ПРЕПОРАКА 3

Зголемување на безбедноста, безбедноста и зајакнувањето на поединците, транспарентноста на личните податоци и вештачката интелигенција.

Владините институции честопати користат лични податоци на граѓаните (адреса, датум на раѓање итн.) за да им овозможат одредени услуги. Јавната администрација често поседува лични (вклучувајќи чувствителни) информации за корисниците во текот на целиот животен циклус на обезбедување на услугата. Овие податоци може да бидат чувани од надлежните институции и да се користат за обработка за цели на обезбедување други услуги. Затоа, владата има законска должност да ги заштити овие информации во согласност со регулативата за заштита на личните податоците. Неисполнувањето на оваа обврска би ја поткопало довербата на јавноста во владините служби.

Со оглед на тоа што личните податоци најчесто се собираат за време на обезбедувањето на јавните услуги (адреси, датуми на раѓање, итн.), од суштинско значење е граѓаните да можат да ги дадат овие лични податоци во безбедна средина, без да стравуваат дека трети страни биле во можност недозволено да пристапат до нив. Тимовите за управување со ризиците потребно е да обезбедат дека јавните е-услуги ги исполнуваат безбедносните барања и прописи, без да го загрозат давањето на јавните дигитални услуги. Во оваа насока, заканите за безбедноста и приватноста, исто така, треба активно да се идентификуваат, а притоа да се применува сеопфатен и пропорционален пристап за обезбедување информации и управување со ризиците од измама. Безбедноста на владините веб-страници претставува се посериозна грижа за граѓаните.

Од владите се очекува да ги заштитат интересите на граѓаните од нарушување на безбедноста на личните податоци и заканите за напади во дигиталниот простор (сајбер безбедноста). Затоа, изборот на соодветна технологија е значајна инвестиција не само за јавната или локалната институција како надлежна за обезбедување на услугата, туку и за корисниците бидејќи тие се и субјекти кои ќе учат и ќе постапат според понудените технолошки можности. Во оваа насока, јавната или локалната институција ќе има огромно влијание врз можноста за креирање, обезбедување и повторување на услугата на одржлив начин. Потенцијалното користење на вештачката интелигенција, пак, значи дека владите мора внимателно да ги разгледаат и да ги решат потенцијалните ризици од имплементацијата на технологијата за вештачка интелигенција при обезбедувањето на јавните дигитални услуги.

Клучни зборови: дигитални услуги, граѓани, дигитална сигурност, диготални права.
Оваа публикација е развиена со поддршка на програмата Механизам за граѓанска отпорност, финансирана од Европската Унија. Нејзината содржина е единствена одговорност на авторите и не мора да ги одразува ставовите на Европската унија.

Цели

Целта на предложената политика за зголемување на безбедноста, безбедноста и зајакнувањето на поединците, транспарентноста на личните податоци и вештачката интелигенција е следна.

Зголемување на безбедноста, сигурноста и зајакнувањето на поединците

• Обезбедувањето на дигитални услуги потребно е да биде сигурно и безбедно за секого (најмалку следните аспекти би требало да бидат опфатени со проценката: политика за безбедност на содржината, колачиња, споделување ресурси со вкрстено потекло, прикачување на јавниот клуч HTTP, строга безбедност на транспортот HTTP, пренасочување, политика за упатување, интегритет на под-ресурс, X-содржина-тип-опции, X-Frame-опции и X-XXS-заштита и сл). Притоа, eID игра клучна улога, исто како и дигиталните решенија;
•Подобрување на безбедноста на веб-страниците преку искористување на алатките за тестирање со отворен код и имплементација на мерки за следење;
Предвидување на безбедноста преку дизајн и приоритет на буџетирањето за да се инвестира повеќе во софистициран план за дигитална (сајбер) безбедност;
• Промовирање на одржливоста на дигиталната иднина (придобивки во други области)

Транспарентност и обезбедување заштита на личните податоци на корисниците

• Со интелигентно споделување и повторна употреба на лични податоци, владата ќе биде во можност да испорачува услуги, пред корисникот да има потреба да ги побара (на пр. детски додаток кој може да се обезбеди проактивно на младите родители кои неодамна добиле бебе и соодветно го евидентирале)

Придобивките од користењето на вештачката интелигенција

• Со персонализирани, предвидливи и превентивни јавни услуги во различни области како што се образование, планирање на транспортот и гаснење пожари, подобрите резултати може да имаат економски мултипликатор: тие не само што заштедуваат директно средства, туку владата исто така може да овозможи поголема продуктивност за граѓаните и компаниите (На пример, моделот на вештачка интелигенција што се користи за дистрибуција на социјалните бенефиции мора темелно да се провери во поглед на вградени предрасуди против одредени сегменти од општеството.)

