ВОДИЧ ЗА ОФИЦЕРИ ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ ВО ЈАВНИ ИНСТИТУЦИИ

МЕТАМОРФОЗИС
Фондација за интернет и општество

КОНЕКТ

ВОДИЧ ЗА ОФИЦЕРИ ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ ВО ЈАВНИ ИНСТИТУЦИИ

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. Листа на кратенки 6
2. Вовед 7
3. Цел 8
4. Дефиниции 9
5. Агенција за заштита на личните податоци (АЗЛП) 10
6. Начела поврзани со обработката на личните податоци и нивна примена 11
    6.1. Законитост, правичност и транспарентност 11
        6.1.1. Законитост 12
        6.1.2. Правичност 15
        6.1.3. Транспарентност 16
    6.2. Ограничување на целта 16
    6.3. Минимален обем на податоци 16
    6.4. Точност 17
    6.5. Ограничен рок на чување 17
    6.6. Безбедност (интегритет и доверливост) 17
7. Отчетност 18
8. Права на субјектите на личните податоци 21
9. Директен маркетинг 25
10. Офицер за заштита на личните податоци 26
    10.1. Определување офицер за заштита на личните податоци 26
    10.2. Потребни квалификации 27
    10.3. Улога на офицерот за заштита на личните податоци 28
11. Задачи и одговорности на офицерот за заштита на личните податоци . 29
    11.1. Прелиминарна функција 30
    11.2. Организациска функција: 33
        Задача 1: Подготовка на евиденција (регистар) на активности за обработка на личните податоци 33
        Задача 2: Преглед на активностите за обработка на личните податоци 34
        Задача 3: Процена на ризиците во врска со активностите за обработка на личните податоци 38
        Задача 4: Управување со активностите за обработка на личните податоци за кои е веројатно дека ќе резултираат со „висок ризик“ за слободите и правата на субјектите, врз основа на спроведена процена на влијанието врз заштитата на личните податоци. 46

Задача 5: Управување со нарушувањето на безбедноста на личните податоци ... 52
Задача 6: Поддршка и промовирање „Техничка и интегрирана заштита на личните податоци“ ... 55
Задача 7: Односи со трети страни (заеднички контролори, контролор–контролор, контролор–обработувач како и клаузули за пренос на лични податоци) ... 56
Задача 8: Постапување по барањата на субјектите на личните податоци ... 56
Задача 9: Следење на функциите за усогласеност односно повторување на активностите од организациските функции, на тековна основа ... 58
11.3. Советодавна функција ... 59
11.4. Ревизорска функција ... 61
12. Соработка со Агенцијата ... 63
Национален портал за е-услуги (uslugi.gov.mk) ... 65
Вештачката интелигенција и обврските на ОЗЛП ... 67
Ефектот на вештачката интелигенција врз човековите права ... 70
ДЕЛ 4 – ПРИЛОЗИ ... 77
Прилог 1 – Предлог-евиденција на активностите за обработка на личните податоци (контролор и обработувач) ... 77
Примерок формат од евиденцијата за обработка на личните податоци на контролорот ... 77
Примерок формат од евиденцијата за обработка на личните податоци на обработувачот ... 78
Прилог 2 – Предлог-детали за мапирање на активностите за обработка на личните податоци ... 80
II.1. Податоци и извори на податоци ... 80
II.2. Обелоденување податоци ... 82
II.3. Правна основа за обработка ... 83
II.4. Информирање на субјектите на личните податоци ... 84
II.5. Прекугранично пренос на податоци (пренос на податоци во трети земји) ... 88
Прилог 3: Пристап усвоен од ENISA (Европска агенција за кибербезбедност) која се надоврзува на меѓународно прифатениот стандард ISO 27005: „Заканите ги злоупотребуваат ранливостите на средствата што доведува до предизвикување штета на организацијата“; ... 93

Прилог 4 – Примери за нарушување на безбедноста на личните податоци и кој да се извести (Од упатствата на WP29) 97
Прилог 5 – Контролна листа за офицерот за заштита на личните податоци во поглед на усогласеноста на работењето на контролорот со Законот за заштита на личните податоци и соодветните подзаконски акти од областа на заштитата на личните податоци.....99
Прилог 6 – Листа за проверка за примена на технички и организациски мерки во согласност со правилникот за безбедност и најдобрите практики од ЕУ..... 110
Прилог 6 – Листа за проверка за клучните области на дејствување во врска со ВИ и човековите права 113

1. ЛИСТА НА КРАТЕНКИ

АЗЛП – Агенција за заштита на личните податоци

ЗЗЛП – Закон за заштита на личните податоци

ОЗЛП – Офицер за заштита на личните податоци

GDPR – Општа регулатива за заштита на личните податоци (General Data Protection Regulation)

МИОА – Министерство за информатичко општество и администрација

ВИ – Вештачка интелигенција

EDPS – Европски супервизор за заштита на лични податоци (European Data Protection Supervisor)

ПВЧП – Процена на влијанието врз човековите права

2. ВОВЕД

Заштитата на личните податоци не е новина во правниот систем на Република Северна Македонија, ниту во државите на Европската Унија. Сепак, ова човеково право популарноста ја стекнува посебно по донесувањето на Општата регулатива за заштита на личните податоци (General Data Protection Regulation 2016/6792[1] – GDPR) во 2016 година, која на изненадување на многумина го помина браникот на бизнис-отпорот и најави ригорозни правила и услови за обработката на личните податоци на граѓаните на ЕУ. Мотивот и целта на ваквата регулатива многумина ја гледаат во развојот на новите технологии, дигитализацијата и глобализацијата каде што личните податоци се оние кои ги движат ваквите процеси. Република Северна Македонија, во процесот на хармонизација на своето законодавство со законодавството на ЕУ, на 24.02.2020 година ја преточува Општата регулатива за заштита на личните податоци (GDPR) во свој национален Закон за заштита на личните податоци (lex generalis)[2]. На овој начин, уште еднаш се нагласува важноста на правото на заштита на личните податоци, како дел од основните права и слободи на граѓаните и како суштинска вредност на секое модерно и технолошки развиено општество.

