МЕТОДОЛОГИЈА ЗА ПРОЦЕНКА НА УСОГЛАСЕНОСТА НА ДИГИТАЛНИ ВЛАДИНИ УСЛУГИ СО ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Март 2022

METAMORPHOSIS
Foundation for Internet and Society

ABA AMERICAN BAR ASSOCIATION
Rule of Law Initiative

Автори: Елена Стојановска и Арбен Гудачи

Оваа публикација е подготвена во рамки на проектот „Техничка и интегрирана заштита на лични податоци-градење инклузивен дигитален екосистем“, поддржан од ABA ROLI, а спроведуван од Фондација Метаморфозис. Содржината од оваа публикација е единствена одговорност на Фондација Метаморфозис и авторите и на ниеден начин не ги одразува ставовите на АБА РОЛИ.

Содржина

1. Значењето на процесот на дигитализација на услугите на владините институции

Процесот на дигитализација е од исклучителна важност од повеќе аспекти како што се обезбедување на квалитетни дигитални услуги, зголемување на транспарентноста на институциите, олеснување на пристапот до услугите од страна на граѓаните, кратење на времето во кое граѓаните можат да ги добијат услугите од страна на институциите.

Дигиталната агенда е на приоритетно место на Владата на Република Северна Македонија. Стратешкиот развој може да се потврди со низата на стратегии и акциски планови во областа на дигитализацијата како што се:

- Национална стратегија за одржлив развој во РМ 2009-2030
- Национална стратегија за развој на информатичкото општество
- Стратегија за спроведување на правото на заштита на личните податоци 2017-2022
- Национална стратегија за сајбер безбедност на РМ 2018-2022
- Стратегија за транспарентност на Владата на РСМ 2019-2021
- Национален оперативен план за широкопојасен интернет 2019-2029
- Програма за работа на Владата на Република Северна Македонија за периодот 2022-2024.

Дел од стратегиите се тесно поврзани со спроведувањето на Дигиталната агенда за Западен Балкан кој беше донесена во 2018 година како дел од стратегијата на ЕУ за проширување во регионот. Главни области на оваа агенда се намалување на трошоците на роамингот, широкопојасниот интернет, развојот на е-влада, е-набавки, е-здравство и дигитални вештини, градењето капацитети во дигиталната доверба и безбедност паралелно со напорите за подобрување на дигитализацијата на индустриите и донесување, спроведување и јакнење на “acquis“ системот.

Во декември 2019 година од страна на Министерството за информатичко општество и администрација беше промовиран Националниот портал за услуги uslugi.gov.mk, каде на едно место може да се најдат информации за услугите кои ги нудат државните институции, вклучително и сите електронски услуги кои се обезбедуваат за граѓаните и бизнисите.

Во 2020 година, Министерството за информатичко општество и администрација потпиша договор за пристапување на Република Северна Македонија кон програмата за дигитална администрација-ИСА2 на Европската Унија. Станува збор за централна програма на Европската Унија која поддржува активности за развој на ИКТ во јавната администрација, давање електронски услуги, и генерално дигитализација во јавниот сектор. По завршувањето на оваа програма, очекувано е истата да се трансформира

во уште поголема програма именувана Digital Europe, која ќе се занимава со идните стандарди и насоки за развој на дигиталната агенда, а Република Северна Македонија активно ќе учествува во дефинирањето на идните решенија и стандарди.

Овој извештај дава преглед на услугите кои владините институции ги имаат дигитализирано и оние кои планираат да ги дигитализираат во текот на 2022 година. Врз основа на овој извештај, како и на релевантните законски прописи и подзаконски акти од Агенцијата за заштита на личните податоци[1], направена е и Методологија за оценување на усогласеноста на обезбедувањето дигитални услуги од страна на владините институции во Северна Македонија со Законот за заштита на лични податоци.

