МЕТОДОЛОГИЈА ЗА ПРОЦЕНА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ ЗА ЈАВНИТЕ УСЛУГИ ШТО СЕ ВО ПРОЦЕС НА ДИГИТАЛИЗАЦИЈА

МЕТАМОРФОЗИС
Фондација за интернет и општество

КОНЕКТ

МЕТОДОЛОГИЈА ЗА ПРОЦЕНА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ ЗА ЈАВНИТЕ УСЛУГИ ШТО СЕ ВО ПРОЦЕС НА ДИГИТАЛИЗАЦИЈА

МЕТАМОРФОЗИС
Фондација за интернет и општество

КОНЕКТ

Издавач:
Фондација за интернет и општество Метаморфозис

Автор:
Инфиго ИС

Уредник:
Весна Радиновска

Преведувач:
Бестел ДОО

Дизајн:
Европа 92 - Кочани

Лектура:
Бестел ДОО

Печати:
Европа 92 - Кочани

Тираж:
75 примероци

Октомври, 2023

Оваа публикација е подготвена со поддршка на Европската Унија. Содржините во овој текст се единствена одговорност на Фондација Метаморфозис и на авторите и на ниеден начин не ги одразуваат ставовите на Европската Унија.

МЕТАМОРФОЗИС
Фондација за интернет и општество

КОНЕКТ

СОДРЖИНА

1. ЦЕЛ, ОПСЕГ И КОРИСНИЦИ

Со оваа Методологија се опишува постапката за вршење на Проценатa на влијанието врз приватноста на јавните услуги што се во процес на дигитализација (понатаму: *ПВЗЛП*) во сите јавни институции (во натамошниот текст: *„Институции“*) и Процена на влијанието што вештачката интелигенција ќе го има врз приватноста на граѓаните, доколку се применува од институциите во процесот на испорака на јавните услуги.

Оваа Методологија го опишува методот и ги определува чекорите при спроведување на ПВЗЛП и ги обезбедува потребните критериуми за процена и референтни примери.

Корисници на овој документ се офицерот за заштита на личните податоци и одговорните лица на организациските единици во институцијата.

2. РЕФЕРЕНТНИ ДОКУМЕНТИ

- Закон за заштита на личните податоци[1]
- Правилник за процесот на процена на влијанието на заштитата на личните податоци[2]
- Листа на видовите операции на обработка за кои се бара спроведување на ПВЗЛП[3]
- Листа на видовите операции на обработка за кои не се бара ПВЗЛП[4]
- Европскиот акт за вештачка интелигенција.[5]

[1] Закон за заштита на личните податоци („Службен весник на РСМ“ број 42 од 16.2.2020 година)

[2] Правилник за процесот на процена на влијанието на заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)

[3] Листа на видовите операции на обработка за кои се бара процена на влијанието врз заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)

[4] Листа на видовите операции на обработка за кои не се бара процена на влијанието врз заштитата на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20)

[5] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

3. ДЕФИНИЦИИ

Дел од наведените дефиниции на термините користени во овој документ се во согласност со членот 4 од Законот за заштита на личните податоци, а дел се појаснување за целосно разбирање на овој документ:

Лични податоци: секоја информација што се однесува на идентификувано физичко лице или физичко лице што може да се идентификува. Идентификувано физичко лице е лице што директно или индиректно може да се идентификува со користење информации какви што се име, број на лична карта, локација и други информации, или еден или повеќе фактори што се специфични за физичкиот, физиолошкиот, психолошкиот, економскиот, културниот или социјалниот идентитет на лицето. Во личните податоци спаѓаат имејл-адресите, телефонски број, биометриски податоци (на пример, отпечаток од прст), локација, IP-адреса, здравствени податоци, религиска припадност, брачен статус и слично.

Посебна категорија лични податоци: лични податоци што откриваат раса или етничко потекло, политички ставови, верски или филозофски убедувања, членство во синдикални организации, генетски податоци, биометриски податоци, здравствени податоци, податоци за сексуалниот живот или за сексуалната припадност.

Деловни (службени) информации: податоци како име и презиме, работна позиција, службен телефонски број, службена адреса, службена имејл-адреса, како и други слични информации за лицето, кои не се за исклучива лична цел.

Контролор: физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење 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.

Обработувач на збирка на лични податоци: физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење јавни овластувања, агенција или друго тело што ги обработува личните податоци во име на контролорот. Примери за обработувач се: софтверска компанија што одржува софтвер за човечки ресурси, cloud сервис провајдер, компанија ангажирана за одржување на ИТ-системот итн.

Проценета на влијанието врз заштитата на личните податоци (ПВЗЛП): процес предвиден да ги опише деловните активности, да ја процени нив-

ната неопходност и пропорционалност, и да помогне во справувањето со ризиците што може да се јават при вршење на тие активности врз правата и слободите на физичките лица. Пример за активности за кои е потребно да се спроведе ПВЗЛП се: обемна обработка на посебна категорија лични податоци или лични податоци поврзани со казнени осуди и казнени дела, обработка на лични податоци со користење систематско набљудување (мониторинг) на јавно достапен простор во големи размери и сл.

Обработка на лични податоци: секоја операција или збир на операции што се извршуваат врз личните податоци, или група лични податоци, автоматски или на друг начин. Под операција/-ии се подразбира: 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.

Дигитализација: процес на претворање информации во дигитален (т.е. компјутерски читлив) формат.

Вештачка интелигенција (ВИ): интелигенција демонстрирана од машини, особено од компјутерски системи. Задачи што би ги извршувала ВИ се решавање проблеми, визуелна перцепција, препознавање глас, носење одлуки, преводи и слично.

4. ГЛАВНИ НАСОКИ

Методологијата за ПВЗЛП е документ што им овозможува на институциите како контролори, и носители на активностите (операциите)[6] за обработка на личните податоци, да ги идентификуваат ризиците поврзани со обработката на личните податоци и своите обврски за воведување мерки за заштита на правата и на слободите на субјектите на лични податоци.

Обврската за спроведување на ПВЗЛП се однесува на секој контролор. Кога обработката целосно или делумно ќе биде извршувана од обработувачот, тогаш обработувачот треба да му помогне на контролорот во спроведувањето на ПВЗЛП при што улогите, обврските и одговорностите на контролорот и на обработувачот ќе бидат утврдени во меѓусебен договор, во согласност со прописите за заштита на личните податоци.

[6] *Во рамките на целиот документ ќе се користат термините активности и операции за обработка на личните податоци, кои се произлезени од Законот за заштита на личните податоци и од Правилникот за процесот на процена на влијанието на заштитата на личните податоци.*

Процесот на ПВЗЛП со себе носи големи придобивки како за контролорот така и за обработувачот. Имено, овој процес ги зема предвид приватноста и заштитата на личните податоци и предвидува имплементација на соодветни технички и организациски мерки, односно активности чија цел е да обезбедат тајност и заштита на податоците, уште во моментот на дефинирање на средствата за обработка. Придобивките од спроведување на ПВЗЛП, вклучуваат: воспоставување систем за рано предупредување, носење информирани одлуки, превенција и минимизирање на ризиците за нарушување на приватноста и заштитата на личните податоци.

ПВЗЛП се спроведува пред да се почне со обработката на личните податоци и кога според природата, обемот, контекстот и целите на обработката постои веројатност да се предизвика висок ризик врз правата и слободите на физичките лица, а особено кога се воведуваат нови технологии за обработка на личните податоци.

ПВЗЛП задолжително се спроведува во случај на:

- обемна обработка на посебните категории лични податоци;
- систематско набљудување јавно достапни простории во големи размери;
- систематска и сеопфатна оцена на личните аспекти што се поврзани со физичките лица, која се заснова на автоматска обработка вклучувајќи и профилирање, а врз чија основа се донесуваат одлуки и имаат правно дејство и значително влијание врз физичкото лице.

Спроведувањето на ПВЗЛП е задолжително и во случај на пренос на податоци во облак, воведување нов производ, обработување податоци за цел што е различна од првично утврдената цел, отпочнување соработка со нови снабдувачи на услуги, воведување на профилирање клиенти, пренос на лични податоци во трети земји, нови аспекти на информациска сигурност и сл. Освен во наведените случаи, ПВЗЛП се спроведува во согласност со „Листата на видовите операции за обработка за кои се бара Процена на влијанието врз заштитата на личните податоци“[7] донесена од Агенцијата за заштита на личните податоци (во понатамошен текст: АЗЛП).

ПВЗЛП не се бара за одредени видови операции на обработка, особено кога:

- операциите за обработка не резултираат со висок ризик за правата и слободите на физичките лица;
- активностите (операциите) претходно биле утврдени дека не се изложени на ризик при извршената процена на влијанието врз заштитата на личните податоци;

[7] Листа на видовите операции за обработка за кои се бара Процена на влијанието врз заштитата на личните податоци (Службен весник на РСМ, бр.122 од 12.5.2020 година).

- обработката е веќе одобрена од АЗЛП.

Освен во наведените случаи, ПВЗЛП не се спроведува во согласност со „Листата на видовите операции за обработка за кои не се бара Процена на влијанието врз заштитата на личните податоци“[8] донесена од АЗЛП.

При вршење процена на влијанието врз заштитата на личните податоци, се користи Извештајот за ПВЗЛП (Прилог бр. 1 од оваа Методологија). Извештајот за ПВЗЛП се користи за собирање податоци, проценување на ризиците, дефинирање на мерките за намалување на ризикот и за известување за резултатите од спроведената ПВЗЛП.

Во случаи кога има заеднички контролори, секој контролор мора јасно и прецизно да дефинира кој дел од активностите на обработка на личните податоци кому му припаѓа.

5. ОДГОВОРНИ ЛИЦА

Во ПВЗЛП се вклучени следните лица:

- **Офицер за заштита на личните податоци**

Офицерот за заштита на личните податоци во однос на активностите за обработка и ПВЗЛП дава препораки, мислења и совети што ги уредуваат следниве прашања:

1. Дали спроведувањето ПВЗЛП е задолжително?
2. Како да се спроведе ПВЗЛП?
3. Избор на методологија за ПВЗЛП.

Офицерот за заштита на личните податоци е лицето што задолжително дава мислење и во однос на изготвената документација при спроведувањето на ПВЗЛП.

- **Одговорно лице на активноста за обработка на личните податоци (сопственик на процес) е одговорното лице во чии надлежности спаѓа активноста што треба да се спроведе или друго овластено лице (на пример, раководител на сектор/служба/одделение).**

ПВЗЛП ја спроведуваат одговорните лица од деловните единици каде што припаѓа активноста за обработка на личните податоци за кои е потребно

[8] Листа на видовите операции за обработка за кои не се бара Процена на влијанието врз заштитата на личните податоци (Службен весник на РСМ, бр.122 од 12.5.2020 година).

да се изврши ПВЗЛП. Според насоките од оваа Методологија, таа се врши во соработка со офицерот за заштита на личните податоци. При спроведувањето се вклучуваат и другите организациски единици во институцијата, кои се поврзани со активноста за обработка со која се планира да се врши обработката на личните податоци.

- **Консултант** – по потреба, институцијата ќе ангажира надворешни лица или независни експерти, во согласност со природата на технолошките и на организациските решенија што ќе се применуваат при активноста на обработка на личните податоци.

6. ФАЗИ ЗА СПРОВЕДУВАЊЕ ПВЗЛП

6.1. Фаза 1: Квалификационен прашалник

Офицерот за заштита на личните податоци заедно со одговорното лице за активноста за обработка на личните податоци ќе одговорат на квалификационите прашања од Извештајот за ПВЗЛП. Овие прашања се неопходни за да се утврди дали конкретната активност за обработка на личните податоци е со висок ризик врз правата и слободите на физичките лица.

Офицерот за заштита на личните податоци, врз основа на квалификацискиот прашалник, ќе утврди дали за конкретната активност за обработка на личните податоци треба да се продолжи со следните фази, односно да се изврши ПВЗЛП. Доколку макар на едно од квалификационите прашања од фаза 1 од Извештајот за ПВЗЛП е одговорено со „ДА“, тогаш за таа активност за обработка на личните податоци треба да се продолжи со следните фази. Покрај активностите утврдени врз основа на квалификацискиот прашалник, за одредени активности треба да се изврши ПВЗЛП затоа што се наоѓаат на Листата на видовите операции за обработка за кои се бара ПВЗЛП (Прилог бр. 2 од оваа Методологија).

