماعات مزامنة داخلية بضع مرات على الأقل في الأسبوع (أو كل يوم عند استخدام إدارة مشروع سكروم) واجتماعات أسبوعية لقائد الفريق. في تلك الاجتماعات، يمكن لأعضاء الفريق مناقشة المشاكل الرئيسية، بما في ذلك قضايا أمن تكنولوجيا المعلومات.

إجراءات لمعالجة المخاطر والفرص

- يتم معالجة المخاطر المرتبطة بنظام معلومات القسم الخاص بنا من قبل الموظفين المسؤولين داخل قسمنا، وإذا لزم الأمر، يتم تصعيدها إلى فريق أمن تكنولوجيا المعلومات داخل قسمنا وإلى مزود خدمة نظام المعلومات (IS).
- يقوم قسم تكنولوجيا المعلومات داخل قسمنا بتقييم المخاطر والفرص، وتحليل التقارير، والمشاركة بنشاط في التخطيط لحلول أمان تكنولوجيا المعلومات، مثل مشتريات البرامج والأجهزة وإجراءات الأمان الجديدة.
- يتم تقديم العديد من الاقتراحات المتعلقة بأمن تكنولوجيا المعلومات من قبل مطور ومزود خدمة IS. وتناقش هذه الاقتراحات وتدرج في خطط أمن تكنولوجيا المعلومات إذا لزم الأمر.

أهداف أمن المعلومات والتخطيط لتحقيقها

- هدفنا هو إنشاء حلول آمنة وموثوقة لإدارة بيانات الدولة والإحصاءات الرسمية
- يعتبر أمن تكنولوجيا المعلومات أولوية قصوى في مؤسستنا، ونحن ندمجها باستمرار في خططنا.
- لدى قسمنا اجتماعات تخطيط، ويتضمن متخصصو أمن تكنولوجيا المعلومات والإدارة تحسينات أمنية في خططنا.

الموارد المستخدمة

- تكفل مختلف الأطراف أمن تكنولوجيا المعلومات، بما في ذلك:
  - الإدارة
  - المحامون
  - IS administrators
  - data engineers and analysts
  - IT support team, including dedicated IT technology and communication security specialists
  - State Data Governance Information System service developer and provider
- الأدوات التنظيمية:
  - الوثائق القانونية
  - التوثيق والإجراءات الداخلية
  - المعلومات المتاحة عن سياسة أمن البيانات ومتطلبات أمنها، المقدمة على الموقع الشبكي لمنظمتنا
- Technical tools:
  - Regular IT tools, such as firewalls, antiviruses, tools for automatic software updates, server and personal computer security managements tools, personal computer and mobile phone security tools
  - Dedicated applications for project and data access rights management (developed by our engineers)
  - Incident reporting systems (Axence nVision, Palantir Foundry)
  - Tools for log analysis (ELK stack, FortiSIEM, etc.)
  - Automatic data scanning tools to identify sensitive data (provided by Palantir Foundry)

الدعم - الكفاءات

- فهم أهمية الأمن
- استخدام أفضل الممارسات في الترميز الآمن وتجهيز البيانات
- اتباع المبادئ التوجيهية العامة لأمن تكنولوجيا المعلومات
- Understanding physical security (such as clean desktop policy, physical access to the building, etc.)

الدعم – التوعية

- يتم تحقيق الوعي الأمني من خلال إعلام موظفينا ومستخدمينا بموضوعات أمنية مختلفة تتعلق بأنظمتنا وتقنيات المعلومات بشكل عام.
- يحصل موظفونا على تنبيهات عبر البريد الإلكتروني من قسم تكنولوجيا المعلومات ونظام المعلومات لدينا.
- يوفر المركز الوطني للأمن السيبراني لمنظمتنا مواد تدريبية، مثل الدورات التدريبية التفاعلية

الدعم - الاتصال

- لدى قسمنا أدوات للإبلاغ عن قضايا أمن تكنولوجيا المعلومات إلى الموارد المسؤولة في قسم تكنولوجيا المعلومات لدينا لاتخاذ مزيد من الإجراءات الفورية ((Axence nVision
- State Data Governance IS has tools to report issues to IS service provider for immediate further action (Palantir Foundry Amplify ticket system)
- IT division and IS service provider constantly notifies our employees on various IT security topics via e-mail messages containing security recommendations and/or reports, such as new security vulnerabilities
- Data pipeline developers can create alerts based on data health checks (Palantir Foundry)
- In urgent cases, IT security team or IS service provider can be contacted 24/7

الدعم - المعلومات الموثقة

- يغطي توثيق أمن المعلومات التي أنشأها المتخصصون لدينا الموضوعات المتعلقة بأمن البيانات و source codeمثل أدوار المستخدم وعلامات أمن البيانات والتفحص للبيانات وتشفير البيانات وتصديرها ومتانة data pipelineوغيرها من الموضوعات. ويجري تحسين هذه الوثائق باستمرار
- يتم توفير المبادئ التوجيهية لأمن تكنولوجيا المعلومات (مثل المبادئ التوجيهية لسلامة البيانات الشخصية، ودليل الترميز الآمن، وما إلى ذلك) من قبل مزود خدمة أمن المعلومات في وثائق المنتج ((Palantir Foundry
- دورات تدريبية تفاعلية عبر الإنترنت وأخبار أمنية وتقارير سنوية عن أمن تكنولوجيا المعلومات يقدمها المركز الوطني للأمن السيبراني على شبكة الإنترنت
- Our employees sign legal security documents when onboarding

عمليات التدقيق الداخلي والتدقيق

- يقوم قسمنا بإجراء عمليات تدقيق وتقييمات عشوائية ودورية وثابتة لأمن تكنولوجيا المعلومات (على سبيل المثال، التحقق النشط من بيانات المشروع وقيود الوصول إلى رمز المصدر، وإجراء مراجعات للرموز، وما إلى ذلك)
- لقد خصص قسمنا موظفين لتحليل سجل تدقيق نظام المعلومات في القسم
- يتم إجراء عمليات التدقيق الأمنية العامة من قبل إدارة تكنولوجيا المعلومات

تقييم الأداء

- تتم مراجعة نتائج عمليات تدقيق الأمن الداخلي وأي حوادث أمنية من قبل متخصصين مسؤولين في أمن تكنولوجيا المعلومات والتكنولوجيا. القائد والإدارة و IS service provider
- نخطط باستمرار ونتخذ الإجراءات المناسبة لتقليل عدد الحوادث الأمنية وتقليل المخاطر الأمنية في إدارتنا

نحن ممتنون لإتاحة الفرصة لنا للمشاركة في مشروع التوأمة، ونأمل أن تعزز هذه المهمة أمن تكنولوجيا المعلومات في منظماتنا.