Законот за заштита на личните податоци (во понатамошниот текст: ЗЗЛП) својата материјална примена ја наоѓа во секоја ситуација која подразбира обработка на личните податоци на граѓаните на Република Северна Македонија, без оглед на тоа дали физичкото односно правното лице што ја врши обработката е од приватниот, државниот или граѓанскиот сектор, притоа водејќи се од концептот на гарантирање на приватноста и личниот интегритет на поединецот. Исклучокот постои само кај оние обработки на лични податоци коишто се вршат од физички лица заради лични активности, односно активности во домот.

Државните и јавни институции потребно е да ги применуваат овие прописи за заштита на личните податоци, независно од тоа дали активностите за обработката на личните податоци на физички лица се во хартиена или електронска форма. Под државни и јавни институции влегуваат сите органи на државната и локалната власт и други државни органи основани во согласност со Уставот и со закон, институциите што вршат дејности од областа на образованието, науката, здравството, културата, трудот, социјалната заштита и заштитата на детето, спортот, како и други дејности од јавен интерес утврден со закон (агенции, фондови, јавни установи и јавни претпријатија, основани од Република Северна Македонија или од општините, од градот Скопје, како и од општините во градот Скопје). Во вакви случаи, определувањето офицер за заштита на личните податоци е задолжително, без оглед на видот и обемот на личните податоци што се обработуваат.

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj (General Data Protection Regulation 2016/6792 – GDPR).

[2] Закон за заштита на личните податоци (Службен весник на РСМ, бр. 42 од 16.02.2020).

3. ЦЕЛ

Целта на овој Водич е да даде практични насоки и препораки како да се пристапи кон примената на важечките прописи од областа на заштитата на личните податоци од страна на државните и јавните институции, во улога на контролори, како и за офицерите за заштита на личните податоци кои се назначени од нивна страна. За негово подобро разбирање, неопходно е претходно читање на Законот за заштита на личните податоци и релевантните подзаконски акти.

Водејќи се од европската регулатива и најдобрите меѓународни и домашни практики од оваа област, овој Водич одговара и дава практични насоки за тоа што е потребно да биде усвоено и применето од страна на контролорите и обработувачите при активностите на обработка на личните податоци, а во насока на полесно разбирање и спроведување на одредбите од релевантната регулатива, притоа минимизирајќи го ризикот од евентуална злоупотреба, како и земајќи ги предвид најновите технологии и технолошки решенија.

Дополнително, овој Водич е посебно наменет да му помогне на лицето назначено на позиција – офицер за заштита на личните податоци – преку обезбедување детални чекори и практични примери за поедноставно извршување на неговите задачи, одговорности и предизвици, во согласност со применливите прописи од оваа област.

За таа цел, овој Водич е поделен на четири дела:

- **ДЕЛ 1**, дава преглед на законските одредби што се однесуваат на определувањето офицер за заштита на личните податоци како и потребните квалификации за назначување на оваа работна позиција;
- **ДЕЛ 2**, детално ги објаснува работните задачи на офицерите, обврските на контролорите и обработувачите, проследени со практични примери од домашната и меѓународната добра практика, особено во поглед на позитивните искуства од досегашната примена на Општата регулатива за заштита на личните податоци, што вклучува и преглед на начелата и правата на субјектите на лични податоци во делот на испораката на електронските јавни услуги на личните податоци.
- **ДЕЛ 3**, ги појаснува примената и влијанието на вештачката интелигенција (во понатамошниот текст: ВИ) врз човековите права, и
- **ДЕЛ 4**, се Прилозите кон овој Водич каде се дадени теркови на обрасци и помошни материјали за нивна примена во секојдневното работење.

4. ДЕФИНИЦИИ

Дефинирањето на термините е во согласност со Законот за заштита на личните податоци и служи за да ги појасни основите врз кои се темели правото на заштита на личните податоци, и тоа:

- **Личен податок** е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може директно или индиректно да се идентификува со помош на идентификатор. Пример за лични податоци се: име и презиме, ЕМБГ, локација, IP-адреса, онлајн идентитет, електронска пошта, потрошувачки навики, банкарски информации и сл.
- **Посебна категорија лични податоци** се оние лични податоци што малку повеќе задираат во приватноста на физичките лица, како што се: расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето или податоци за сексуалниот живот или сексуалната ориентација на физичкото лице.
- **Субјект на лични податоци** е физичкото лице чии лични податоци се обработуваат.
- **Обработка на лични податоци** е секоја активност која се извршува врз личните податоци, автоматски или на друг начин, како што се: собирање, евидентирање, организирање, структурирање, чување, приспособување или промена, повлекување, консултирање, увид, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, усогласување или комбинирање, ограничување, бришење или уништување.
- **Цел на обработка** претставува причината поради која се обработуваат личните податоци заради исполнување законска обврска, договор или вршење работи од јавен интерес.
- **Активност за обработка на лични податоци** претставува секоја поединечна деловна активност за чиешто вршење се неопходни лични податоци. Примери за активности за обработка на личните податоци се: исплата на плата, евиденција на работното време, склучување договор за вработување, внесување нов вработен во апликација за човечки ресурси, издавање дозволи и уверенија, пресметка на данок и други јавни давачки, упис на ученици во основно и средно образование, обезбедување здравствена заштита и слично.