2. Методологија за оценување на усогласеноста на обезбедувањето дигитални услуги од страна на владините институции во Северна Македонија со Законот за заштита на лични податоци

Главната цел на истражувањето е да се процени нивото на усогласеност на процесот на дигитализирање на услугите, но и на функционалноста на самите дигитални услуги или алатки со Законот за заштита на личните податоци[2].

Согласно Законот за заштита на личните податоци, институциите се контролори на збирки на лични податоци и треба да го усогласат своето работење со одредбите на законот преку воспоставување на систем за безбедност и заштита на личните податоци. Системот за безбедност и заштита на личните податоци треба детално да ги дефинира збирките за заштита на личните податоци, техничките и организациските мерки за заштита на личните податоци, овластувањата на лицата кои вршат обработка на лични податоци, односите со трети страни кои во име и за сметка на институцијата обработуваат или користат лични податоци кои првично биле обработени од самата институција. Системот за безбедност и заштита на личните податоци задолжително треба да го дефинира и начинот на кој граѓаните – субјекти на личните податоци можат да ги остварат своите права кои произлегуваат од законот.

1 Закон за заштита на личните податоци
Правилник за безбедност на обработката на личните податоци
Правилник за процесот на проценка на влијанието на заштитата на личните податоци
Листа на операции за кои се бара проценка на влијанието на заштитата на личните податоци
Листа на операции за кои не се бара проценка на влијанието на заштитата на личните податоци
Правилник за начинот на известување за операции со висок ризик

2 **„Личен податок"** е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува (субјект на лични податоци), а физичко лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на идентификатор како што се име и презиме, матичен број на граѓанинот, податоци за локација, идентификатор преку интернет, или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, генетски, ментален, економски, културен или социјален идентитет на тоа физичко лице.

Во процесот на усогласување, секоја институција треба првично да тргне од проценка на тоа дали ги исполнува начелата за обработка на личните податоци кои се јасно дефинирани во Законот за заштита на личните податоци.

- **„законитост, правичност и транспарентност“** – личните податоци се обработуваат во согласност со закон, во доволна мера и на транспарентен начин
- **„ограничување на целите“** – личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели
- **„минимален обем на податоци“** – личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат
- **„точност“** – личните податоци точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени
- **„ограничување на рокот на чување“** – личните податоци се чувани во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци
- **„интегритет и доверливост“** – личните податоци се обработени на начин кој обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки
- **„отчетност“** - контролорот е одговорен за усогласеноста со Законот за заштита на личните податоци, при што е должен да ја демонстрира усогласеноста

Трендот на дигитализација на услуги кои институциите им ги нудат на граѓаните е во постојан раст. Дел од факторите кои влијаат за се поголемиот број на дигитални услуги се зголемената достапност и се почестото користење на интернетот од страна на граѓаните, потребата за транспарентност и отчетност на институциите, вклучувањето на Република Северна Македонија кон програмата на Европската унија за дигитализација на администрацијата. Од март 2020 година, живеењето и функционирањето во време на пандемија ја наметна потребата за надградување на дел од постоечките дигитални услуги како и развој на сосем нови дигитални услуги насочени токму кон олеснување на комуникацијата помеѓу граѓаните и институциите.

Еден од клучните аспекти во воведувањето на квалитетни дигитални услуги од страна на институциите е уредувањето на заштитата над обработката[3] на личните податоци на граѓаните кои ги користат тие услуги. Различни институции нудат различни

3 **„Обработка на личните податоци“** е секоја операција или збир на операции кои се извршуваат врз личните податоци, или група на лични податоци, автоматски или на друг начин, како што се: собирање, евидентирање, организирање, структурирање, чување, приспособување или промена, повлекување, консултирање, увид, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, усогласување или комбинирање, ограничување, бришење или уништување.

видови на дигитални услуги и канали за комуникација со граѓаните па со самото тоа изнаоѓањето на различни модели на системи за заштита и безбедност на личните податоци е неопходно.