Предизвици

Потребата од овие мерки произлегува од неколку предизвици.
Отворените стандарди им помагаат на услугите да функционираат со тоа што трошат помалку време, обидувајќи се да воспостават “комуникација“ помеѓу различни сервисни системи. Употребата на заеднички компоненти и обрасци значи дека оние кои се генерално тестирани, давателите на услуги можат да им обезбедат на корисниците добро искуство, на рентабилен начин. Ако давателите на услуги развијат свои

компоненти или модели, тие треба да ги споделат така што другите даватели на услуги во рамки на државната власт, ќе можат да го користат нивното искуство. Стандардните владини компоненти (со можност за споделување информации за нови компоненти или тенденции што тие ги создаваат или прилагодуваат), на пример, онаа достапна на порталот uslugi.gov.mk, треба да се користат како добро искуство од други државни или локални органи кои би сакале да обезбедат дигитални јавни услуги, во насока на заштеда на нивните ограничени ресурси. Во оваа линија, користење и креирање на интерфејс за програмирање на апликации (API) и, каде што е можно, сигурен извор на податоци, како што се официјалните регистри, исто така треба да се користат, во насока на зголемување на квалитетот на јавната дигитална услуга.

Притоа, се препорачува да се користи сеопфатен и пропорционален пристап во обезбедувањето информации и управувањето со ризикот од сајбер и измами при идентификување на заканите за безбедноста и приватноста. Дополнително, безбедноста на јавната дигитална средина во споредба со приватната сè уште е отворено прашање, предмет на понатамошна регулација и во ЕУ.

Исто така, Владата може да ја искористи моќта на вештачката интелигенција преку персонализирани услуги и автоматизирани процеси. Вештачката интелигенција може да придонесе за подобрување на квалитетот на животот во сите сегменти на општеството, преку воведување на иновации како што се предвидувачка здравствена заштита, адаптивното образование и оптимизиран одговор на кризи.

Во оваа насока, од Владата се очекува да го отвори патот за искористување на потенцијалот на вештачката интелигенција, да спроведе соодветна едукација за потенцијалот на вештачката интелигенција, да ги идентификува можностите и да го поддржи усвојувањето на технологии за вештачка интелигенција на етички и безбеден начин кој ги опфаќа ризиците од овие технологии. Но, владата не може сама да го направи тоа. Истражувачките институции и универзитетите, на пример, може да го водат тестирањето и развојот на нови алгоритми за вештачка интелигенција и да ги направат нивните решенија достапни за комерцијализација. Тие, исто така, можат да соработуваат со владини ентитети за да го поддржат развојот на сеопфатен сет на политики и упатства за организациите, во насока на обезбедување на сигурна, одговорна и етичка употреба на вештачката интелигенција во технологиите што ги развиваат и применуваат. Граѓаните можат да бидат катализатори на овие промени, во насока на испорака на поквалитетни, побрзи и персонализирани услуги од субјектите од јавниот и приватниот сектор; тие исто така можат да бидат гласноговорници за приватноста, безбедноста и етичките ризици поврзани со вештачката интелигенција. Доколку се пристапи внимателно, земајќи ги предвид уникатните предизвици, вештачката интелигенција суштински би влијаела на трансформацијата и би и помогнала на

Република С. Македонија да ја искористи економската вредност на вештачката интелигенција.

Целна група

Целната група за зголемување на сигурноста и безбедноста на дигиталниот јавен простор, притоа обезбедувајќи транспарентност и заштита на личните податоци (особено во однос на чувствителните податоци), како и користењето на предностите на вештачката интелигенција во зголемувањето на нивото на квалитет на дигиталните јавни услуги, првенствено ги вклучува:

-Министерство за информатичко општество и администрација (подоцна: Агенција за безбедност на мрежни системи и информациски системи и дигитална трансформација), и други релевантни јавни органи кои се одговорни за обезбедување подобар квалитет на јавните е-услуги во Северна Македонија и користат владина платформа за интероперабилност;
- Граѓаните како секундарна група, бидејќи се ставени во центарот на дигиталната трансформација и подоброто искуство на клиентите преку проширување и обезбедување подобар квалитет на јавните дигитални услуги, ќе овозможат уживање на човекови права во процесот на дигитална трансформација.