За примарна дејност на контролорот се сметаат клучните активности што се потребни за постигнување на целите на контролорот, при што примарната

дејност не мора да биде само онаа која се однесува на обработката на личните податоци, туку и другите активности што предвидуваат обработка на личните податоци (пр., давањето услуги во областа на електронските комуникации, профилирањето, следењето на локацијата преку мобилните апликации, следењето на податоците за здравјето преку мобилните апликации, итн.). Овие примери се однесуваат на редовното и систематското следење на субјектите на личните податоци, односно на сите форми на следење и профилирање преку интернет, а терминот следење не е ограничен само на виртуелната средина.

Имено, со развојот на технологијата сè повеќе се актуализира и прашањето на вештачката интелигенција. И покрај позитивните аспекти што со себе ги носи овој развој, сепак, посебно при пишувањето на регулативата (законска и подзаконска), се очекува да се посвети посебно внимание на човековите права, владеењето на правото и етиката, доколку се користи ВИ во деловните процеси на институциите.

Во поглед на органите на државната власт, употребата на ВИ и основните технологии имаат свое влијание во поглед на широк спектар области, вклучувајќи ги здравството, образованието, спроведувањето прописи и општествената одговорност. Во таа насока, се наметнуваат низа прашања што има потреба да бидат разгледани, бидејќи ВИ има потенцијал да ги наруши токму човековите права и да ги поткопа законите што ги штитат.

Обработката на голем обем податоци, во комбинација со ВИ, може да го загрози правото на приватност, поради постоење ризик од зголемен надзор и мониторинг на поединците. Лицата кои имаат пристап до технологијата што ја овозможува ВИ можат да пребаруваат јавни записи и други достапни податоци значајно побрзо отколку што би било можно, без користење на технологија.

5. АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (АЗЛП)

Агенцијата за заштита на личните податоци е самостоен независен државен орган надлежен да врши надзор на законитоста на преземените активности при обработката на личните податоци на територијата на Република Северна Македонија како и да врши заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци.

Главната цел на Агенцијата е јакнење, промоција и заштита на приватноста на податоците на физичките лица преку спроведување надзор, давање насоки, како и мислења во согласност со законските прописи.

6. НАЧЕЛА ПОВРЗАНИ СО ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ И НИВНА ПРИМЕНА

Законот за заштита на личните податоци дозволува обработка на личните податоци, доколку при обработката се применети пропишаните шест начела[3].

Откако прецизно и детално ќе се утврдат сите активности за обработката на личните податоци во рамките на институцијата, тогаш следниот чекор е на секоја поединечна активност да се применат овие начела.

Контролорите се должни да дејствуваат во согласност со начелата за заштита на личните податоци.

6.1. Законитост, правичност и транспарентност

Личните податоци можат да се обработуваат единствено доколку постои законска основа[4] за обработка и на начин што е правичен и транспарентен кон субјектот на личните податоци, чии лични податоци се обработуваат.

[3] Член 9 став 1 од Законот за заштита на личните податоци (Службен весник на РСМ, број 42 од 16.2.2020 година).

[4] Член 10 од Законот за заштита на личните податоци (Службен весник на РСМ, број 42 од 16.2.2020 година).

6.1.1. Законитост

За да може да се спроведе активноста за обработка на личните податоци, мора да постои законска основа за таквата обработка. Притоа, законитоста не значи нужно дека обработката мора да биде во согласност со конкретен закон, како што повеќето од нас првично ќе помислат, туку дека обработката на личните податоци смее да се врши исклучиво според одредени правила што ги пропишува ЗЗЛП. Иако постојат шест видови законски основи, само пет од нив се применливи за јавниот сектор, и тоа се:

6.1.1.1. Законска обврска:

Активноста за обработката на личните податоци која е потребна за институцијата да исполни законска обврска е онаа активност која својата законитост ќе ја најде во член 10 став 1 алинеја 3 од Законот. Доколку за конкретна активност во Евиденцијата на активностите за обработка се утврди законска основа, понатаму е лесно да се препознаат активностите што институцијата има законска обврска да ги преземе.

Примери:

- Обработката на податоците за исплата на плата на вработените, поради тоа што институцијата има законска обврска на своите вработени да им исплати плата и таа обврска не може да ја исполни, без претходно да им ги обработи личните податоци.
- Обработката на личните податоци од страна на надлежниот центар за социјална работа има правна основа (Закон за социјална заштита[5]) на потенцијалниот корисник на гарантирана минимална помош да му обработува лични податоци какви што се име, презиме, адреса на живеење, место на раѓање, ЕМБГ, образование, работен статус, државјанство, етничка припадност, број на лична карта и сл.

6.1.1.2. Исполнување договор:

Обработката е потребна за исполнувањето на договорот каде што едната договорна страна е субјектот на личните податоци, или за да се преземат активности за барање на субјектот на лични податоци пред склучување на договорот (член 10 став 1 алинеја 2 од Законот). Во таа насока, доколку активноста не произлегува од договорот, тогаш обработката на личните податоци мора да биде опфатена со некој друг правен основ.