Проценката на усогласеноста на постоечките дигитални услуги и на услугите кои владините институции планираат да ги дигитализираат во текот на 2022 година ќе се направи во три дела, односно преку: **1. дефинирање на дигиталните услуги и нивната достапност, 2. оценка на транспарентноста на обработката на личните податоци и 3. оценка на предвидените технички и организациски мерки за заштита на личните податоци.**

2.1. Дефинирање на дигиталните услуги и нивната достапност

Во првиот дел ќе се анализира на кој начин се дефинирани дигиталните услуги, која институција ги обезбедува, односно се јавува во улога на контролор[4] на лични податоци кои се обработуваат при користењето на дигиталната услуга и на кој начин се истите достапни до граѓаните.

Согласно Законот за заштита на личните податоци, личните податоци се собираат и обработуваат исклучиво за целите дефинирани во релевантен закон, договор или согласност на субјектот на личните податоци.

Еден дел од дигиталните услуги претставуваат алтернативен (електронски) начин за добивање на услугата. Овие услуги се поврзани со права на граѓаните кои произлегуваат од секторските закони со кои е јасно пропишана и процедурата за нивно остварување. Другиот дел од дигиталните услуги се услуги кои се достапни исклучиво електронски, односно, граѓаните не би можеле инаку да ги добијат. Во овој дел се истражува дали е јасно дефинирана целта на обработката и во која мера ќе треба да се интервенира во интерните акти за заштита на личните податоци на институцијата за да се обезбеди процесот на давање на дигиталната услуга.

Во голем дел од случаите, институциите поставуваат електронски верзии од обрасците и барањата на своите веб страници со што сметаат дека ја обезбедиле услугата по електронски пат. Она што е клучно да се утврди е дали всушност услугата е целосно достапна електронски, односно, дали граѓанинот има можност целата постапка да ја заврши електронски без да има потреба физички да ја посети институцијата во кој било момент од процесот.

Нивото на дигитална писменост е различно кај различни категории на граѓани па со самото тоа институциите треба да најдат начин како да им ја доближат услугата на граѓаните. Институциите треба да обезбедат јасни информации со кои ќе им

4 **„Контролор“** е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или посебните критериуми за негово определување.

помогнат на граѓаните полесно разбирање на дигиталните услуги и поттикнување на нивното користење.

Со цел обезбедување на квалитетни дигитални услуги, институциите треба да обезбедат дополнителен капацитет за ИТ поддршка, развој на софтвери, достава на документи и слично. Најчесто се ангажираат други правни лица кои во име и за сметка на институцијата вршат обработка на дел од личните податоци кои се обработуваат во процесот на остварување на дигиталната услуга, а со самото тоа имаат и обврска да го регулираат односот контролор-обработувач[5].

Прашањата од овој дел се тесно поврзани со почитувањето на начелата за:

- **„законитост, правичност и транспарентност“** – личните податоци се обработуваат во согласност со закон, во доволна мера и на транспарентен начин и
- **„ограничување на целите“** – личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели.

2.2. Оценка на транспарентноста на обработката на личните податоци

Во вториот дел ќе се анализира на кој начин институциите ги исполнуваат обврските за информирање на граѓаните за заштита на нивните лични податоци кои се обработуваат при користењето на дигиталната услуга.

Согласно Законот за заштита на личните податоци, институцијата – контролор е должна да ги информира субјектите на личните податоци за обработката на нивните лични податоци при користењето на дигиталната услуга. Оваа информација треба да биде достапна во форма на Политика за приватност, на локацијата каде се наоѓа и самата услуга. Истакнувањето на Политика за приватност значи дека институциите личните податоци ги обработуваат на транспарентен начин и дали отворено ја демонстрираат усогласеноста со Законот за заштита на личните податоци.