Институција која ја развива мерката

Одговорно тело: Владата на Република Северна Македонија главно преку Националниот совет за дигитална трансформација на општеството и Министерството за информатичко општество и администрација (подоцна: Агенција за безбедност на мрежни системи и информациски системи и дигитална трансформација), како и универзитети, истражувачки институти, деловни комори, и други релевантни тела (Национален центар за интернет безбедност итн.), се органите кои треба да бидат одговорни за зголемување на безбедноста, безбедноста и зајакнувањето на бизнисите, транспарентноста на личните податоци и вештачката интелигенција.

Имплементација

Процесот на имплементација се состои од неколку чекори:

Препорака 1: Дополнителен развој на законодавството во областа на безбедност, сигурност и зајакнување на деловните субјекти

Владата преку релевантните министерства ќе соработува со експерти, засегнати страни и други релевантни страни, со цел понатамошно развивање на детална правна рамка за подобра организациска, институционална и техничка средина (Концептот на дигитална трансформација на општеството, Национална стратегија за реформа на јавната администрација 2023- 2030 година, Национална ИКТ

стратегија за Северна Македонија 2023-2027 година, Национален оперативен план за широкопојасен интернет (2019 – 2029 година), Национална стратегија за вештачка интелигенција во Република Северна Македонија и друга релевантна регулатива во областа на заштитата на податоците и сајбер безбедноста итн).

Во развојот на политиката, очекувањата на корисниците потребно е да бидат ставени во фокусот. Во оваа насока, секоја јавна институција вклучена во процесот треба да управува со очекувањата на корисниците во однос на дигиталните јавни услуги. Ова би ги опфатило следните аспекти:

Транспарентност и заштита на лични податоци

- Нивото на дигитален пристап на корисниците до нивните лични податоци (нема пристап; се даваат информации за пристап до сопствените податоци преку офлајн канали; податоци достапни на барање и проактивно информирани од владата за тоа кои податоци се чуваат);
- Степенот до кој корисниците можат да ги менуваат и следат нивните лични податоци преку најрелевантните владини веб-портали;
- Можност за следење на субјектот на личните податоци кој имал пристап до нив и за каква.

Потребно е да се развие детален ИКТ стратешки документ, со вклучување на различни засегнати страни, и што е најважно да биде навремено донесена и имплементирана. Оваа национална стратегија треба да вклучува проценка на квалитетот на јавните услуги за граѓаните, за да се осигура дека тие го поседуваат посакуваното ниво на квалитет и да се обезбедат потребните услови за активно учество на граѓаните. Врз основа на заклучокот од оценката, треба да се донесе соодветна законска регулатива, како и други релевантни пропратни документи за спроведување, следење и мерење на имплементацијата.

По формирањето на релевантна јавна институција - Агенција за безбедност на мрежни системи и информациски системи и дигитална трансформација, Агенцијата ќе ги спроведува координирањето, поддршката и следењето на горенаведените активности. За време на имплементацијата, треба да се воспостават соодветни механизми за следење и известување, преку оваа релевантна институција за координација на активностите на различни јавни институции и локалната самоуправа, додека Министерството за финансии би обезбедило соодветна буџетска распределба (доколку е потребно).

Употреба на вештачка интелигенција

Сајбер безбедноста во дигиталната ера е значаен проблем. Зголемениот пристап до интернет создава потреба од стратегија за сајбер безбедност. Стратегијата има за цел да изгради капацитет, да ги заштити критичните информациски системи и да обезбеди едукација и свест за сајбер безбедноста. Главниот предизвик е дефинирање на акциони планови и управувачка структура за успешна имплементација на стратегијата, која би обезбедила безбедна онлајн средина.