Примери за активност која својата законитост ја наоѓа во овој основ:

- обработка на лична биографија доставена по распишан оглас за вработување, како активност којашто му претходни на договорот за вработу-

[5] (Службен весник на РСМ, бр.104 од 23.5.2019).

вање (без оглед што тој може и да не биде склучен поради неизбирање на кандидатот).

- обработка на лични податоци (име, презиме, адреса и ЕМБГ) за склучување договор за јавна набавка каде носителот е физичко лице.

6.1.1.3. Заштита на живот или суштински интерес:

Обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице.

Овој правен основ се користи во ретки ситуации, кога активноста за обработка на личните податоци може да биде потребна за спасување на нечиј живот, што најчесто е поврзано со потреба за обезбедување на итна медицинска помош.

Пример:

- обработка на лична карта или друг документ за идентификација на лице во бессознание, со цел да му се укаже прва помош или возачка дозвола за да се види крвна група.

6.1.1.4. Вршење работи од јавен интерес или јавно овластување:

Обработката е потребна за извршување работи од јавен интерес или при вршење јавно овластување на контролорот утврдено со Закон.

Пример:

- За запишување ученици во средните училишта, согласно Законот за средното образование, се собираат лични податоци како име и презиме на ученикот, датум и место на раѓање, адреса и место на живеење, место на раѓање, пол, презиме и име на родители или старатели.
- За целите за аплицирање за стипендии, Министерството за образование и наука, покрај името и презимето, адресата на живеење на студентот, ги собира и податоците за државјанство, трансакциска сметка, како и постигнатиот успех на учениците.

6.1.1.5. Согласност:

Субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или повеќе конкретни цели. Согласноста мора да биде слободно дадена, јасна и треба лесно да може да се повлече, па затоа контролорите треба да внимаваат, секогаш кога како правен основ за обработка на лични податоци се користи добиена согласност (повеќе не се дозволуваат практиките со автоматско означување на полиња за согласност).

Пример:

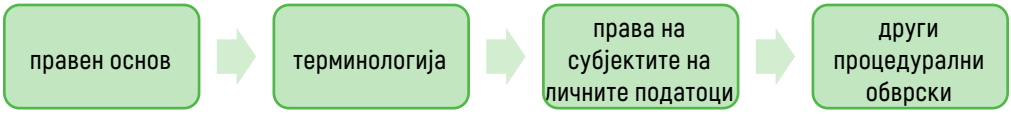
Обработката на податоците на институцијата за објава на фотографиите е дозволена доколку има стриктна согласност од субјектот/родител/старател

на лични податоци за целите на објавата на фотографии на деца од воспитно-образовна установа.

Напомена: *Во поглед на правниот основ од точка 5.1.1, при хармонизација на секторската легислатива со Законот за заштита на личните податоци, Агенцијата за заштита на лични податоци има донесено Одлука за утврдување на методологијата за хармонизација на секторската легислатива*[6].

Во таа насока, првиот чекор на надлежните министерства е проверка и идентификување дали одреден закон се однесува на собирање, обработка, чување, користење и доставување на личните податоци, односно дали вклучува какви било активности за обработка на личните податоци. Се препорачува да бидат идентификувани релевантните постојни закони што треба да се променат (изменат и дополнат) за тие да можат понатаму бидат усогласени со одредбите од Законот за заштита на личните податоци. Во случај на подготовка на нови закони во кои има активности за обработка на личните податоци, одговорноста за усогласеноста на новото законско решение е на министерството што го предлага тој закон.

Со цел да се оцени дали се исполнети одредени барања што произлегуваат од Законот за заштита на личните податоци, за проверка на постојните и новите закони што се однесуваат на обработката на личните податоци, можат да се послужат следните критериуми:



1. Правен основ на обработка

- Обработката на личните податоци е законита, само ако и до оној степен доколку за неа има правен основ за обработка (пр., исполнување законска обврска, извршување работи од јавен интерес или при вршење на јавно овластување и сл.).

2. Приспособување на терминологијата

- Термините што се користат во важечките закони треба да се приспособат на терминологијата од Законот за заштита на личните податоци, за да се обезбеди правна конзистентност (пр., Користење на терминот „обработка" за дефинирање на сите операции или збирот операции што се извршуваат врз личните податоци).

3. Права на субјектите на личните податоци

- Дефинирање на ограничувањата на правата на субјектите директно во самиот закон и со исполнување на одредени барања од Законот за

[6] (Службен весник на РСМ, бр. 38 од 21.2.2022).

заштита на личните податоци (оправдано ограничување заради потребата за обезбедување на една или повеќе цели и законска одредба која го дефинира ограничувањето).

4. Други процедурални обврски

- Проверка дали важечкиот закон содржи и дали е потребно да се вградат конкретни законски одредби (пр., Обврска за бришење, коригирање или ограничување на обработката). Ваквите обврски треба да се спроведуваат по службена должност од страна на јавните органи, бидејќи таа обврска постои без оглед на фактот дали субјектот на личните податоци побарал остварување на неговото право за бришење на личните податоци или не.