Одговорениот квалификациски прашалник заедно со документацијата (понуда, предлог договор, услуга и сл.) се доставува до офицерот за заштита на личните податоци.

Ако врз основа на квалификацискиите прашања се утврди дека нема потреба од спроведување ПВЗЛП, активноста не се наоѓа на Листата на видовите операции за обработка за кои се бара ПВЗЛП, сепак, офицерот за заштита на личните податоци може да одлучи да се спроведе ПВЗЛП доколку смета дека институцијата треба да добие појасен преглед на ризиците што може да се случат.

Исклучок се активностите што се опфатени со Листата на видовите операции за обработка за кои не се бара ПВЗЛП (Прилог бр. 3 од оваа Методологија). Офицерот за заштита на личните податоци е должен да следи доколку на листите од прилозите 2 и 3 од оваа Методологија, некои активности се додадени/отстранети.

6.2. Фаза 2: Опис на активноста за обработка на личните податоци

Одговорното лице на активноста за обработка на личните податоци треба да даде целосен опис на активноста за обработка на личните податоци. Конкретно, треба да даде опис на природата, опсегот, на контекстот и на целта на активноста, а со цел да се добие појасна и попрецизна слика на планираната активност. Сево ова ќе придонесе за попрецизно комплетирање на следните фази.

Во оваа фаза се утврдува контекстот на обработка и се наведуваат односно се опишуваат најмалку следниве информации:

- Активноста за обработка на лични податоци;
- Цел на обработката;
- Движење на податоците;
- Метод(и) на добивање на податоците;
- Начин и средства за обработка на податоците (користена опрема, мрежи, човечки ресурси итн.);
- Субјекти што се вклучени во обработката (контролори, обработувачи, корисници итн.);
- Рок на чување.

6.3. Фаза 3: Консултација

Во оваа фаза, потребно е да се утврди кој сè ќе биде консултиран за вршењето на активноста за обработка на личните податоци. Офицерот за заштита на личните податоци одлучува дали и кога ќе побара мислење од субјектите на личните податоци чии лични податоци ќе бидат опфатени со активноста.

Мислењето од субјектите на личните податоци или од нивните претставници, може да биде побарано преку различни методи, во зависност од контекстот (на пример, општа студија поврзана со целта и со средствата на активноста за обработка, со поставување прашања до претставниците на

субјектите на лични податоци, или преку анкети што се испраќаат до идните клиенти на контролорот).

Доколку конечната одлука на институцијата се разликува од мислењето на субјектите на лични податоци, причините за продолжување или за прекин на обработката на личните податоци задолжително треба да се образложат во Извештајот за ПВЗЛП. Доколку, пак, институцијата одлучи да не бара мислење од субјектите на лични податоци (на пример: доколку со тоа би се загрозила доверливоста на работните планови во институцијата или тоа е несразмерно и/или неизводливо), образложението за ваквата одлука треба да се документира во Извештајот за ПВЗЛП.

Исто така, можна е вклученост и на други страни што би биле консултирани за активноста, какви што се консултанти со различна експертиза, или, пак, обработувачи.

6.4. Фаза 4: Процена на неопходност и пропорционалност

За активноста за обработка на личните податоци за која е потребна ПВЗЛП, одговорното лице на активноста за обработка на личните податоци го пополнува Извештајот за ПВЗЛП. По потреба, одговорното лице може да побара помош и поддршка за оваа фаза од Офицерот за заштита на личните податоци. Целта на оваа фаза е да се аргументира потребата од таквата активност, односно да се аргументира нејзината неопходност и да се утврди дали е предвидено користење онолку лични податоци, пропорционално на целта.

Офицерот за заштита на личните податоци го проверува квалификацискиот прашалник заедно со придружната документација и може да побара дополнително објаснување или да постави дополнителни прашања за да се разјаснат сите аспекти од планираната обработка на личните податоци.

Одговорното лице на активноста за обработка кое има обврска да спроведе ПВЗЛП, е должно од потенцијалните понудувачи да ги обезбеди сите податоци за услугата што ја нудат и да ја прибави релевантната документација во врска со обработката на личните податоци на сите подобработувачи (општи услови, договори, безбедносни мерки, постојна ПВЗЛП на подобработувачот и сл.).

6.5. Фаза 5: Идентификување и процена на ризици

Во оваа фаза, одговорното лице на активноста за обработка на личните податоци треба да ги идентификува заканите што можат да се случат и да ја загрозат безбедноста на личните податоци, односно да ги загрозат правата и

слободите на физичките лица. Дополнително, во оваа фаза треба да се идентификува веројатноста и влијанието доколку се реализираат овие закани.

При утврдување на ризиците што се поврзани со обработката, особено ќе се земат предвид заканите што можат да придонесат за случајно или за незаконско уништување, губење, менување, неовластено откривање на личните податоци или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

Влијанието (последица во случај да се реализира заканата) може да биде:

- **ниско**, кога физичките лица можат да се соочат со неколку помали непријатности, кои ќе ги надминат без проблем;
- **средно**, кога физичките лица можат да се соочат со значителни непријатности, кои ќе можат да ги надминат и покрај одредени тешкотии;
- **високо**, кога физичките лица можат да се соочат со значителни последици, кои би требало да можат да ги надминат, но со сериозни тешкотии; и
- **многу високо**, кога физичките лица можат да се соочат со значителни, па дури и неповратни последици, кои најверојатно нема да можат да ги надминат.
- Веројатноста (одредена закана да настане поради недостаток или слабост на контролите), пак, може да биде:
- **ниска** – очекувано е заканата/настанот да се реализира еднаш годишно или поретко**;**
- **средна** – очекувано е заканата/настанот да се реализира на шест месеци или поретко**;**
- **висока** – очекувано е заканата/настанот да се реализира еднаш месечно.
- Вредноста на веројатноста и на влијанието се утврдува врз основа на анализа на следните параметри:
- Вредност на активноста за обработка на која се однесува ризикот, односно заканата;
- Ранливости на активностите за обработка што овозможуваат реализација на ризикот, односно на заканите;
- Претходни искуства и глобални или регионални трендови поврзани со идентификуваната закана;
- Постојни сигурносни контроли спроведени над информациските ресурси што се дел од активностите за обработка.

Вкупниот ризик се пресметува како функција од веројатноста да се случи заканата и влијанието (последица) што таа закана би го имала.

ризик = веројатност x влијание

Веројатност	Матрица на ризик			
В (Висока)	**Н**	**С**	**В**	**МВ**
С (Средна)	**Н**	**С**	**В**	**МВ**
Н (Ниска)	**Н**	**Н**	**С**	**В**
Влијание	**Н** (ниско)	**С** (Средно)	**В** (Високо)	**МВ** (Многу високо)

6.6. Фаза 6: Определување мерки за намалување на ризиците

Откако ќе се идентификуваат ризиците, Офицерот за заштита на личните податоци во соработка со одговорното лице за активноста на обработка на личните податоци, а по потреба и во соработка со лицата одговорни за информацискиот систем и неговата безбедност, ќе утврдат заштитни мерки за намалување на ризиците. Задолжително се третираат ризиците што од пресметката се покажале со вкупен ризик среден, висок или многу висок.

Планот за справување со ризиците ќе биде вметнат во Извештајот за ПВЗЛП. Задолжително треба да се наведат следниве информации:

- Сигурносни мерки што треба да се спроведат за управување со ризикот:

Во продолжение, пример на мерки што можат да се спроведат во согласност со начелата за заштита на личните податоци.

Во согласност со начелото на законитост, правичност и транспарентност – Дефинирање Политика за приватност, Обука и подигање на свеста на вработените во однос на заштитата на личните податоци, соодветна форма на согласност и можност за нејзино повлекување, соодветна правна основа за обработка, информирање на субјектот (субјектот е навремено известен кои лични податоци ќе се обработуваат, за кои цели, кој ќе ги обработува, кому може да му се обрати, рок на чување, права на субјектот), навремено постапување по барања на субјектите и сл.

Во согласност со начелото на ограничување на целите – Собирање и обработка на лични податоци само за точно определени цели. На пример, да се информираат и да се обучат лицата што обработуваат лични податоци и имаат пристап до нив дека личните податоци собрани за една цел не смеат

да се користат за други цели, како, на пример, профилирање, неовластено откривање и сл.

Во согласност со начелото на минимален обем на податоци – Дефинирање минимална количина податоци што е потребна за исполнување на целта (не е соодветно да се собираат дополнителни податоци што не се потребни за постигнување на целта), псевдонимизација и сл.

Во согласност со начелото на точност – Потребно е да се дефинираат мерки со кои собраните податоци се точни и ажурирани во секој момент, да му се даде можност на субјектот да го оствари своето право за исправка на податоците што се неточни и нецелосни.

Во согласност со начелото на ограничување на рокот на чување – Потребна е соодветна постапка за бришење или за уништување на личните податоци по истекот на рокот за нивно чување. Воведување технички мерки за автоматизирано бришење по дефинираниот рок на чување на личните податоци.

Во согласност со начелото на интегритет и доверливост – Примена на донесените ИТ-процедури за технички и организациски мерки (криптирање на опремата, криптирање бази на податоци, псевдонимизација, физичка контрола на пристап, пристап до податоци ограничен само на вработени, употреба на „силни" лозинки, проверка на автентичност, сигурносни копии, firewall итн.), ИТ-безбедност, навремено известување за нарушување на безбедноста (загуба, објава, неовластен пристап), превенција на инциденти итн.).

Во согласност со начелото на отчетност – Почитување на одредбите за обработка на личните податоци, дефинирани правила и постапки за обработка на личните податоци, соодветен пренос на личните податоци, обука на вработените во институцијата за внимателно, превентивно и проактивно работење.

Сигурносни мерки треба да се спроведат и на личните податоци што ќе се пренесуваат во трети земји (надвор од ЕУ, на пример: складирање на сервер). Треба да се дефинира која е причината и кои лични податоци ќе се пренесуваат надвор од ЕУ, како и кои мерки ќе се преземаат при преносот на личните податоци. Дали преносот на личните податоци ќе биде уреден со меѓународен договор, одлука за соодветност од страна на АЗЛП или Европската комисија или изречна согласност на субјектот на лични податоци?

Мерки за заштита на личните податоци при преносот во трети земји:

- стандардни договорни клаузули за заштита на личните податоци што ги утврдува АЗЛП[9] или се одобрени од Европската комисија (eng. SCC – standard contractual clauses[10]);

[9] Стандардни договорни клаузули (АЗЛП)

[10] Standard contractual clauses for international transfers (European Commission)

- задолжителни корпоративни правила;
- одобрени обврзувачки и извршни обврски на контролорот или на обработувачот во трета земја за примена на соодветни безбедносни мерки и заштита на правата на субјектите на лични податоци.

❖ Одговорни лица за имплементација на мерките (офицер за заштита на лични податоци, одговорно лице на активноста за обработка на лични податоци [сопственик на процес – раководител на сектор] и консултант [надворешно ангажирано лице или независни експерти]);

❖ Рокови за спроведување мерки за намалување на идентификуваните ризици.

6.7. Фаза 7: Запис за имплементацијата на сигурносните мерки

Сигурносните мерки што биле имплементирани, треба да се евидентираат во Извештајот за ПВЗЛП во колоната „Запис за завршување".

7. ПРЕТХОДНА КОНСУЛТАЦИЈА СО АГЕНЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Доколку резултатите од ПВЗЛП индицираат дека активноста за обработка на личните податоци е со висок ризик дури и откако ќе се спроведат сигурносните мерки, а институцијата има интерес да ја врши предметната активност за обработка на лични податоци, тогаш офицерот за заштита на личните податоци мора да се консултира со АЗЛП пред да започне вршењето на предметната активност.

Без оглед на резултатите од ПВЗЛП, односно за секој ризик (низок, среден, висок или многу висок), институцијата ќе побара претходно одобрение од АЗЛП за да може да врши обработка на личните податоци за цели на јавен интерес, вклучувајќи и обработка за цели на социјална заштита и јавно здравство. Ваквото одобрение особено ќе се бара во случај кога:

- основните активности на институцијата се состојат од операции за обработка, кои поради својата природа, опсег и/или цели, бараат во голема мера редовно и систематско следење на субјектите на лични податоци;
- основните активности на институцијата се состојат од обемна обработка на посебни категории лични податоци или лични податоци поврзани со казнени осуди и казнени дела;

- ќе се врши систематско набљудување на простори или на простории во големи размери.