За доследна примена на начелото на транспарентност, Политиката за приватност треба особено да содржи информации за идентитетот на контролорот, правната основа за обработката на личните податоци, целта за обработката на личните податоци, категориите на личните податоци кои се потребни за да може да се добие дигиталната услуга, рокот во кој се чуваат личните податоци кои се обработени при остварувањето на дигиталната услуга, дали личните податоци се споделуваат или се откриваат на друго правно лице во процесот на давање на дигиталната услуга. Дополнително, Политиката за приватност треба да даде општа информација и опис на техничките мерки кои контролорот ги презема за да ги заштити личните податоци

5 **„Обработувач“** е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело кое ги обработува личните податоци во име на контролорот.

кои се обработуваат во процесот на давање на дигиталната услуга.

Политиката за приватност треба да содржи и информација за тоа кои права согласно закон ги уживаат субјектите на личните податоци, корисници на дигиталната услуга, но и на кој начин можат истите да ги остварат.

Прашањата од овој дел се тесно поврзани со почитувањето на начелата за:

- **„законитост, правичност и транспарентност“** – личните податоци се обработуваат во согласност со закон, во доволна мера и на транспарентен начин и
- **„ограничување на целите“** – личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели.
- **„минимален обем на податоци“** – личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат
- **„ограничување на рокот на чување“** – личните податоци се чувани во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци
- **„отчетност“** - контролорот е одговорен за усогласеноста со Законот за заштита на личните податоци, при што е должен да ја демонстрира усогласеноста

2.3. Оценка на предвидените технички и организациски мерки за заштита на личните податоци

Во третиот дел ќе се анализира на кој начин се институциите ги исполнуваат обврските за обезбедување на технички и организациски мерки за заштита на нивните лични податоци кои се обработуваат при користењето на дигиталната услуга.

Согласно Правилникот за безбедност на обработката на личните податоци донесен од страна на Агенцијата за заштита на личните податоци, веб страниците, веб платформите и сличните дигитални алатки на кои се поставени дигиталните услуги треба да бидат обезбедени со соодветни безбедносни протоколи. Безбедносните протоколи се особено важни кога добивањето на дигиталната услуга е овозможено со претходно креирање на кориснички профил од страна на субјектот на личните податоци кој сака да ја користи дигиталната услуга. Покрај безбедносните протоколи, контролорот треба да примени и посебен начин на верификација на корисникот со што ќе обезбеди дополнителни технички мерки за заштита на приватноста при користењето на дигиталната услуга.

Собирањето на општите информации за корисникот при неговото пристапување на локацијата каде што се наоѓа дигиталната услуга треба да биде транспарентно, но и да му се даде право на корисникот да одбере за кои информации од неговата посета на локацијата се согласува да бидат собрани. Институциите треба да истакнат Политика за колачиња која задолжително ќе даде опции за корисникот да може да

се согласи, да не се согласи или пак да одбере кои колачиња ќе бидат активни.

Дигиталните услуги можат да бидат поврзани и со други веб-страници, бази на институции различни од онаа која ја нуди дигиталната услуга. Овие случаи налагаат дополнително обезбедување на целиот процес на користење на дигиталните услуги. Обврската за заштита на личните податоци во случаите како овој не е само на страната на контролорот, туку и на онаа институција со која има поврзување и интеракција.

Обезбедувањето на соодветни технички и организациски мерки за заштита на личните податоци во голема мера зависи и од проценката на влијанието врз заштитата на личните податоци, особено за новите дигитални услуги и услугите за кои не постои законски пропишана процедура. Препорачливо е институциите да донесат свои методологии врз основа на кои ќе вршат проценка врз влијанието врз заштитата на личните податоци како дел од интерната документација за заштита на личните податоци.

Прашањата од овој дел се тесно поврзани со почитувањето на начелата за:

- **„интегритет и доверливост“** – личните податоци се обработени на начин кој обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки
- **„точност“** – личните податоци се точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени.

Март 2022

METAMORPHOSIS

Foundation for Internet and Society