6.1.1.5. Легитимен интерес

Обработката која се заснова на легитимен интерес на контролорот, **не е применлива за јавниот сектор**. Генерално, овој основ се дефинира како деловен интерес на контролорот да врши одредена активност за обработка на личните податоци и тој интерес да преовладува над правата и слободите на субјектите чии лични податоци се засегнати со активноста на обработка.

Кога организацијата користи легитимен интерес како правен основ за обработка, таа мора да спроведе тест за балансираност, односно да утврди дали активноста за обработка е неопходна за организацијата да функционира/да ја врши својата дејност, односно дали активноста на обработката може да се смета дека не преовладува над правата и слободите на субјектот на лични податоци. Доколку со одговорите на овие прашања се покаже дека се преовладува над интересите или основните права и слободи на субјектот, тогаш организацијата не може да го користи легитимниот интерес како правен основ за обработката.

За една активност да биде законита, доволно е да е остварен еден од наведените законски основи. Вообичаена погрешна пракса е да се бара согласност од субјектите на личните податоци и покрај тоа што постои друг законски основ за активностите на обработка на личните податоци.

6.1.2. Правичност

Правичноста, односно фер обработката подразбира дека субјектот на личните податоци мора да биде свесен за фактот дека неговите лични податоци се обработуваат, да ја знае целта на обработката и како тие податоци се собираат, чуваат и користат, што ќе му овозможи да донесе информирана одлука дали е согласен со таквата обработка (во случаите кога обработката е заснована на согласност) и дека има можност да ги користи своите права за заштита на личните податоци[7].

[7] Глава IX од овој Водич.

6.1.3. Транспарентност

Нетранспарентноста при обработката на личните податоци историски е позната како еден од најголемите ризици врз приватноста на физичките лица. Различни организации за своите потреби собираат различни податоци, без притоа физичкото лице да биде информирано, за која цел се собираат неговите лични податоци, како се обработуваат, колку се чуваат и слично.

Тесно поврзана со правичноста, транспарентноста подразбира дека институциите мора да бидат отворени и јасни кон субјектите на личните податоци, пред да започнат со обработката на нивните лични податоци. На пример, со презентирање на Известување за приватност, Политика за приватност, Политика за употреба на колачиња и сл., со што субјектот би бил запознаен со деталите за обработката уште пред да ги даде своите лични податоци.

Пр., Изработка на Политика за приватност со која ќе се предвидат општи податоци за обработката на личните податоци за посета на официјалната интернет-страница и/или користење одредени административни услуги преку неа, а заради остварување на законските задачи и овластувања.

Интернет-страницата и таквите обрасци треба јасно да дадат информации за тоа како субјектите на личните податоци можат да ги остварат своите права (вклучувајќи јасна јавна објава со контакт податоци за офицерот – иако тоа не треба неопходно да вклучува име и презиме на офицерот);

6.2. Ограничување на целта

Личните податоци треба да се собираат само за конкретни, јасни и легитимни цели и тие не смеат да бидат предмет на обработка, на начин кој не е во согласност со тие цели. Сепак, натамошната обработка на личните податоци за целите на архивирањето од јавен интерес, за научни и историски истражувања и за статистички цели, согласно член 86, став (2) од ЗЗЛП, не се смета за несоодветна, согласно иницијалната цел за обработката.

6.3. Минимален обем на податоци

Обработката на личните податоци мора да биде соодветна, релевантна и ограничена, само на она што е неопходно за постигнување на целите на таквата обработка и во таа насока доколку целта на обработката не може разумно да се постигне на друг начин.

6.4. Точност

Контролорите мора да се осигурат дека личните податоци се точни и, кога тоа е потребно, да ги ажурираат, со преземање разумни чекори/мерки за бришење, односно исправка на неточните лични податоци, без непотребно одложување и во согласност со целта за која се обработуваат. Конкретно, контролорите треба точно да ги запишуваат информациите што ги собираат или добиваат, заедно со изворот на таквите информации.

6.5. Ограничен рок на чување

Личните податоци треба да се чуваат во форма која дозволува идентификација на субјектите на личните податоци, за периодот потребен за целите за кои се обработуваат. Во таа насока, потребно е контролорите да предвидат временски рок за бришење на личните податоци или за периодична ревизија. При дефинирање на рокот на чување, контролорот најпрво мора да се осигури дали постојат дефинирани законски рокови за чување на личните податоци, па доколку не, ќе мора да ги дефинира роковите со свои интерни правила.

6.6. Безбедност (интегритет и доверливост)

Личните податоци треба да се обработуваат на начин кој обезбедува соодветна безбедност и доверливост на нив, вклучително и заштита од неовластен или незаконски пристап или користење на личните податоци и опремата што се користи за обработка, како и од случајно губење, уништување или оштетување, преку примена на соодветни технички и организациски мерки.

Контролорите се одговорни за усогласеноста со сите горенаведени начела за заштитата на личните податоци, во насока на преземање одговорност за нивната обработка на личните податоци и усогласеноста со ЗЗЛП, да демонстрираат усогласеност и да бидат во можност да ја докажат, вклучително и пред АЗЛП, со приложување евиденција и примена на соодветни мерки.

7. ОТЧЕТНОСТ

Отчетноста[8] претставува една од новините во законската регулатива. Од особена важност е да се разбере значењето на терминот отчетност кој Законот го опишува како обврска на контролорот да работи според начелата што се однесуваат на обработката на личните податоци, како и должноста да може да го докаже тоа.