АЗЛП ќе биде консултирана од институцијата за време на изработување предлог-закони или подзаконски акти што се донесуваат врз основа на тие закони, а кои се однесуваат на обработката на личните податоци.

Офицерот за заштита на личните податоци ќе ѝ ги обезбеди на АЗЛП следните информации:

- Одговорности на контролорот, заеднички контролор(и) и обработувач(и);
- Цели и средства на планираната обработка;
- Предвидени сигурносни мерки за заштита на личните податоци;
- Контакт податоци на Офицерот за заштита на личните податоци; и
- Извештај од спроведената ПВЗЛП.

8. РЕДОВНО РЕВИДИРАЊЕ НА ПВЗЛП

Офицерот за заштита на личните податоци мора да ја ревидира ПВЗЛП во некој од следниве случаи:

- Ако се променат ризиците поврзани со активностите за обработка на личните податоци (на пример, некој од ризиците преминал од средно во високо ниво);
- Ако има значителна промена во активностите за обработка на личните податоци (на пример, ако се променат предметот, целта и начините за обработката на личните податоци);
- Ако настане промена во техничките и во организациските мерки (на пример, доколку се имплементира некој нов софтвер, систем и сл.);
- Ако настане потреба за меѓуграничен пренос на податоците (на пример, некоја од активностите предвидува пренос на лични податоци при користење услуги во облак кон држави од ЕУ, Европски економски простор (ЕЕП) или кон трети земји);
- Ако има промена во законските барања (промена на закон врз чија основа се спроведува обработката на личните податоци); или
- Ако институцијата дејствува како обработувач, а контролорот бара ПВЗЛП да биде ревидирана и сл.

9. ПРОЦЕНА НА ВЛИЈАНИЕТО ШТО ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА ЌЕ ГО ИМА ВРЗ ПРИВАТНОСТА НА ГРАЃАНИТЕ[11]

Секој ден вештачката интелигенција (во понатамошниот текст: ВИ) го менува начинот на кој го доживуваме светот. Веќе користиме ВИ за да го пронајдеме најкраткиот и најбрзиот пат до дома, да нè предупреди за сомнителна активност на нашите банкарски сметки и да ги филтрираме спам-мејловите.

За граѓаните, примената на технологиите за ВИ ќе резултира со поперсонализирано и поефикасно искуство. За луѓето што работат во јавниот сектор, тоа значи намалување на часовите што ги поминуваат на основните задачи, што ќе им даде повеќе време да потрошат на иновативни начини за подобрување на услугите.

Потенцијалните употреби на ВИ во јавниот сектор се значајни, но мора да бидат урамнотежени со етички, правични и безбедносни размислувања.

ВИ е истражувачко поле што опфаќа филозофија, логика, статистика, компјутерски науки, математика, невронаука, лингвистика, когнитивна психологија и економија.

Дискусијата помеѓу предностите на технологијата за ВИ и ризиците за нашите човекови права станува најочигледна во полето на приватноста. Приватноста е основно човеково право, суштинско за да се живее во достоинство и безбедност. Но, во дигиталното опкружување, вклучително и кога користиме апликации и платформи за социјални медиуми, се собираат големи количини лични податоци – со или без наше знаење – и тие може да се користат за да нè профилираат и да произведат предвидувања за нашето однесување. Ние објавуваме податоци за нашето здравје, за политичките идеи и за семејниот живот без да знаеме кој ќе ги користи овие податоци, за какви цели и зошто.

Машините функционираат врз основа на она што им го кажуваат луѓето. Ако системот се храни со човечки предрасуди (свесни или несвесни), резултатот неизбежно ќе биде пристрасен. Постои недостаток во разновидноста и вклучувањето во дизајнот на системите за ВИ: наместо нашите одлуки да бидат пообјективни, тие би можеле да ја зајакнат дискриминацијата и предрасудите.

[11] *Овој процес сè уште не е уреден во Република Северна Македонија. Користени се материјали од Европскиот акт за вештачката интелигенција што Европскиот парламент го донесе на 14.6.2023 и други материјали што ја уредуваат оваа материја.*

9.1. Дефиниции:

- Според Актот за вештачка интелигенција[12] (во понатамошниот текст: Актот), дефиниција за ***„систем за вештачка интелигенција" (систем за ВИ)*** значи *„софтвер што е развиен со една или со повеќе од техниките и пристапите наведени во Анекс I од Актот (Прилог бр. 4 од оваа Методологија) и може за даден сет на цели дефинирани од човекот, да генерира резултати какви што се содржина, предвидувања, препораки или одлуки што влијаат врз средини со кои тие комуницираат"*; иако во согласност со Актот од Европскиот парламент од јуни 2023 година дефинициите се спорна точка на дискусија што нагласуваат дека дефиницијата на системите за ВИ е прилично широка и би опфатила многу повеќе од она што субјективно се подразбира како ВИ, вклучувајќи ги и наједноставните алгоритми за пребарување, сортирање и рутирање, кои последователно би биле предмет до нови правила;
- ***„провајдер или давател"*** *значи физичко или правно лице, државна институција, агенција или друго тело што развива систем за ВИ или што има развиен систем за ВИ, со цел да го пласира на пазарот или да го стави во употреба под свое име или заштитен знак, без разлика дали тоа ќе биде наплатено или ќе биде бесплатно;*
- ***„корисник"*** *значи секое физичко или правно лице, државна институција, агенција или друго тело што користи систем за ВИ под негова надлежност, освен кога системот за ВИ се користи во текот на лична непрофесионална активност.*

Треба да се направи разлика во однос на обврските помеѓу провајдерот и корисникот на даден високоризичен систем за ВИ. Провајдерите се примарна цел во однос на усогласеноста, како и обврските во согласност со Актот за ВИ. Освен што треба да ги задоволуваат подолу наведените барања, имаат и обврски за соработка и обезбедување информации до корисниците под одредени околности. Покрај провајдерите, увозниците и дистрибутерите на системите за ВИ имаат одредени обврски според членовите 26 и 27 од Актот. Овие обврски, сепак, најчесто се за потврда, верификација и за целите на обезбедување информации.

Обврските на корисниците се предвидени во член 29 од Актот според кој корисниците ќе користат високоризични системи за ВИ во согласност со упатствата, ќе имплементираат човечки надзор и следење на работата на високоризичниот систем за ВИ, ќе ги земат предвид одредбите за заштита на податоците и ќе соработуваат со националните органи.

[12] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

9.2. Европскиот акт за вештачка интелигенција

Имајќи го ова предвид, Европската комисија во април 2021 година го поднесе предлогот на Европскиот акт за ВИ, што пратениците на Европскиот парламент го донесоа две години подоцна, во јуни 2023.

Нацрт-актот за ВИ е првиот обид да се донесе хоризонтална регулатива за ВИ. Предложената законска рамка го регулира користењето на системите за ВИ и поврзаните ризици. Комисијата предлага да се воспостави технолошки неутрална дефиниција за системите за ВИ и да се утврди класификација на системите за ВИ, при што секоја група би имала различни услови и обврски, кои ќе се утврдуваат врз основа на „пристап заснован на ризик". Системите за ВИ што резултираат со „неприфатливо" ниво на ризик, би биле забранети. Голем дел од високоризичните системи за ВИ ќе бидат дозволени за употреба, но ќе мораат да исполнат определени услови и обврски за да добијат пристап до пазарот на ЕУ. Оние системи за ВИ што резултираат со „ограничено" ниво на ризик, ќе бидат предмет на едноставни обврски за транспарентност.

Главната позиција на земјите членки на ЕУ во декември 2021 година беше претставена од Советот на ЕУ, а Парламентот гласаше за неговата позиција во јуни 2023 година. Пратениците на ЕУ започнаа преговори за финализирање на новата легислатива, со значителни измени на предлогот на Комисијата, вклучувајќи ревидирање на дефиницијата за системи за ВИ, проширување на списокот на забранети системи за ВИ и наметнување обврски на ВИ за општа намена и генеративни модели на ВИ како што е ChatGPT.[13]

9.3. Вештачката интелигенција и нејзиното влијание врз правата на граѓаните

ВИ во последните години бележи брз напредок, а со нејзиното развивање се овозможува поголема примена во сите области на општеството што придонесува за подобрување и олеснување на животот на граѓаните.

Со користењето на ВИ во областа на здравството, може да се дојде до подобрување на здравствената заштита (на пример: поставување попрецизна и побрза дијагноза на пациентите, овозможување превенција од разни болести за да избегнат пациентите понатамошни заболувања итн.). ВИ може да се применува и за побрзо, поедноставно и поквалитетно остварување на правата од социјална заштита (на пример: детски додаток за образование – студирање, користење право на родителски додаток за дете итн.), за доделување стипендии, субвенции, зголемување на ефикасноста на земјо-

[13] Извор: Wikipedia - ChatGPT

делството, придонесување и адаптирање на климатските промени, подобрување на производните системи (преку зголемување на безбедноста на граѓаните), а сè со цел и во насока на одржување или унапредување на квалитетот на животот на граѓаните.

Покрај горенаведените придобивки што со себе ги носи ВИ, таа носи и потенцијални ризици, кои можат да бидат во најразлична форма.

Системите за ВИ може да доведат до дискриминација и да предизвикаат нееднаквост меѓу граѓаните. До дискриминација може да дојде бидејќи податоците што се користат за да ѝ помогнат на ВИ да донесува одлуки, во себе веќе содржат пристрасност (дискриминација врз основа на пол, боја на кожа, националност, вероисповед итн.).

Покрај ова, ВИ може да биде пробиена или манипулирана, што неизбежно ќе резултира со значителна штета на правата и на слободите на граѓаните. Друг ризик може да биде и зависноста од ВИ за донесување важни одлуки. Иако ВИ може да помогне да се автоматизираат процесите и да се идентификуваат проблемите, таа не го заменува човечкото расудување.

Погрешната примена на ВИ може значително да ги загрози правата на граѓаните, не само како такви, туку и во начинот на нивното остварување и практикување.

ВИ, всушност, може негативно да влијае врз широк опсег на нашите човекови права. Проблемот се надополнува со фактот што одлуките се носат врз основа на овие системи, а притоа не постои транспарентност, отчетност и заштитни мерки за тоа како тие се дизајнирани, како функционираат и како може да се менуваат со текот на времето.

Одлуките донесени без да се преиспитаат резултатите од погрешниот алгоритам, може да имаат сериозни последици за човекот. На пример, лицата со попреченост кои имаат право на придобивки од областа на здравствената заштита се погрешно отфрлени од софтверот и тие понатаму се соочиле со последици од таквата одлука. ВИ има потенцијал да им помогне на луѓето максимално да го искористат своето време, слобода и среќа. При што, многу е тешко, а со тоа и неопходно да се најде вистинската рамнотежа помеѓу технолошкиот развој и заштитата на човековите права.

Сите организации без разлика дали станува збор за државен орган или за приватна компанија, треба да поседуваат ВИ-експертиза за да функционира Актот за ВИ ефективно. Актот за ВИ нема да функционира и ќе направи значителна штета доколку институциите немаат доволно експертиза за тоа како да ги тестираат системите за ВИ, како да го евалуираат нивното влијание врз општеството и како да управуваат со нив ефективно.

9.3.1. Процена на влијанието врз човековите права на системите за ВИ

Една од основните меѓународни и уставни обврски е заштитата на човековите права, која јавните институции треба да ја земат предвид при набавка на системите за ВИ или системите управувани од алгоритам.

Пред да биде дизајниран, развиен или имплементиран какво било систем за ВИ, потребно е да се спроведе Процена на влијание врз човековите права на системите за ВИ, поради фактот што системите за ВИ би имале потенцијално негативно влијание врз човековите права и тие може да претставуваат закана за животната средина, човечкиот живот, демократијата и за владеењето на правото.