Заложбите на државата за дигиталниот сектор и безбедноста на податоците, пред се за подобрување на услугите и заштита на информациите во дигиталниот свет. Овие напори треба да се синхронизираат со меѓународните стандарди за дигитален идентитет и сајбер безбедност, со цел да се изгради напредна и безбедна дигитална средина во земјата. Во оваа насока, добра практика од различни земји може да користи Владата за различни услуги за животни настани (здравство, транспорт и сл.). Националната здравствена служба во Обединетото Кралство, на пример, формираше Национална база на податоци за сликање на градниот кош COVID-19 која содржи заедничка библиотека со рендгенски снимки на граден кош, КТ скенови и слики со МРИ за да го поддржи тестирањето и развојот на технологии за вештачка интелигенција за лекување на КОВИД. -19 и разни други здравствени состојби. Сингапур го воведе „Прашај го Џејми“, виртуелен асистент кој им помага на граѓаните и бизнисите да се движат низ владините услуги низ околу 70 владини агенции преку разговор и глас со ВИ. Воведе и Владата на Северна Македонија, а беше формирана работна група со цел да се создаде првата Национална стратегија за вештачка интелигенција во Република Северна Македонија. Стратегијата е дел од планот за економски развој на Република Северна Македонија и дел од Националната стратегија за развој 2021-2041 година. Понатамошните активности во однос на вештачката интелигенција треба да се интензивираат во однос на усвојување на дополнителна релевантна регулатива за употреба на вештачка интелигенција бидејќи таа го изложува бизнисот на ризик од злоупотреба, па Владата мора да ги заштити бизнисите, како и да управува со прашањата за приватност. , безбедност, правичност, надзор, принцип заснован на ризик, безбедност и перформанси, транспарентност, одговорност и човекови права, како главни етички предизвици во развојот на системи управувани од вештачка интелигенција.

Препорака 2: Усвојување методологија за оцена на квалитетот на јавните е-услуги

Потребно е да се подготви методологија за проценка на квалитетот на дигиталните јавни услуги (национални и прекугранични) наменети за граѓаните кои се нудат од страна на државните власти, кои ќе ги вклучи и сајбер и безбедносните ризици. Целта е да се осигура дека овие услуги го поседуваат посакуваното ниво на квалитет и обезбедени се потребните услови за активно учество на граѓаните. Врз основа на заклучокот од оценката, треба да се пристапи кон понатамошно доуредување на законската регулатива, согласно потребите.

Препорака 3: Создавање на релевантна институција за кибер безбедност

Потребно да се формира Национален центар за интернет безбедност, под капата на Министерството за информатичко општество и администрација или како независно тело, одговорно во полето на кибер безбедноста.

Засегнати страни и партнери

Успешната имплементација на мерката ќе бара соработка со различни засегнати страни и партнери, за да бидат вклучени во спроведувањето на мерката. Дополнителни организации и засегнати страни кои можат да бидат вклучени во спроведувањето на мерката, исто така, ќе опфатат:

- Јавни/државни институции кои обезбедуваат е-услуги на национално и локално ниво;
- Граѓаните како сегашни и потенцијални корисници на е-услугите;
- Локални граѓански организации и локални медиуми.

Клучни индикатори за успешност

Клучни индикатори за успешност кои можат да се користат за мерење на успехот се:

• Ниво на задоволство на граѓаните во однос на степенот на можноста да ја извести владата за неточни лични податоци или да ја процени усогласената процедура за информирање на владата за нивното незадоволство од тоа како владата ги користи нивните податоци;

• Статистика на спроведените мерки преку мониторинг и евалуација на индикаторите за успешност пропишани со релевантна документација, во однос на безбедноста на дигиталниот јавен простор и правото на заштита на личните податоци (проценка, измена и следење), како и потенцијалното влијание врз употребата на вештачката интелигенција.

Влијание

Мерката резултира со зајакнување на положбата на граѓаните во центарот на дигиталната трансформација и негување на нивните дигитални права, преку постојано зголемување на квалитетот на јавните е-услуги за граѓаните:

• Обезбедување безбеден јавен дигитален простор во согласност со релеватната регулатива;

• Тимовите за управување со ризици потребно е да обезбедат дека јавните дигитални услуги ги исполнуваат безбедносните барања и се усогласени со релевантната регулатива, без да го загрозат обезбедувањето на услугата;

• Натамошно усогласување на националното со законодавството на ЕУ во областа на електронските комуникации, широкопојасен интернет, мрежна безбедност и информациски системи, архивско и документарно работење итн.;

• Активно идентификување на заканите за безбедноста и приватноста на јавната дигитална услуга и спроведување сеопфатен и пропорционален пристап за обезбедување информации и управување со ризикот од измама;

• Собирање и обработка на личните информации на корисниците на начин кој е безбеден и ја почитува нивната приватност;

• Поддржан понатамошен развој и имплементација на регулаторни рамки за заштита на податоците, што вклучува регулирање на тоа како јавните институции ги складираат и користат личните податоци на луѓето во дигиталниот простор и нивното право да ги менуваат овие податоци;