Поинаку кажано, отчетноста најдобро би се опишала како збир обврски со кои треба да се усогласи институцијата за да биде во можност да ја покаже и докаже усогласеноста со применливата регулатива за заштита на личните податоци. Токму отчетноста, како законско барање, ни укажува дека патот на една институција до целосно усогласување на своето работење со Законот за заштита на личните податоци и релевантните подзаконски акти не е еднократен, туку претставува непрекинат процес, кој има свој почеток и е предмет на постојано надградување. Причината за тоа е што Законот не „бара" да се усогласи институцијата, туку да се усогласи начинот на работењето, што подразбира имплементирање правила на дејствување што овозможуваат заштита на личните податоци кои се користат и обработуваат во работните процеси на институцијата.

Едноставното усвојување и имплементирање внатрешни политики и процедури, или формално комплетирање одредени формулари/изјави и сл., повеќе не се доволни за една институција да се смета за усогласена со применливата регулатива, туку мора да се работи на воспоставувањето суштински правила за дејствување, подигнување на свеста и, со тоа, градење на културата за заштита на личните податоци од страна на сите вклучени чинители.

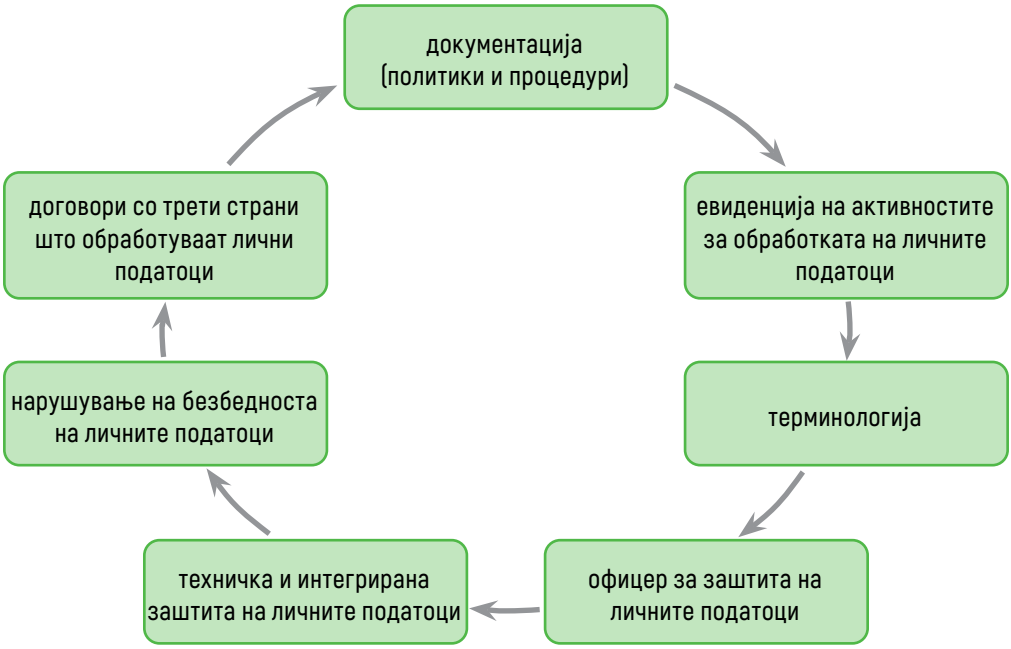
7.1. Демонстрирање на отчетноста

Демонстрирањето на отчетноста од страна на јавните институции предвидува повеќе фази што графички би можеле да се претстават на следниот начин:

7.1.1. Документација (Изработка на политики и процедури што ги опфаќаат сите активности на обработка)

Документацијата игра значајна улога во новините поврзани со отчетноста. Таа му овозможува на контролорот и/или обработувачот на лични податоци да ја гарантира и покаже усогласеноста со неговите обврски, како и презетите чекори.

[8] Член 9 став 2 од Законот за заштита на личните податоци (Службен весник на РСМ бр. 42 од 16.02.2020 година).



Обезбедувањето на документацијата предвидува повеќе аспекти како што се евиденција на активностите за обработка, процена на влијанието на заштитата на личните податоци, евиденција за нарушувањето на безбедноста на личните податоци, како и преземените корективни мерки, информативни известувања, докази за обезбедување согласност од субјектите на личните податоци, процедури што се однесуваат на остварување на правата, договори со обработувачите и надворешните лица кои се даватели на услуги, алатки за надзор на преноси надвор од Европската унија, писмена анализа на офицерот за непостоење на судир на интереси итн.

Документацијата, како суштинска алатка, дава детален преглед на спроведените активности за обработката на личните податоци и овозможува да се планира нивното управување. Од тие причини, потребно е документацијата да биде чувана, односно да се осигури дека таа е релевантна, односно е предмет на редовно ажурирање.

7.1.2. Евиденција на активностите за обработка на личните податоци

Во однос на водењето евиденција за активностите за обработка, таа претставува обврска на контролорот, односно обработувачот на лични податоци.

Преку евиденцијата се спроведува следењето на имплементираните активности за обработка на личните податоци, овозможувајќи му на офицерот целосен увид во активностите за обработка и, следствено, можност за предлагање мерки, потребни за нивен редовен надзор.

7.1.3. Процена на влијанието на заштитата на личните податоци (ПВЗЛП)

Со вршењето на ПВЗЛП, каде што е потребно, јавните институции ќе ја демонстрираат отчетноста со ефективно документирање и со осврнување кон обработките што можат да резултираат со висок ризик по правата и слободите на физичките лица.