Проценатa на влијанието врз човековите права игра клучна улога во заштитата на човековите права и е од суштинско значење за обезбедување доверба на јавноста во технологијата поврзана со ВИ. За да се стекне довербата во системите за ВИ, проценитe на влијанието треба да бидат задолжителна практика каде што човековите права ќе бидат соодветно разгледани и целосно почитувани. Без разлика на донесената методологија, процесот на оценување мора да биде транспарентен, одговорен, партиципативен и вграден во поширокиот општествен контекст на кој технологијата може да има влијание.

Во продолжение предлагаме рамка на индикатори[14] кои имаат за цел да обезбедат насоки за проценатa на влијанието при набавка на системите за ВИ кои ќе обезбедат заштита на човековите права. Следејќи ги индикаторите, на државните институции и на програмерите им се дава доволно флексибилност да го приспособат процесот на процена и истовремено да потврдат дали нивните методи се соодветни за да се направи точна процена и да се ублажи влијанието врз човековите права.

- *Индикатор 1: Нормативна рамка*

Овој индикатор мери дали процесот на оценување е заснован на релевантните меѓународни правни стандарди поврзани со човековите права. Неговата цел е, исто така, да се осигури дали обемот и содржината на проценатa овозможува точна идентификација и ублажување на негативните влијанија врз човековите права, вклучително и ситуации каде што негативните влијанија врз човековите права се неприфатливо високи и е невозможно да се ублажат.

- *Индикатор 2: Транспарентен и одговорен процес на оценување*

Овој индикатор мери дали проценитe на влијанието се транспарентни, отчетни и повторувачки (вградени во животниот циклус на системите за ВИ). Исто така, мери колку е јасна поделбата на улоги и одговорности помеѓу јав-

[14] *Извор: Draft indicators for human rights impact assessment of IT services/products in procurement processes by European Center for Not-for-Profit Law prepared for the needs of the project "Privacy by Design – Building an Inclusive Digital Ecosystem", supported by the EU and implemented by Metamorphosis Foundation and Association Konekt.*

ните институции и снабдувачите како и меѓу вработените кај двете страни за да се превенира дисперзијата на отчетноста. Овој индикатор го мери нивото на транспарентност на процесите за набавка и процена на влијанието, вклучувајќи и информации што треба да бидат откриени од страна на снабдувачот/одговорниот за развој на софтверот на државната институција.

❖ *Индикатор 3. Методологија за процена на влијанието*

Овој индикатор мери дали методологијата за проценатa на влијанието на човековите права гарантира значаен и одговорен одраз на влијанијата на системот за ВИ. Овој дел не наметнува специфичен метод за оценување, туку содржи список на прашања за да се процени дали избраната методологија е соодветна, ефективна и точна за да се обезбеди усогласеност со човековите права.

❖ *Индикатор 4: Значаен ангажман на засегнатите страни*

Овој индикатор мери дали релевантните засегнати страни (засегнати поединци и групи, граѓански организации, синдикати, национални институти за човекови права, индустриски здруженија, експерти за човекови права, академски експерти итн.) се ангажирани за дефинирање на (потенцијалните) влијанија на системот за ВИ. Ваквиот ангажман е со цел прецизно да се идентификуваат ризиците како и мерките за нивно ублажување, а со тоа и градење на довербата на јавноста во технологијата.

❖ *Индикатор 5. Ефективен надзор и следење*

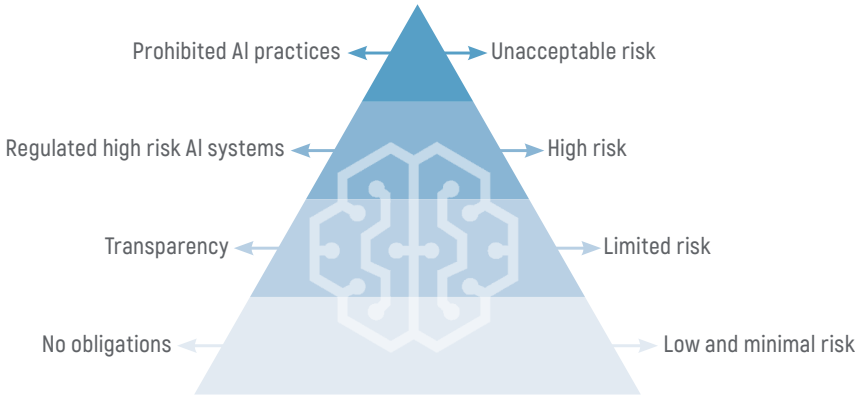
Овој индикатор мери дали проценатa на влијанието е отчетна пред надворешниот надзор/ревизор и дали е предмет на јавна контрола. Целта на овој индикатор е да гарантира институционална рамка за мониторинг и континуирана процена во случај да има промена во контекстот и појава на нови влијанија врз човековите права.

9.4. Ризици според Европскиот акт за вештачка интелигенција[15]

Актот во себе предвидува пристап заснован на ризици по системите, кои можат да бидат:

- Систем со неприфатлив ризик;
- Систем со висок ризик;
- Систем со ограничен ризик;
- Систем со низок или минимален ризик.

[15] Извор: EPRS | European Parliamentary Research Service: Briefing, EU Legislation in Progress (Artificial intelligence act



Извор: Европска комисија.

Слика 1: Класифицирани нивоа на ризик

Концептот на „систем заснован на ВИ со висок ризик" не е експлицитно дефиниран. Наместо тоа, група системи за вештачка интелигенција се класифицирани како такви под услов да се исполнети одредени услови.

Актот не нуди строго утврдена дефиниција за „систем за ВИ со висок ризик", но ги класифицира специфичните употреби на ВИ како високоризични и тие се наведени во Прилог бр. 5 од оваа Методологија.

Прилог бр. 5, како дел од Актот, детално ги прикажува високоризичните системи за ВИ, може да биде изменет од Европската комисија по одредени услови наведени во Актот. Актот за ВИ мора да утврди јасно и правно дефинирани стандарди за примена доколку легислативата стапи на сила. Легислативата мора да поддржи објективен процес за да се одреди кои системи се „високоризични" и да го отстрани секој „дополнителен слој" додаден во процесот за класификација на висок ризик. Таквиот слој ќе им дозволи на одговорните лица за развој на ВИ без одговорност или надзор да одлучат дали нивните системи претставуваат доволно „значаен ризик" за да се гарантира правната контрола според регулативата.

Ваквиот процес на класификација на ризици носи опасност од поткопување на целиот Акт за ВИ, односно поставување несовладливи предизвици за спроведување, усогласување и поттикнување на поголемите компании да ги класифицираат своите системи за ВИ со пониско ниво на ризик.

Според погоренаведеното, Актот:

- би вовел висока правна несигурност за тоа кои системи се сметаат за „високоризични";
- би довел до фрагментација на единствениот пазар на ЕУ, со различни толкувања за тоа што претставува „висок ризик" во земјите членки;

- би резултирал со тоа дека властите на земјите членки би се соочиле со сериозни предизвици за спроведување на законодавството, без доволно ресурси за доволно следење на самооценувањето на програмерите;
- би им дозволил на програмерите да ги избегнат основните барања на законот, кои имаат за цел да ги направат нивните системи побезбедни и посигурни. Ова би ги ставило во неповолна положба одговорните развивачи на ВИ.

Прашањето за тоа кои системи за ВИ треба да бидат забранети (и како овие системи прецизно да се дефинираат) и какви видови системи за ВИ треба да се класифицираат како високоризични, останува тема на тековна дебата, како и на критики од циркулација на првичниот предлог на Европската комисија.

❖ **Неприфатлив ризик: Забранети практики на вештачка интелигенција**

Според Поглавје 2, член 5 од Актот, овие системи на ВИ се забранети за употреба, бидејќи создаваат неприфатлив ризик што претставува закана за безбедноста, здравјето, егзистенцијата и правата на луѓето. Тоа се системи што користат штетни манипулативни „сублиминални техники, односно техники што можат да бидат опасни за луѓето", кои предизвикуваат физичка или психолошка повреда на луѓето, системи за вештачка интелигенција што искористуваат одредени ранливи групи луѓе (со физичка и со ментална попреченост), системи користени од страна на државни органи или во нивно име за евалуација или класификација на доверливоста на физичките лица во одреден временски период врз основа на нивното социјално однесување или системи за далечинска биометриска идентификација „во реално време" во јавно достапни простори за целите на спроведување на законот, освен во ограничен број случаи наведени во глава 2, член 5 од Актот.

❖ **Висок ризик: Регулирани високоризични системи за вештачка интелигенција**

Поглавје 3, член 6 од Предложениот акт за ВИ ги регулира „високоризичните" системи за ВИ што влијаат врз здравјето, безбедноста и основните човекови права. Еден систем се смета за високоризичен кога се исполнети следните услови:

- Системи што се користат како безбедносна компонента на производ или кои потпаѓаат под здравјето и безбедноста на законодавство на ЕУ за хармонизација (на пример, играчки, авијација, автомобили, медицински помагала, лифтови).
- Системот за вештачка интелигенција како производ, подложи на conformity assessment (во понатамошниот текст познат како проце-

на на сообразност, објаснета подетално во деловите 10 и 11), а од трета страна пред да биде ставен на пазарот на ЕУ.

Дополнително, одредени системи за ВИ се класифицирани како високоризични и овие системи се наведени во Прилог 2 (од оваа Методологија) од Актот за вештачка интелигенција на ЕУ.

Постојат осум главни системи за ВИ што може да се класифицираат како високоризични, и тоа:

- **Биометриска идентификација и категоризација на физички лица**

- Системи за вештачка интелигенција наменети да се користат за далечинска биометриска идентификација на физички лица „во реално и нереално време".

- **Управување и функционирање на критичната инфраструктура**

- Системи за ВИ наменети да се користат како безбедносни компоненти во управување и функционирање на патниот сообраќај и снабдувањето со вода, гас, парно и електрична енергија.

- **Образование и стручна обука**

- Системи за ВИ наменети да се користат за да се одреди пристапот или да се назначат физички лица во образовни и стручни установи, системи за вештачка интелигенција наменети да се користат за целите на оценување на учениците во образовните институции и стручна обука и за оценување на учесниците на тестовите што вообичаено се потребни за прием во образовните институции (на пример, бодување на испити).

- **Вработување, управување со вработените и пристап до самовработување**

- Системи за вештачка интелигенција наменети да се користат за регрутирање или за селекција на физички лица, особено за огласување слободни работни места, анализа или филтрирање апликации за вработување, оценување кандидати за време на интервјуа или тестови како и ВИ наменета да се користи за донесување одлуки за унапредување и за раскинување на договорните односи поврзани со работата, за распределба на задачи и за следење и оценување на перформансите и на однесувањето на вработените или на ангажираните лица.

- **Пристап и придобивки од користењето на приватните и на јавните услуги**

- Системи за ВИ наменети да се користат од државните органи или во име на државните органи за да се оцени подобноста на физичките лица за социјални и јавни услуги, како и за доделување, намалување, отповикување

или враќање на таквите придобивки и услуги, системи за ВИ наменети да се користат за процена на кредитната способност на физички лица или за утврдување на нивниот кредитен рејтинг, системи за ВИ наменети да се користат за испраќање или за утврдување приоритет во испраќањето на службите за прв одговор во итни случаи, вклучително и од пожарникари и медицинска помош.

- **Спроведување на законот**

- Системи за ВИ наменети да ги користат органите за спроведување на законот за изработка на поединечни процени на ризик на физички лица, со цел да се процени ризикот физичкото лице да изврши дело спротивно на законот или да го повтори делото или потенцијалните жртви на кривични дела; системи за ВИ наменети да ги користат органите за спроведување на законот како полиграф и слични алатки или за откривање на емоционалната состојба на физичко лице; системи за ВИ наменети да се користат од органите за спроведување на законот за откривање длабоки фалсификати како што е наведено во член 52(3) од Актот; системи за ВИ наменети да ги користат органите за спроведување на законот за оцена на веродостојноста на доказите во текот на истрагата или гонењето на сторителите на кривични дела; системи за ВИ наменети да ги користат органите за спроведување на законот за предвидување на појава или повторување на вистинско или потенцијално кривично дело врз основа на профилирање физички лица како што е наведено во член 3(4) од Директивата (ЕУ) 2016/680[16] или процена на особини и карактеристики на личноста или криминално однесување во минатото на физички лица или групи физички лица; системи за ВИ наменети да ги користат органите за спроведување на законот за профилирање физички лица како што е наведено во член 3(4) од Директивата (ЕУ) 2016/680 во текот на откривање, истрага или гонење на сторителите на кривични дела; системи за ВИ наменети да се користат за аналитика на криминал во однос на физички лица, дозволувајќи им на органите за спроведување на законот да пребаруваат сложени поврзани и неповрзани големи збирки на податоци достапни од различни извори на податоци или во различни формати на податоци, со цел да се идентификуваат непознати шеми или да се откријат скриени односи во податоците.