• Обезбедување на соодветно тестирање за ранливост и пенетрација;
• Користење на специфичен пристап во електронската идентификација и верификација на балансирање на ризиците на пропорционален начин (за оние дигитални е-услуги кои бараат идентификација или проверка);
• Креирање план и обезбедување на потребни ресурси кои овозможуваат безбедносно управување, за време на траењето на оваа дигитална е-услуга (на пример, со одговор на нови закани, воведување контролни механизми и примена на софтверски безбедносни закрпи);
• Информирање и подигање на свеста кај корисниците за политиката за заштита на приватноста;
• Следење на техничките мерки за заштита на приватните податоци регулирано со пропис;
• Обезбедување дека секој нов изворен код е отворен и може повторно да се употребува, а во исто време да биде објавен во согласност со соодветни лиценци и зачувување на интелектуалната сопственост (ако не е можно одредено подмножество од изворниот код да биде објавено поради чувствителни владините политики, тие треба да бидат наведени како такви);
• Обезбедување дека давателот на услуги треба да може редовно да прави промени на софтверот, без поголем период на недостапност на услугата поради овие ажурирања;
• Редовно тестирање на квалитетот и тестирање на услуги во средина слична како онаа во реалноста;
• Постоење на соодветен мониторинг и одржлив план за одговор на проблемите кои се утврдено со таквиот мониторинг;
• Корекција на можни договорни или организациски проблеми кои се пречка за достапност на услугата (на пример, договор за заедничка терминологија, алатки, начин на работа на техничарите, оддел за поддршка и сл.)

Добра практика

Купување (повлекување) сметки и изводи преку Интернет, низ целиот свет (Ирска)

Овој пример е убава илустрација за тоа како може да се користи новата технологија (интернет) за да се обезбеди подобар квалитет и зголемена достапност на услугите за издавање јавни сертификати и извори во Ирска. Може да биде корисно и за други стандарди.

Веб-страницата www.certificates.ie е развиена како паметен начин да им овозможи на клиентите да купуваат сертификати и изјави за настани во животот (извод од матична книга на родени, посвојување, брак, смрт, а од неодамна и потврди за брак) преку Интернет, од кое било место во Ирска или во странство. Тоа е нов и иновативен начин на обезбедување на услугата, што доведе до вистинска заштеда, во однос на користењето на интернет решение, како и можност за преиспитување на сегашниот модел на работа, како и креирање и имплементирање на нови процеси кои ја зголемуваат ефикасноста. Ваквиот пристап на Владата беше предводен од Службата за водење на матични книги во источниот дел на земјата (CRS-ERA), во име на Националната служба за регистри (CRS) и Генералниот регистар на граѓани

(GRO), користејќи сопствени информациски ресурси.
Веб-страницата беше лансирана во ноември 2019 година, а до крајот на 2010 година, околу 5% од сите потврди беа издадени онлајн. Истовремено, времето на чекање е намалено на помалку од 5 работни дена од страна на 92% корисници (кои не биле физички присутни, односно кои поднеле барање преку Интернет, телефон или пошта).
Претходно, за да добиете сертификат, требаше да дојдете лично, да испратите пополнет формулар онлајн, заедно со повратна поштарина или во последно време да аплицирате телефонски преку кредитна или дебитна картичка.
Пред да се воведе оваа интернет-страница, телефонските прашања покажаа дека клиентите го поздравуваат пристапот да не мора да доаѓаат лично за да ги добијат сертификатите или изјавите.
Работата преку Интернет доведе до заштеда на државата - потреба од интервенции од вработените затоа што сега самите клиенти ги внесуваат сите детали во барањето, а го намалуваат користењето на готовина преку безбеден финансиски систем кој ги намалува административните трошоци. Во ситуација на ограничена достапност на надворешни ресурси, потребен беше иновативен пристап, со цел да се намалат трошоците и благодарение на партнерскиот пристап, страницата беше развиена од внатрешен проектен тим во кој соработуваа секторот за информатика и вработените од матичните служби. Ова се предностите на овој пристап:
• Подобрено корисничко искуство;
• Поголема моќ на граѓанинот;
• Можност граѓаните да нарачуваат изјави и потврди од удобноста на нивниот дом или од кое било место, од каде што имаат пристап до интернет;
• Поефикасно користење на времето на вработените - можност за подобро управување со обемот на работа, намалување на потребата од канцеларии, подобрено корисничко искуство. Сето ова беше заеднички партнерски пристап со други државни агенции кои беа во корист и на државата и на граѓаните, благодарение на користењето на интернет технологијата и нејзината примена.