7.1.4. Офицер за заштита на лични податоци

Назначувањето на офицерот за заштита на личните податоци е еден од начините на кој јавната институција ја демонстрира својата отчетност.

7.1.5. Техничка и интегрирана заштита на личните податоци

Овој пристап природно ќе ги води јавните институции до отчетност и усогласеност. Техничката и интегрирана заштита на личните податоци значи дека правото на приватност е земено предвид во секој чекор од обработката – од собирањето на личните податоци па сè до нивното евентуално бришење.

7.1.6. Нарушување на безбедноста на личните податоци

Одржување записи за нарушувањата на безбедноста на личните податоци и, каде што е потребно, пријавување нарушувања на безбедноста на личните податоци е, исто така, начин на којшто се демонстрира отчетноста.

7.1.7. Договори со трети страни што обработуваат лични податоци

Склучување договори со организациите што обработуваат лични податоци во име на институцијата, без разлика дали станува збор за однос контролор со контролор, контролор со обработувач или заеднички контролори.

Отчетноста, како таква, е непрекинат процес. Мерките коишто сте ги примениле мора редовно да се ревидираат и, кога е потребно, да се ажурираат.

Отчетноста може да ви помогне да изградите доверба кај субјектите на личните податоци и може да ви помогне при супервизија од страна на Агенцијата за заштита на личните податоци.

8. ПРАВА НА СУБЈЕКТИТЕ НА ЛИЧНИТЕ ПОДАТОЦИ

Субјектите на личните податоци ги имаат следните права:

- Право на информираност;
- Право на пристап;
- Право на исправка;
- Право на бришење;
- Право на ограничување на обработката;
- Право на преносливост;
- Право на приговор;
- Право да не биде предмет на автоматизирано донесување поединечни одлуки и профилирање;
- Право на поднесување барање до Агенцијата.

8.1. Право на информираност

Според законот, субјектот на личните податоци има право да биде информиран за идентитетот на контролорот, неговите контакт-податоци, целта на обработката, законската основа на обработката и други релевантни информации коишто се неопходни за да осигурат правична и транспарентна обработка на личните податоци.

Пр.: Известување за приватност, Политика за приватност и сл.

8.2. Право на пристап

Секој субјект на лични податоци може да побара информација од контролорот дали се обработуваат неговите лични податоци и, доколку се обработуваат, да добие пристап до личните податоци и тоа: за целите на обработката, категориите на личните податоци што се обработуваат, корисниците или категориите корисници на кои се откриени или ќе бидат откриени личните податоци, особено корисниците во трети земји или меѓународни организации, предвидениот рок за кој ќе се чуваат личните податоци, има право да се бара, од страна на контролорот, исправка или бришење на личните податоци или ограничување на обработката на личните податоци поврзани со субјектот на личните податоци, или право на приговор против таквата обработка, право на поднесување барање до АЗЛП, кога личните подато-

ци не се собираат од субјектот на личните податоци, и сите достапни информации за нивниот извор и постоењето на автоматизиран процес на одлучување, вклучително и профилирањето на кои контролорот треба да му одговори... Контролорот е должен да обезбеди копија од личните податоци што се обработуваат. Ако субјектот на личните податоци поднесе барање по електронски пат, на субјектот на личните податоци информациите ќе му бидат обезбедени на вообичаен начин кој се користи во случај на електронска форма, освен ако субјектот на личните податоци не побарал поинаку.

8.3. Право на исправка

На барање на субјектот на лични податоци, контролорот е обврзан да ги дополни, измени и избрише личните податоци или да престане со обработката на личните податоци, во случаи кога тие се нецелосни, неточни или застарени, или доколку обработката е незаконска.

Без оглед на фактот дали субјектот на лични податоци поднесол лично барање, кога утврдил дека личните податоци се нецелосни, неточни или застарени, контролорот е обврзан да ги дополни, измени или избрише.

Рокот за исправка е **15 дена** од денот на поднесувањето на барањето.

8.4. Право на бришење

Субјектот на личните податоци има право да побара од контролорот да ги избрише неговите лични податоци, доколку е исполнет некој од следните услови:

- Личните податоци повеќе не се потребни за целите за коишто биле собрани.
- Доколку обработката се засновала на согласност, а субјектот на личните податоци ја повлекол согласноста.
- Субјектот на личните податоци поднесол приговор против обработката.
- Личните податоци биле обработувани незаконски.
- Личните податоци треба да бидат избришани како резултат на законска обврска на контролорот.
- Личните податоци биле собрани во врска со услуги од информатичко општество на деца.

Доколку контролорот ги објавил јавно личните податоци за коишто е побарано да бидат избришани (на пр., социјални медиуми), мора да преземе разумни мерки за да ги информира сите трети страни коишто во меѓувреме

ги преземале личните податоци за да ги обработуваат како контролори, за остварување на правото на бришење.

Контролорот може да го одбие барањето на субјектот на личните податоци да ги избрише неговите податоци, доколку обработката е потребна за остварување на правото на слобода на изразување и информирање, за усогласување на контролорот со законската обврска или за извршување работи од јавен интерес меѓу кои и јавното здравство, како и за целите на архивирањето од јавен интерес за научни, историски или статистички истражувања.

Рокот за исправка е **30 дена** од денот на поднесувањето на барањето.