- **Управување со миграцијата, азил и гранична контрола**

- Системи за ВИ наменети да се користат од надлежните државни органи како полиграф и слични алатки или да се открие емоционалната состојба на физичко лице; системи за ВИ наменети да се користат од надлежните државни органи за да се процени ризикот, вклучително и безбедносниот ри-

[16] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

зик, ризик од незаконска имиграција или здравствен ризик, што го носи физичкото лице што има намера да влезе или влегло на територијата на земја членка на ЕУ; системи за ВИ наменети да ги користат надлежните државни органи за проверка на автентичноста на патните исправи и придружната документација на физички лица и откривање неавтентични документи со проверка на нивните безбедносни карактеристики; системи за ВИ наменети да им помогнат на надлежните државни органи за испитување на барањата за азил, виза и дозволи за престој и придружните жалби во однос на подобноста на физичките лица што аплицираат.

- **Спроведување на правдата и на демократските процеси**

- Системи за ВИ наменети да им помогнат на правосудните органи во истражувањето и во толкувањето на фактите и на законот и при примената на законот на конкретен збир факти.

Слика 2. Класифицирани системи на ВИ со висок ризик

Сепак, мора да се нагласи дека не се смета за високоризичен секој систем за ВИ во овие категории. Постојат ставови за секое од овие полиња, што мора детално да се испитаат за да се утврди дали даден систем за ВИ навистина се смета за високоризичен или не.

Сите овие високоризични системи за ВИ ќе подложат на збир на нови правила, вклучувајќи:

- Услов за ex-ante процена на сообразност: Давателите на високоризични системи за ВИ ќе се бара да ги регистрираат своите системи во базата на податоци на ЕУ (управувана од Европската комисија), пред да бидат пуштени на пазарот или ставени во употреба. Сите производи и услуги засновани на ВИ регулирани со постојното законодавство за безбедност на производите, ќе потпаднат под постојните рамки што веќе се применуваат (на пример, за медицински помагала). Даватели на системи за ВИ кои во моментов не се регулирани од законодавството на ЕУ, ќе треба да спроведат сопствена процена на сообразност (самооценување) дека се усогласени со новите барања и можат да користат „CE" ознака. Само на системите со ВИ со висок ризик што се користат за биометриска идентификација ќе им се бара процена на сообразност од страна на „овластено тело".
- Други барања: Ваквите високоризични системи за ВИ треба да се усогласат со низа барања особено за управување со ризик, тестирање, техничка робусност, обука и управување со податоци, транспарентност, човечки надзор и сајбербезбедност (Поглавје 2, членови од 8 до 15 од Актот). Во овој поглед, давателите на услуги, увозниците, дистрибутерите и корисниците на високоризичните системи за ВИ би морале да исполнат низа обврски. Давателите надвор од ЕУ ќе бараат овластен претставник во ЕУ за да (меѓу другото) спроведат процена на сообразност, да воспостават систем за мониторинг по неговото ставање во функција и по потреба да се преземат корективни мерки. Системите за ВИ што се во согласност со новите хармонизирани стандарди на ЕУ, во моментов во развој, ќе имаат корист од претпоставката за усогласеност со нацрт-барањата на Актот.

❖ **Ограничен ризик: Обврски за транспарентност**

Системите за ВИ што се класифицирани како системи со „ограничен ризик", какви што се системи што комуницираат со луѓе (т.е. чет-ботови), системи за препознавање емоции, системи за биометриска категоризација и системи за ВИ што генерираат или манипулираат со слики, аудиосодржини или видеосодржини (eng. deep fake), би биле предмет на ограничен сет обврски за транспарентност. Како, на пример, провајдерите обезбедуваат информации за системите за ВИ што се наменети за интеракција со физички лица да се дизајнирани и развиени на таков начин што физичките лица се информи-

рани дека имаат интеракција со систем на ВИ, освен ако тоа не е очигледно од околностите и од контекстот на употреба или, пак, физичките лица што се изложени на систем за препознавање емоции или систем за биометриска категоризација, се известени за работата на самиот систем.

- **Низок или минимален ризик: Нема обврски**

Сите други системи за ВИ што претставуваат само низок или минимален ризик може да се развијат и да се користат во ЕУ без да се усогласат со какви било дополнителни законски обврски. Сепак, предложениот Акт го предвидува создавањето кодекси на однесување за да се поттикнат провајдерите на системи за ВИ со низок ризик доброволно да ги применуваат задолжителните барања за високоризичните системи за ВИ.

9.5. Барањата за високоризичните системи за вештачка интелигенција

Актот ги поставува барањата за високоризичните системи за ВИ во Поглавје 2 и последователно наметнува обврски на провајдерите на услуги, како и на корисниците на овие системи.

Постојат седум главни барања предвидени според членовите од 9 до 15 од Актот, кои системите за ВИ треба да ги исполнат за да се сметаат за доверливи, и тоа:

1. Систем за управување со ризик;
2. Управување со податоци;
3. Техничка документација;
4. Водење евиденција;
5. Транспарентност и давање информации на корисниците;
6. Човечки надзор;
7. Точност, отпорност и сајбербезбедност.

Слика 3. Барања за системи за вештачка интелиґенција со висок ризик

Усогласеноста со овие барања е задолжителна за опфатените ентитети. Меѓутоа, нивото на усогласеност ќе се определи земајќи го предвид општопризнаениот „state of the art" во согласност со член 8 алинеја 1 од Актот. Дополнително, усогласеноста со овие барања може да бара земање предвид одредби за други спорни прашања вклучувајќи, но не ограничувајќи се на, одговорност за производот, заштита на податоци, авторски права, интелектуална сопственост и деловни тајни. Притоа, правилното усогласување ќе бара детална и повеќеслојна анализа што е приспособена на спецификите на секој систем за ВИ.

Важно е дека повеќето од овие барања мора да бидат вградени во дизајнот на системот за ВИ со висок ризик. Освен техничката документација што треба да ја подготви провајдерот, другите барања треба да се земат предвид уште од најраните фази на дизајнирање и развој на системот за ВИ. Дури и ако провајдерот не е дизајнер/развивач на системот, тие сепак треба да се погрижат барањата од тоа Поглавје да се вградени во системот за да се постигне усогласеност.

9.6. Надзорно тело

Земјите членки бараат да се назначат „надлежни“ или „овластени“ органи, кои би имале за задача да ја нагледуваат имплементацијата и усогласеноста со регулативата на системите за ВИ. Органите за надзор ќе бидат одговорни за оценување на усогласеноста на провајдерите со обврските и барањата за високоризичните системи за ВИ. Тие би имале пристап до доверливи информации (вклучувајќи го изворниот код на системите за ВИ) и би биле обврзани со обезбедување на таа доверливост.

Понатаму, од нив ќе се бара да преземат какви било корективни мерки за забрана, ограничување, повлекување или отповикување системи за ВИ што не се во согласност со Актот или кои, иако се усогласени, претставуваат ризик за здравјето или за безбедноста на луѓето и заштитата на нивните права. Во случај на постојана неусогласеност, земјите членки ќе мора да преземат соодветни мерки за ограничување, забрана, отповикување или повлекување на високоризичниот систем за ВИ од пазарот.

10. ПРОЦЕНА НА СООБРАЗНОСТ (ENG. CONFORMITY ASSESSMENT)

Клучна обврска што ја наметнуваат високоризичните системи за ВИ е процена на сообразност што провајдерите на таквите системи треба да ја спроведат пред да ги пласираат на пазарот.

Процена на сообразност е законска обврска дизајнирана да ја поттикне одговорноста што се однесува само на системи за ВИ класифицирани како „високоризични“.

Дополнително, нова процена на сообразност треба да се изврши кога систем за ВИ со висок ризик е суштински изменет или резултира со модификација намената за системот за ВИ.

Овој процес треба да го спроведе провајдерот на високоризичниот систем, но исто така, во специфични ситуации може да го спроведе производителот, дистрибутерот, како и трета страна.

Специфичната процена на сообразност, што треба да се спроведе за високоризичните системи за ВИ, зависи од категоријата и од видот на вештачката интелигенција што е во прашање.

Актот предвидува два различни типа процена на сообразност во зависност од типот на високоризичниот систем за ВИ, и тоа:

❖ Внатрешна процена

Оваа процена не бара вклучување независна трета страна. Провајдерот/производителот на ВИ-системот/друга трета страна мора:

- Да потврди дека има имплементирано систем за управување со квалитет, кој вклучува многу карактеристики, вклучително и управување со ризик, процедура за пријавување инциденти (на пример, нарушување на безбедноста на податоците, неисправност на системот и идентификација на ризици што претходно не биле очигледни) и процедури за тестирање и валидација за управување со податоци.
- Да ги има испитано информациите во техничката документација на системот за ВИ за да ја оцени усогласеноста на системот за ВИ со релевантните суштински барања за високоризични системи за ВИ според предложената регулатива.
- Да потврди дека процесот на дизајнирање и развој на системот за ВИ и неговото следење по пласирањето на пазарот што е наведено во член 61 е во согласност со техничката документација на системот (оваа документација вклучува информации за способностите на системот за ВИ и ограничување на системот, користени алгоритми, податоци, обука, тестирање и процеси на валидација).

Откако одговорниот ентитет ќе ја спроведе внатрешната процена на сообразност, тој треба да изготви писмена изјава за усогласеност, за секој систем за ВИ.

„CE" ознаката за Процена на сообразност треба да биде видлива, читлива и неизбришлива за сите системи за ВИ во висок ризик. Онаму каде не е можно или не е оправдано поради природата на високоризичниот систем за ВИ, ознаката се става на придружната документација, како што е соодветно.

❖ Процена од трета страна (овластено тело)

Оваа процена ја спроведува независна трета страна, која ќе издаде сертификат за потврдување на усогласеноста на системот за ВИ.

Од провајдерот ќе се бара да достави документација и информации во врска со системот за управување со квалитет и техничката документација, според процесот објаснет во Прилог 7 од оваа Методологија, а овластеното тело ќе ги користи документацијата и информациите за да утврди дали системот за ВИ ги исполнува релевантните барања.

Покрај тоа, предложената регулатива ќе бара од провајдерот да му дозволи на овластеното тело да пристапи до просториите каде што се одвива ди-

зајнот, развојот и тестирањето на системите за ВИ, да врши „периодични ревизии" за да се осигури дека провајдерот ги одржува и ги применува системите за управување со квалитет и, онаму каде што е разумно неопходно за да се оцени сообразноста, пристап до изворниот код на системот за ВИ. Доколку овластеното тело утврди дека системот за ВИ со висок ризик е во согласност со барањата, тоа ќе издаде сертификат за процена на техничката документација, кој има ограничена временска важност и може да биде суспендиран или повлечен од овластеното тело. Слично на внатрешната процена на сообразност, процесот на процена на сообразност извршен од трета страна, провајдерот треба да ја подготви изјавата за усогласеност и да ја стави ознаката за усогласеност „CE". За да го заврши процесот, провајдерот треба да изготви формулар за декларација – што содржи, меѓу другото, опис на спроведената постапка за процена на сообразност.

Во случај овластеното тело да оцени дека високоризичниот систем за ВИ не е во согласност со барањата за високоризичните системи за ВИ, тоа треба да му го соопшти и детално да му го објасни на провајдерот или на друг одговорен ентитет. Провајдерот (или друг одговорен ентитет) има право на жалба против одлуката на овластеното тело. Во овој случај, провајдерот/одговорниот ентитет мора да ги преземе потребните корективни активности. Овие активности може да варираат од повторување на процесот за усогласување со барањата, до повлекување на системот од пазарот.