Извор: Квалитет на јавната администрација - Лента со алатки за практичари, издание 2017 година (скратена верзија)

Заштита на приватноста и податоците и ориентација на јавната администрација кон граѓаните (Италија)

Јавната администрација мора да обезбеди имплементација на директивите на ЕУ, особено оние кои се однесуваат на приватноста, пристапот, транспарентноста и заштитата на личните податоци. Посебен случај се здравствените услуги, иако во денешно време технологијата нуди широк спектар на алатки кои овозможуваат автоматско ракување со чувствителни податоци. Во овој случај, важно е меѓусебно поврзување на базите кои имаат податоци за здравствената заштита, за да се обезбеди најдобра здравствена заштита.
Италијанските јавни служби ги прегледаа своите внатрешни процедури,

за оние кои често не сакаат да понудат дигитални услуги на граѓаните. Проблемот е решен со примена на нов систем кој гарантира ракување со чувствителните податоци, на ист начин како што се гарантира приватноста на граѓаните. Беше развиен нов модел и беше дизајнирана политика за приватност. Формирана е посебна канцеларија за справување со критичните прашања што требаше да се решат во врска со обработката на личните податоци. Овој модел го овозможува следново:

• Системот за квалитет на приватност на институцијата треба да биде опремен со систем за поттикнување на управувањето кој е поврзан со внатрешната контрола на квалитетот, поставувајќи годишни цели за да се обезбеди приватност која, доколку не се почитува, влијае на распределбата на економските резултати;

• создавање мрежа на вработени за да се обезбеди усогласеност со правилата за приватност во одделот на секоја организација, во соработка со националната Агенција за заштита на лични податоци и преку разгледување на внатрешните процеси за управување со податоци;

• поголемо знаење меѓу операторите, подобрување на нивните вештини и ставови кон грижата и заштитата на корисниците;

• лансирање на иновативна комуникациска кампања која ќе бара учество на клиентите, за да се обезбеди максимален резултат од веќе донесените мерки, зголемување на еманципацијата и односите

Извор: Квалитет на јавната администрација - Лента со алатки за практичари, издание 2017 година (скратена верзија)

Белгија/ Datavindplaats (Пронаоѓач на податоци)

Релевантни клучни димензии (и): Транспарентност, Клучни овозможувачи Животен настан: Редовно деловно работење, транспорт, здравје, започнување бизнис, студирање, кариера

1. Опис на добра практика:

Datavindplaats (местото за наоѓање податоци), е првата иницијатива која комбинира геопросторни, „отворени“ и „затворени“ податоци и API во еден многу лесен портал за корисниците. Надминувањето на јазот помеѓу потребните стандарди ја подобрува размената на податоци, го намалува и поедноставува одржувањето, ја зголемува ефикасноста и конзистентноста и го одржува колку е можно поедноставно за давателите на податоци да ги обезбедат нивните податоци само еднаш, притоа допирајќи до најширокатa можна публика. Метаподатоците прикажани во Datavindplaats се засноваат на чадор концептот на консолидиран стандард, изоставувајќи многу концепти специфични за конкретен домен, така што корисничкиот интерфејс може да остане едноставен, јасен, лесен за користење и посакуван. На овој начин Datavindplaats станува олеснувач за следната генерација на решенија за податоци за повторно употребување.

2. Придобивки

• Заштедено време поради тоа што треба да пребарувате само еден портал за

податоците или API што му се потребни на корисникот
• Заштедено време со прикажување на сложени детали на начин попријатен за корисниците
• За добавувачи на податоци: само едно место каде што треба да ги опишат збирките на податоци и само еден каталог за кој треба да ја одржуваат содржината.

3. Клучни фактори за успех
• Успешно надминат семантичкиот јаз помеѓу различните домени што е прв во светот;
• Консолидирани постоечки каталози на збирки на податоци и овозможен увид во сите API што не биле присутни во ниту еден постоечки каталог
• Трансформирани информациите од техничкиот домен во почитлив формат, читлив за корисници кои не се умешни во дадениот домен.

Преносливост

Нема конкретни предизвици или ограничувања кои би можеле да ја попречат преносливоста на горенаведените примери во Северна Македонија