Системите за ВИ со висок ризик мора да подложат на нови процени секогаш кога се „суштински изменети", без разлика дали изменетиот систем ќе продолжи да се користи од тековниот корисник или е наменет да биде пошироко дистрибуиран. Во секој случај, потребна е нова процена од овластено тело на секои 5 години, без разлика дали системот е изменет или не.

11. ПРОЦЕНА НА СООБРАЗНОСТ VS ПВЗЛП

Овој дел компаративно ги анализира предложените процена на сообразност и ПВЗЛП. Иако и двете обврски бараат да се изврши процена на активностите за обработка на лични податоци со висок ризик (во случај на ПВЗЛП) и системи за ВИ (во случајот на процена на сообразност), постојат и разлики и заеднички карактеристики што треба да се истакнат.

Според ЗЗЛП и Правилникот за процесот на процена на влијанието на заштитата на личните податоци, контролорот е актерот што ги одредува целите и начините за обработка на личните податоци. Контролорот е одговорен за усогласеност со Законот и со Правилникот, за процена дали ќе се изврши ПВЗЛП и за извршување на која било ПВЗЛП. Според Актот, процена на сообразност првенствено спроведува провајдерот на високоризичниот систем за ВИ (или производителот на производот, дистрибутерот или увозникот или трето лице, кога се исполнети посебните услови).

При спроведување на ПВЗЛП, контролорот треба да ги идентификува заканите за правата и слободите на физичките лица, да ги процени ризиците во однос на нивната сериозност и веројатноста тие да се материјализираат и конечно да одлучи за соодветните мерки што ќе ги ублажат високите ризици. Спротивно на тоа, процена на сообразност бара испитување дали високоризичниот систем за ВИ ги исполнува специфичните барања утврдени со Актот, а наведени погоре во документот. Во листата на видовите операции на обработка за кои се бара ПВЗЛП се вклучени операции за обработка што можат да се поврзат со систем за ВИ, како што се, на пример: „обработка на лични податоци за систематско и сеопфатно профилирање или автоматско донесување одлуки со цел да се извлечат заклучоци и да се донесат одлуки што произведуваат правно дејство, кои во голема мера влијаат врз физичкото лице и/или врз повеќе лица или кои помагаат при донесување одлуки за нечиј пристап до услуга или некој вид услуга или некоја погодност“, „обработка на посебни категории лични податоци со цел профилирање или автоматско донесување одлуки“ или „обработка на лични податоци на деца со цел профилирање, автоматско одлучување или за цели на маркетинг или за директно понудување на услуги наменети за нив“.

Актот од друга страна утврдува кои системи за ВИ се квалификуваат како „високоризични“ и затоа бара да се спроведе процена на сообразност. Не се остава на дискреционо право на одговорниот субјект да процени дали е потребно да се спроведе процена на сообразност. За да се спроведе процена на сообразност, не е важно дали се обработуваат лични податоци, иако тие може да се обработуваат како дел од употребата на системот за ВИ. Доволно е системот за ВИ да потпадне под рамката на Актот и да се квалификува како „високоризичен“.

За спроведување на ПВЗЛП, контролорот мора да ја процени „активноста за обработка" во однос на ризиците што ги носи за правата и слободите на физичките лица. Поконкретно, контролорот мора да ги разгледа природата, опсегот, контекстот и целите на обработката, како и нејзината неопходност и пропорционалност со наведената цел.

За спроведување процена на сообразност, провајдерот мора да процени дали системот или производот е дизајниран и развиен во согласност со специфичните барања на Актот наменети за високоризичните системи за ВИ.

Според ЗЗЛП, контролорот е тој што ги одредува целите и средствата за обработка на личните податоци и тој утврдува дали треба да се изврши ПВЗЛП.

Додека, пак, според Актот за ВИ, процена на сообразност првенствено спроведува провајдерот на високоризичниот систем за ВИ (или производителот на производот, дистрибутерот или увозникот или трето лице, кога се исполнети посебни услови).

Обврските за спроведување на ПВЗЛП и процена на сообразност се различни по обем, содржина и цели. Во некои области тие се поврзани и може дури и да се преклопуваат особено кога системите за ВИ со висок ризик вклучуваат обработка на лични податоци.

Високоризичните системи за ВИ што вклучуваат обработка на лични податоци може да се надополнат или да добијат поддршка од контролорите што спроведуваат ПВЗЛП. Обврската на Актот и спроведувањето процена на сообразност, може да ја пополни празнината во однос на одговорностите на провајдерите и на контролорите што ги користат овие системи за обработка на лични податоци. Меѓутоа, ако ентитетот е и провајдер и контролор во однос на систем за ВИ што ќе обработува лични податоци, тогаш тој ентитет ќе изврши и ПВЗЛП и процена на сообразност.

Крајната цел на ПВЗЛП е да ги повика контролорите на одговорност за нивните постапки и да гарантира поефикасна заштита на правата на субјектите. Целта на проценатa на сообразност од друга страна е да гарантира усогласеност со одредени барања, кои се создадени од мерки за ублажување системи што со себе носат високи ризици.

12. ПРИЛОГ БР. 1

ИЗВЕШТАЈ ЗА ПВЗЛП

(Пополнет примерок)

Податоци за контролорот

Назив на контролорот	*Институција X*
Офицер за заштита на личните податоци	*Име и презиме*
Предмет/Назив на ПВЗЛП	*Апликација за автоматско одлучување за доделување стипендии*

Фаза 1: Квалификациски прашалник

Одговорете со ДА или со НЕ на прашањата во прилог.	Да	Не
1. Дали при вршење на активноста се собираат, се користат, се чуваат или се споделуваат какви било лични податоци од посебна категорија?		*Не*
2. Дали при вршењето на активноста се користат лични податоци за да предвидат некакви лични преференции, локација, движење, финансиска состојба, здравствени или работни перформанси на физички лица?		*Не*
3. Дали при вршење на активноста се обработуваат лични податоци поврзани со казнените осуди и казнените дела или прекршочната одговорност?		*Не*
4. Дали со активноста се овозможува донесување одлуки што можат значително негативно да влијаат врз физичките лица?	*Да*	
5. Дали активноста предвидува употреба на нови технологии или технолошки решенија за обработка или со можност за обработка на лични податоци што служат за анализирање или предвидување на економската состојба, здравјето, личните желби или интереси, сигурноста или однесувањето, локацијата или движењето на физичките лица?		*Не*

6. Дали активноста подразбира обработка на лични податоци собрани од трети страни (лица), кои се земаат предвид за донесување одлуки поврзани со склучување, раскинување, одбивање или продолжување договори за давање услуги на физички лица?		*Не*
7. Дали активноста подразбира обработка на лични податоци преку поврзување, споредување или вршење проверка на сличностите од повеќе извори?		*Не*
8. Дали активноста вклучува следење на локацијата или на однесувањето на физичкото лице во случај на систематска обработка на податоците за комуникација (метаподатоци) настанати – генерирани со употреба на телефон, интернет или други средства (канали) за комуникација, какви што се GSM, GPS, Wi-Fi, за следење и за обработка на податоците за локацијата?		*Не*
9. Дали активноста подразбира обработка на лични податоци преку користење уреди и технологии, кај кои доколку настане инцидент, може да го загрози здравјето на едно или на повеќе лица?		*Не*
10. Дали со активноста се врши некакво систематско следење на јавните површини во голема мера?		*Не*
11. Дали има некои други ризици поврзани со употребата на вашиот производ/услуга за правата и слободите на физичките лица?	*Да*	
12. Дали активноста подразбира надзор или следење на вработените лица?		*Не*

Фаза 2: Обработка на личните податоци

Опис на природата на обработката: Како би се собирале, употребувале, чувале и бришеле личните податоци? Кој е изворот од каде што ќе се добиваат личните податоци? Дали личните податоци ќе се споделуваат со трети страни („трета страна" е секое физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење јавни овластувања, агенција или друго тело, кое не е субјект на лични податоци, контролор, обработувач или лице што под директно овластување на контролорот или на обработувачот е овластено да ги обработува податоците)?

Ги собираме податоците на следните начини:

- *Со директна интеракција со корисниците кога аплицираат за стипендија;*
- *Со користење автоматизирани технологии кога корисниците ја користат веб-апликацијата.*

Главно ги употребуваме личните податоци за да провериме дали лицето ги исполнува условите за добивање стипендија. Дополнително, податоците ги употребуваме за да ги известиме субјектите што се веќе регистрирани за други отворени повици за доделување стипендија.

Ги употребуваме податоците за да ги исполниме следните цели:

- *Креирање кориснички профил;*
- *Управување со релациите со субјектите (на пример, одговарање на прашања, поплаки и сл.);*
- *За администрирање и заштита на веб-апликацијата (на пример, одржување и поддршка на апликацијата, решавање проблеми, хостирање и сл.);*
- *За верификување на идентитетот на корисникот и пружање безбедна платформа;*
- *За усогласување со регулаторни и правни обврски.*

Колачиња

Нашата веб-апликација користи колачиња за следните цели:
Користиме неопходни колачиња, кои не се предмет на барање согласност, за следните цели:

- *Автентикација на корисничка сметка;*
- *Безбедност и спречување измами;*
- *Балансирање на оптоварувањето на веб-страницата (load balancing);*
- *Преференции за колачиња за алатката за согласност за користење колачиња.*

Чување и бришење на податоците

Веб-апликацијата е хостирана во Северна Македонија и сите нејзини податоци се чуваат во Северна Македонија.
Податоците се чуваат во согласност со законски пропишаните рокови. Оние податоци за кои нема законски пропишан рок, се чуваат во согласност со Политиката за рокови на чување (во прилог).

Споделување со трети страни

Податоците на субјектите се споделуваат со Министерство за финансии заради исплата на средствата за стипендија. Пристап до податоците исто така има и компанијата што е одговорна за развој на апликацијата.
Во Политиката за приватност се наведени сите засегнати страни што имаат пристап до личните податоци на субјектите.

Мерки за безбедност на личните податоци

Ги користиме следните мерки за безбедност:

- *Бараме од корисниците што креираат своја корисничка сметка да употребуваат комплексни лозинки со букви, бројки, најмалку 1 специјален знак и најмалку 1 голема буква. Лозинките да бидат со минимум 10 карактери;*
- *Користиме SSL-заштита на нашата страница за најавување;*
- *Имаме политика за редовно бришење на сите фајлови, бази на податоци или апликации што повеќе не се користат;*
- *На сите податоци редовно им се прави сигурносна копија;*
- *Вршиме редовни скенирања на ранливости на нашата веб-апликација и на серверите.*

Опишете го опсегот на обработката:

- Која е природата на личните податоци?
- Дали се обработуваат лични податоци од посебна категорија или лични податоци од казнена евиденција?
- Колкава количина лични податоци ќе бидат собрани и употребувани?
- Колку често?
- Колку долго ќе се чуваат?
- Колку физички лица ќе бидат засегнати?
- Колкава географска површина ќе биде опфатена?

Податоци што ќе бидат обработувани:

- *податоци за идентитет: име, презиме, корисничко име, датум на раѓање;*
- *податоци за контакт: адреса, имејл-адреса, телефонски број;*
- *финансиски податоци: податоци за месечните примања на родителите/старателите за последните 3 (месеци);*
- *технички податоци: IP-адреса, податоци за најава... итн.;*

Посебна категорија лични податоци: *Не обработуваме посебна категорија лични податоци.*

Количина лични податоци: *Очекуваме веб-апликацијата годишно да има околу 10.000 корисници.*

Географска површина: *Субјектите чии лични податоци ќе бидат обработувани се лоцирани исклучиво во Република Северна Македонија. Веб-апликацијата е хостирана во Република Северна Македонија.*

Опишете го контекстот на обработката:

- Која е природата на односот помеѓу институцијата и физичките лица?
- Колкава контрола би имале физичките лица?
- Дали тие би очекувале да им ги обработувате личните податоци на ваков начин?
- Дали обработката опфаќа обработка на лични податоци на деца или на други ранливи групи?
- Дали постојат некои причини за загриженост за овој тип обработка или сигурносни пропусти?
- Каква е моменталната состојба на технологијата што би се користела?
- Дали постојат некои причини за загриженост на јавноста што треба да се земат предвид?

На нашата веб-апликација, студентите можат да аплицираат за добивање стипендија. Самиот систем по добиените информации од студентите одредува дали некој студент ги исполнува/не ги исполнува условите за добивање на стипендијата. Студентите се информирани за ваквиот начин на обработка во Политиката за приватност, која е достапна при самото посетување на оваа веб-апликација. Студентите можат во секој момент да се обратат до Министерството и да добијат објаснување за начинот на кој функционира самиот алгоритам...

Опишете ја целта на обработката:

- Што е целта на проектот/деловниот процес, кои се предвидените активности на обработка на личните податоци односно што се сака да се постигне?
- Кое е влијанието врз физичките лица?
- Кои се придобивките од обработката – за вас и пошироко?

Целта е да се автоматизира и да се забрза процесот на доделување стипендии. Исто така, целта е и да се забрза и самото време на аплицирање и добивање резултат од самата апликација.

Фаза 3: Консултација

Земете предвид како ќе се консултирате со засегнатите страни: опишете кога и како ќе побарате мислење од физичките лица – или објаснете зошто тоа не е соодветно да се прави. Кој друг ќе биде инволвиран во вашата институција? Дали ќе има вклучено и обработувачи? Дали ќе бидат вклучени консултанти за информациска сигурност или други консултанти?

Пред самата имплементација на системот, беа консултирани и физичките лица. Беше доставен прашалник до сите физички лица за да се процени нивната заинтересираност и/или загриженост за имплементација на ваквиот систем. Самиот систем односно резултатите од барањата беа потврдувани/коригирани од вработените во Министерството како би се намалил бројот на грешки од страна на самиот систем.

Фаза 4: Процена на неопходност и пропорционалност

Опишете ги мерките за усогласеност и пропорционалност, конкретно: Која е законската основа за обработка? Дали со обработката ќе се постигне посакуваната цел? Дали постои некој друг начин со кој истата цел може да се постигне? Како ќе се спречи да се обработуваат личните податоци неовластено за други цели? Како ќе се постигне квалитет на податоците и минимален обем на личните податоци? Кои информации ќе им се дадат на физичките лица? Како се гарантира остварувањето на правата на физичките лица како субјекти на лични податоци? Кои мерки ќе се преземат за усогласеност на обработувачот? Како ќе се заштитат меѓународни преноси? Дали личните податоци ќе се пренесуваат во трети земји (надвор од ЕУ, на пример: складирање на сервер)? Која е причината за пренос на личните податоци надвор од ЕУ? Кои лични податоци ќе се пренесуваат надвор од ЕУ? Кои мерки ќе се преземаат при пренос на личните податоци? (На пример, користење „облак", органите на финансиската контрола разменуваат податоци во контекст на меѓународен пренос на лични податоци за целите на управна/административна соработка.)
Законската основа на оваа обработка е Законот за студентски стандард и Правилникот за видот на студентските стипендии и начинот на доделување студентски стипендии. *Да, со обработката се постигнува посакуваната цел.* *Не постои друг начин да се постигне истата цел.* *Податоците за оние студенти што аплицирале за добивање стипендија, се анонимизираат и се чуваат во согласност со Процедурата за рокови на чување, при што се спречува неовластен пристап до нив. Во самата веб-апликација се обработуваат само неопходните податоци, односно податоците неопходни за остварување на целта. Во врска со квалитетот на податоците, самиот студент ја потврдува точноста на внесените податоци, при што за потврдувањето на идентитетот на корисникот, се користи систем за електронска идентификација на корисникот.* *Информациите како и остварувањето на правата на субјектите, се наведени во Политиката за приватност.* *Пред самото одбирање на обработувачот, одговорен за развој на веб-апликацијата, беше утврдено (со физички пристап до неговите простории и увид во неговата документација) дека тој ги применува одредбите од ЗЗЛП и со него беше склучен договор (стандардни договорни клаузули).* *Нема пренос надвор од границите на РСМ.*

Фаза 5: Идентификување и проценување ризици

Опишете ја заканата	Веројатност од закана	Влијание на закана	Вкупен ризик
недостаток на системот	**Мала**, средна, голема веројатност	Ниско, средно, **високо**, многу високо	Низок, **среден** или висок

Фаза 6: Мерки за намалување на ризик

Идентификување заштитни мерки што треба да се преземат за да се намалат или да се елиминираат ризиците идентификувани со среден и висок и многу висок ризик во фазата 5				
Ризик	**Предлог сигурносна мерка**	**Одобрена мерка**	**Одговорно лице за имплементација**	**Рок за спроведување**
недостаток на системот	*план за закрепнување од катастрофи локација и план за континуитет во работењето*	***Да**/Не*	*Служба за ИТ*	*31.12.2023 г.*

Фаза 7: Запис

	Име/позиција/датум	**Забелешка**
Одобрени мерки од:	*Име и презиме, одговорно лице од сектор, 1.1.2023 г.*	Вклучете ги активностите во планот на проектот, со датум и одговорност за спроведување
Обезбедено мислење од ОЗЛП:	*Име и презиме*	ОЗЛП треба да даде мислење дали обработката може да се врши
Краток опис на мислењето на ОЗЛП: *Офицерот смета дека обработката може да се врши откако ќе се имплементираат соодветните безбедносни мерки и откако ќе се осигури дека системот дава реални резултати и резултати што не ги нарушуваат правата и слободите на физичките лица.*		
Мислењето на ОЗЛП е прифатено или не, од:	*Мислењето е прифатено од: име и презиме.*	Доколку не е прифатено, објаснете зошто
Коментар:/		
Одговорите од консултациите се ревидирани од:	*Име и презиме, раководител на сектор*	Ако вашата одлука отстапува од мислењата на физичките лица, мора да ги објасните вашите причини
Коментар:/		
Оваа ПВЗЛП ќе ја чува:	*Име и презиме, одговорен од сектор*	ОЗЛП треба да ја ревидира усогласеноста со ПВЗЛП

13. ПРИЛОГ БР. 2

ЛИСТА НА ВИДОВИТЕ ОПЕРАЦИИ НА ОБРАБОТКА ЗА КОИ СЕ БАРА ПРОЦЕНА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Процена на влијанието врз заштитата на личните податоци задолжително се бара за одредени видови операции на обработка, особено кога:

- обработка на лични податоци за систематско и сеопфатно профилирање или автоматско донесување одлуки со цел да се извлечат заклучоци и да се донесат одлуки што произведуваат правно дејство, кои во голема мера влијаат врз физичкото лице и/или на повеќе лица или кои помагаат при донесување одлуки за нечиј пристап до услуга или некој вид услуга или некоја погодност (на пример, како што се обработка на лични информации во врска со економски или финансиски статус, здравје, лични преференции, интереси, сигурност, однесување, податоци за локација, итн.);
- обработка на посебни категории лични податоци со цел профилирање или автоматско донесување одлуки;
- обработка на посебни категории лични податоци, т.е. податоци што откриваат расно или етничко потекло, политичко мислење, религиозно или филозофско уверување или членство во синдикат, како и обработка на генетски податоци, биометриски податоци, со цел единствено идентификување на лицата, здравствени податоци или податоци за сексуалниот живот или за сексуалната ориентација на индивидуата;
- обемна обработка на посебни категории лични податоци или лични податоци поврзани со казнените осуди и казнените дела (член 14 од Законот за заштита на личните податоци) или прекршочната одговорност;
- обработка на лични податоци на деца со цел профилирање, автоматско одлучување или за цели на маркетинг или за директно понудување услуги наменети за нив;
- обработка на лични податоци собрани од трети страни (лица), кои се земаат предвид за донесување одлуки поврзани со склучување, раскинување, одбивање или продолжување договори за давање услуги на физички лица;
- обработка на лични податоци со користење систематско набљудување (мониторинг) на јавно достапен простор во големи размери;
- употреба на нови технологии или технолошки решенија за обработка на лични податоци или со можност за обработка на лични податоци што

служат за анализирање или предвидување на економската состојба, здравјето, личните желби или интереси, сигурноста или однесувањето, локацијата или движењето на физичките лица;

- обработка на лични податоци преку поврзување, споредување или вршење проверка на сличностите од повеќе извори;
- обработка на лични податоци на начин што вклучува следење на локацијата или на однесувањето на физичкото лице во случај на систематска обработка на податоците за комуникација (метаподатоци) настанати – генерирани со употреба на телефон, интернет или други средства (канали) за комуникација, какви што се GSM, GPS, Wi-Fi, за следење и обработка на податоците за локацијата;
- обработка на лични податоци преку користење уреди и технологии, кај кои доколку настане инцидент, може да го загрози здравјето на една личност или на повеќе лица (субјекти на лични податоци); и обработка на посебни категории лични податоци на вработените кои се користат за единствена идентификација на вработените од страна на работодавачот и во други случаи на обработка на податоци за лица – вработени од страна на работодавачот преку користење апликација или систем за следење на нивната работа, движење и комуникација и слично (на пример, обработка на лични податоци за следење на вршењето на работната обврска, движењето, комуникација и сл.).

14. ПРИЛОГ БР. 3

ЛИСТА НА АКТИВНОСТИ ЗА КОИ НЕ СЕ БАРА ПВЗЛП

Процена на влијанието врз заштитата на личните податоци не се бара за одредени видови операции на обработка, особено кога:

- активностите на обработка не резултираат со висок ризик за правата и слободите на физичките лица;
- процесите (активностите) претходно биле утврдени дека не се изложени на ризик при извршената процена на влијанието врз заштитата на личните податоци;
- обработката е веќе одобрена од Агенцијата за заштита на личните податоци;
- за обработката веќе има постојна јасна и специфична правна основа во

правниот систем на Република Северна Македонија и кога проценатa на влијанието врз заштитата на личните податоци веќе е спроведена како дел од воспоставувањето на таа правна основа според членот 10 став (3) од Законот за заштита на личните податоци;

- е изведена како дел од проценатa на влијанието што произлегува од основата на јавниот интерес и кога проценатa на влијанието врз заштитата на личните податоци била елемент на таа процена според членот 10 став (3) од Законот за заштита на личните податоци.

Оваа Листа ја пропишува Агенцијата за заштита на личните податоци. Офицерот за заштита на личните податоци има обврска да ги следи промените и да ги имплементира во системот на институцијата.

15. ПРИЛОГ БР. 4

АНЕКС I ОД АКТОТ
ТЕХНИКИ И ПРИСТАПИ НА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА

член 3 точка 1 од Актот

(а) Пристапи за машинско учење, вклучувајќи учење под надзор, учење без надзор како и зајакнување на учењето, користејќи широк спектар методи вклучувајќи и длабинско учење;

(б) Пристапи засновани на логика и знаење, вклучително и претставување на знаењето, индуктивно (логичко) програмирање, бази на знаење, инференцијални и дедуктивни двигатели (eng. Inferential and deductive engines), (симболичко) расудување и експертски системи;

(в) Статистички пристапи, Баесова процена (eng. Bayesian estimation), методи за пребарување и оптимизација.

16. ПРИЛОГ БР. 5

АНЕКС III ОД АКТОТ
ВИСОКОРИЗИЧНИ СИСТЕМИ ЗА ВИ НАВЕДЕНИ ВО ЧЛЕН 6(2)

Високоризичните системи за вештачка интелигенција во согласност со член 6(2) се системи за вештачка интелигенција наведени во која било од следниве области:

1. Биометриска идентификација и категоризација на физички лица:

(a) Системи за вештачка интелигенција наменети да се користат за далечинско биометриска идентификација на физички лица „во реално и во нереално време";

2. Управување и функционирање на критичната инфраструктура:

(a) Системи за вештачка интелигенција наменети да се користат како безбедносни компоненти во управувањето и функционирањето на патниот сообраќај и снабдување со вода, гас, парно и електрична енергија.

3. Образование и стручно оспособување:

(a) Системи за вештачка интелигенција наменети да се користат за целите за одредување пристап или распоредување физички лица во образовни и стручни установи;

(б) Системи за вештачка интелигенција наменети да се користат за целите за оценување на студентите во образовните и во стручните установи и за оценување на учесниците на тестовите што вообичаено се потребни за прием во образовните институции.

4. Вработување, управување со вработените и пристап до самовработување:

(a) Системи за вештачка интелигенција наменети да се користат за регрутирање или за избор на физички лица, особено за огласување слободни работни места, скрининг или филтрирање на апликации за вработување, оценување кандидати за време на интервјуа или тестови;

(б) Системи за вештачка интелигенција наменети да се користат за донесување одлуки за унапредување и прекинување договорни односи поврзани со работата, за распределба на задачите и за следење и оценување на перформансите и на однесувањето на вработените или на ангажираните лица.

5. Пристап до и уживање во основните приватни и јавни услуги и придобивки:

(а) Системи за вештачка интелигенција наменети да ги користат државните органи или во име на државните органи да ја оценат подобноста на физичките лица за бенефиции и услуги за јавна помош, како и да се доделат, намалат, отповикаат или да се вратат таквите бенефиции и услуги;

(б) Системи за вештачка интелигенција наменети да се користат за оценување на кредитната способност на физичките лица или да го утврдат нивниот кредитен рејтинг, со исклучок на системи за вештачка интелигенција ставени во услуга од мали провајдери за нивна употреба;

(в) Системи за вештачка интелигенција наменети да се користат за испраќање или за утврдување приоритет во испраќање служби во итни случаи, вклучително и пожарникари и медицинска помош.

6. Спроведување на законот:

(а) Системи за вештачка интелигенција наменети да ги користат органите за спроведување на законот за изработка на индивидуални процени на ризик на физички лица, со цел да се процени ризикот физичко лице да изврши дело спротивно на законот или ризикот од потенцијални жртви на кривични дела;

(б) Системи за вештачка интелигенција наменети да се користат од органите за спроведување на законот како полиграф и слични алатки или да се открие емоционалната состојба на физичкото лице;

(в) Системи за вештачка интелигенција наменети да ги користат органите за спроведување на законот за откривање длабоки фалсификати како што е наведено во член 52(3) од Актот;

(г) Системи за вештачка интелигенција наменети да ги користат органите за спроведување на законот за евалуација на веродостојноста на доказите во текот на истрагата или при гонењето на сторителите на кривични дела;

(д) Системи за вештачка интелигенција наменети да ги користат органите за спроведување на законот за предвидување на појавата или повторното појавување на вистинско или потенцијално кривично дело врз основа на профилирање физички лица како што е наведено во член 3(4) од Директивата (ЕУ) 2016/680 или процена на особини и карактеристики на личноста или минато криминално однесување на физички лица или на групи физички лица;

(ѓ) Системи за вештачка интелигенција наменети да ги користат органите за спроведување на законот за профилирање физички лица како што е наведено во член 3(4) од Директивата (ЕУ) 2016/680 во тек на откривање, истрага или гонење на сторителите на кривични дела;

(е) Системи за вештачка интелигенција наменети да се користат за аналитика на криминал во однос на физички лица, дозволувајќи им на органите за спроведување на законот да пребаруваат големи, сложени, поврзани и неповрзани збирки податоци достапни од различни извори на податоци или во различни формати на податоци, со цел да се идентификуваат непознати шеми или да се откријат скриени односи во податоците.

7. Управување со миграција, азил и гранична контрола:

(а) Системи за вештачка интелигенција наменети за надлежните државни органи, како полиграф и слични алатки или за откривање на емоционалната состојба на физичко лице;

(б) Системи за вештачка интелигенција наменети за надлежните државни органи за да проценат ризик, вклучително и безбедносниот ризик, ризик од нередовна имиграција или здравствен ризик од физичко лице што има намера да влезе или влегло на територијата на земја членка на ЕУ;

(в) Системи за вештачка интелигенција наменети за надлежните државни органи за проверка на автентичноста на патните исправи и придружната документација на физички лица и откривање неавтентични документи со проверка на нивните безбедносни карактеристики;

(г) Системи за вештачка интелигенција наменети да им помогнат на надлежните државни органи за испитувањето барања за азил, визи и дозволи за престој и поврзани жалби во однос на подобноста на физичките лица што аплицираат за некаков статус.

8. Управување на правдата и на демократските процеси:

(а) Системи за вештачка интелигенција наменети да му помогнат на судскиот орган во истражувањето и толкувањето на фактите и на законот и при примената на правото на конкретен збир факти.

17. ПРИЛОГ БР. 6

АНЕКС VI ОД АКТОТ
ПРОЦЕДУРА ЗА ПРОЦЕНА НА СООДВЕТНОСТ ЗАСНОВАНА НА ВНАТРЕШНА КОНТРОЛА

1. Процедурата за процена на соодветност заснована на внатрешна контрола е базирана на точките 2, 3 и 4;

2. Провајдерот потврдува дека имплементираниот систем за управување со квалитет е во согласност со барањата од Актот;

3. Провајдерот ги прегледува информациите содржани во техничката документација за да се процени усогласеноста на системот за ВИ со релевантните неопходни барања наведени во Актот;

4. Провајдерот исто така потврдува дека процесот на дизајнирање и развој на системот за ВИ и неговото мониторирање по пуштање на пазарот наведено во Актот е во согласност со техничката документација.

18. ПРИЛОГ БР. 7

АНЕКС VII ОД АКТОТ
ПРОЦЕНА НА СООДВЕТНОСТ ЗАСНОВАНА НА ОЦЕНА НА СИСТЕМОТ ЗА УПРАВУВАЊЕ СО КВАЛИТЕТ И ПРОЦЕНА НА ТЕХНИЧКАТА ДОКУМЕНТАЦИЈА

1. Вовед

Сообразност врз основа на процена на системот за управување со квалитет и процена на техничката документација е процедура за процена на соодветност базирана на точките од 2 до 5.

2. Преглед

Одобрениот систем за управување со квалитет за дизајн, развој и тестирање на системите за вештачка интелигенција во согласност со член 17 ќе биде прегледан во согласност со точка 3 и ќе биде предмет на надзор како што е наведено во точка 5. Техничката документација на системот за ВИ ќе биде прегледана во согласност со точка 4.

3. Систем за управување со квалитет

3.1. Апликацијата на провајдерот ќе вклучува:

(а) име и адреса на провајдерот и, доколку пријавата е поднесена од овластен претставник, негово име и адреса, исто така;

(б) список на системи за вештачка интелигенција опфатени со истиот систем за управување со квалитет;

(в) техничка документација за секој систем за вештачка интелигенција покриен со истиот систем за управување со квалитет;

(г) документација во врска со системот за управување со квалитет која ќе ги покрива сите аспекти наведени во член 17;

(д) опис на процедурите што се воспоставени за да се осигури дека системот за управување со квалитетот останува соодветен и ефективен;

(ѓ) писмена изјава дека истата пријава не е поднесена до ниедно друго овластено тело.

3.2. Системот за управување со квалитет ќе биде оценето од овластеното тело, кое ќе утврди дали ги задоволува барањата наведени во член 17. За одлуката се известува провајдерот или неговиот овластен претставник. Известувањето ги содржи заклучоците од оцената на системот за управување со квалитет и образложената одлука заснована на проценатa.

3.3. Системот за управување со квалитет како што е одобрен, провајдерот ќе продолжи да го имплементира и да го одржува за да остане адекватен и ефикасен.

3.4. Секоја планирана промена на веќе одобрениот систем за управување со квалитет или на списокот на системи за вештачка интелигенција опфатени од него, ќе биде доставена на внимание до овластеното тело од страна на провајдерот.

Предложените измени ќе ги разгледа овластеното тело, кое ќе одлучи дали модифицираниот систем за управување со квалитет продолжува да ги задоволува барањата наведени во точка 3.2 или дали е неопходна повторна процена.

Овластеното тело ќе го извести провајдерот за својата одлука. Известувањето ќе ги содржи заклучоците од проценатa на промените и причината за донесената одлука од проценатa.

4. Контрола на техничката документација

4.1. Во прилог на пријавата од точка 3, пријава со овластено тело по нивен избор ќе биде поднесена од провајдерот за процена на техничката документација која се однесува на системот за вештачка интелигенција кој провајдерот има намера да го пласира на пазарот или да го пушти во употреба и кој е покриен со системот за управување со квалитет наведен во точка 3.

4.2. Апликацијата ќе вклучува:

(а) име и адреса на провајдерот;

(б) писмена изјава дека истата пријава не е поднесена до ниедно друго овластено тело;

(в) техничка документација од Актот.

4.3. Овластеното тело ќе ја испита техничката документација. За оваа цел, на овластеното тело ќе му се даде целосен пристап до обуката и до тестирањето на збирките на податоци што ги користи провајдерот, вклучително и преку интерфејси за програмирање апликации (API) или други соодветни средства и алатки што овозможуваат далечински пристап.

4.4. При испитувањето на техничката документација, овластеното тело може да бара провајдерот да обезбеди дополнителни докази или да изврши дополнителни тестови за да овозможи правилна процена на усогласеноста на системот за вештачка интелигенција со барањата утврдени во Актот. Секогаш кога овластеното тело не е задоволно со тестовите што ги извршил провајдерот, овластеното тело директно ќе изврши соодветни тестови.

4.5. Онаму каде што е потребно да се процени сообразноста на системот за вештачка интелигенција со висок ризик со барањата утврдени во Актот и по образложено барање, надзорното тело, исто така, ќе добие пристап до изворниот код на системот за вештачка интелигенција.

4.6. За одлуката се известува провајдерот или неговиот овластен претставник. Известувањето ќе ги содржи заклучоците од оцената на техничката документација и образложената одлука за проценатa.

Кога системот за вештачка интелигенција е во согласност со барањата наведени во Актот, овластеното тело издава ЕУ-сертификат за оцена на техничката документација. Во сертификатот се наведува името и адресата на провајдерот, заклучоците од испитувањето, условите (доколку ги има) за неговата важност и податоците неопходни за идентификација на системот за вештачка интелигенција.

Сертификатот и неговите анекси ги содржат сите релевантни информации за да се овозможи процена на сообразноста на системот за вештачка интелигенција и да се овозможи контрола на системот за вештачката интелигенција додека е во употреба, онаму каде што е применливо.

Кога системот за вештачка интелигенција не е во согласност со барањата наведени во Актот, овластеното тело ќе одбие да издаде ЕУ-сертификат за оцена на техничка документација и соодветно ќе го извести барателот, давајќи детални причини за неговото одбивање.

Онаму каде што системот за вештачка интелигенција не го исполнува условот во врска со податоците што се користат за обука на системот, ќе биде потребна повторна обука на системот за вештачка интелигенција пред да се аплицира за нова оцена на сообразност. Во овој случај, образложената одлука од проценатa на надзорното тело кое одбива да го издаде ЕУ-сертификатот за оцена на техничката документација, ќе содржи конкретни размислувања за квалитетот на податоците што се користат за обука на системот за вештачка интелигенција, особено за причините за неусогласеност.

4.7. Секоја промена на системот за вештачка интелигенција што може да влијае врз усогласеноста на системот за вештачка интелигенција, барањата или неговата намена, ја одобрува овластеното тело кое го издало ЕУ-сертификатот за процена на техничката документација. Провајдерот ќе го информира таквото овластено тело за неговата намера да воведе некоја од горенаведените промени или ако на друг начин стане свесен за појавата на таквите промени. Предвидените промени ги оценува овластеното тело, кое ќе одлучи дали тие промени бараат нова оцена на сообразност со Актот, или дали тие би можеле да се решат со помош на дополнување на ЕУ-сертификатот за процена на техничката документација. Во вториот случај, овластеното тело ќе ги процени промените, ќе го извести провајдерот за својата одлука и, каде што промените се одобрени, на провајдерот ќе му издаде додаток на ЕУ-сертификатот за процена на техничката документација.

5. Надзор на одобрениот систем за управување со квалитет.

5.1. Целта на надзорот што го врши овластеното тело наведено во точка 3 е да се увери дека провајдерот соодветно ги исполнува условите и одредбите од одобрениот систем за управување со квалитет.

5.2. За целите на проценатa, провајдерот му дозволува на овластеното тело пристап до простории во кои се одвива дизајнот, развојот и тестирањето на системите за вештачка интелигенција. Провајдерот дополнително ќе ги сподели со овластеното тело сите потребни информации.

5.3. Овластеното тело врши периодични ревизии за да се увери дека провајдерот го одржува и го применува системот за управување со квалитет и ќе му достави на провајдерот ревизорски извештај. Во контекст на тие ревизии, овластеното тело може да изврши дополнителни тестови на системите за вештачка интелигенција за кои е издаден ЕУ-сертификат за процена на техничката документација.