Напомена: *Контролорот мора за ова барање да ги извести трети страни (корисници) на кои им се дадени на користење конкретните лични податоци.*

8.5. Право на ограничување на обработката

Субјектот на личните податоци има право да побара ограничување на обработката на неговите лични податоци доколку:

- Точноста на личните податоци е оспорена од страна на субјектот (обработката ќе биде ограничена додека се провери точноста на податоците).
- Обработката е незаконска, а субјектот се спротивставува личните податоци да се избришат.
- Контролорот нема повеќе потреба од личните податоци од причина што целта за нивната обработка е исполнета, а субјектот бара да се чуваат поради остварување на негови правни барања.
- Субјектот на личните податоци поднесол приговор за обработката и додека се чека верификација чии интереси преовладуваат (легитимните интереси на контролорот наспроти интересите на субјектот) обработката се ограничува.

Напомена: *Последниот услов од ова право не е применлив за јавните институции поради тоа што легитимниот интерес како правен основ не е применлив за јавните институции.*

8.6. Право на преносливост

Законот му дава право на субјектот на личните податоци да ги добие неговите лични податоци во структуриран, вообичаено користен и машински читлив формат. Исто така, субјектот на личните податоци има право овие лични податоци да ги пренесе на друг контролор, без попречување од стра-

на на контролорот од кого се бара преносливоста. Условите под кои ова право може да се искористи се:

- Тој му ги има дадено личните податоци на контролорот.
- Обработката се врши врз основа на согласност или врз основа на договорна обврска.
- Обработката се врши на автоматизиран начин.

8.7. Право на приговор

Доколку личните податоци на субјектот се обработуваат врз основа на јавен интерес на контролорот, вклучувајќи профилирање и директен маркетинг, субјектот има право да поднесе приговор против таквата обработка. Контролорот, како одговор на приговорот, ќе мора да ја запре обработката, освен ако не докаже дека неговиот интерес преовладува над интересите, правата и слободите на субјектот на личните податоци.

Напомена: *Ова право мора да се предочи на субјектот на јасен начин, издвоено како информација од останатите информации коишто му се даваат во Известување за приватност, Политиката за приватност и сл.*

8.8. Право да не биде предмет на автоматизирано донесување на поединечни одлуки и профилирање

Ова право се однесува само на оние одлуки што се засновани исклучиво на автоматска обработка и профилирање и кои предизвикуваат правни последици или на сличен начин влијаат на субјектот на личните податоци. Контролорот ќе го одбие ова барање доколку одлуката која е предмет на автоматска обработка или профилирање:

- е потребна за склучување или извршување договор меѓу субјектот на личните податоци и контролорот,
- е дозволена со закон којшто се применува во однос на контролорот, или
- се заснова на изречна согласност на субјектот на личните податоци.

8.9. Право на поднесување барање до Агенцијата за заштита на личните податоци

Секој субјект на лични податоци има право да поднесе барање до Агенцијата доколку смета дека обработката на личните податоци ги прекршува од-

редбите од овој закон, притоа не доведувајќи ги во прашање кои било други управни или судски средства за правна заштита.

Во врска со овие права, офицерот за заштита на личните податоци е задолжен за остварување на правата на субјектите на лични податоци и за исполнување на обврските на контролорот.

9. ДИРЕКТЕН МАРКЕТИНГ

Маркетингот често ја преминува границата на приватноста, со што посебно се занимава новиот ЗЗЛП. Секое современо купување, бара собирање на одредени лични податоци и вклучува активности насочени кон откривањето на намерите и навиките на потрошувачите, со цел да се приспособи понудата.

Директниот маркетинг ја опфаќа секоја комуникација, остварена преку кои било средства за презентирање маркетинг-материјал или рекламирање, која е насочена кон обработката на лични податоци на одредено физичко лице. Притоа, оваа комуникација најчесто опфаќа достава на персонализирани писма по пошта, контактирање по телефон, електронска пошта, СМС, скокачки (поп-ап) прозорци, но и други начини. Како и за секоја обработка на лични податоци, така и за маркетинг-целите, мора да постои релевантна правна основа, а таа може да се добие преку обезбедување директна согласност од страна на субјектот на личните податоци.

При обработката на личните податоци за целите на директниот маркетинг, контролорот мора да постапува според правилата од Законот за заштита на личните податоци, односно:

- Да постои законска основа за обработка (согласност на субјектот на личните податоци).
- Информација до субјектот на личните податоци за обработката на личните податоци за целите на маркетингот (принцип на транспарентност).
- Имплементирање соодветни технички и организациски мерки за заштита на личните податоци, вклучително и писмен договор со задолжителни одредби склучен со обработувачот кој ќе врши директен маркетинг во име на контролорот (на пр., маркетинг-агенции).
- Да не се врши пренос надвор од ЕУ/Европскиот економски простор, освен доколку не се исполнети законските услови (одредби за сообразност) кои дозволуваат да се изврши овој пренос.

- Останати барања од Законот за заштита на личните податоци.

Напомена: Се препорачува при подготовката ма Изјавата за согласност, таа да биде посебна за оваа конкретна цел, односно да не биде дел на генерално давање согласности за различни цели, пр., автоматска обработка (профилирање), фотографирање и сл.

На субјектот на личните податоци треба да му биде овозможено правото на повлекување (eng. opt out) на дадената изјава за согласност за обработка на личните податоци за целите на директниот маркетинг. За начинот на кој може да ја повлече согласноста, субјектот е однапред информиран (преку Политика за приватност, известување за приватност. Политика за колачиња и сл.) при што повлекувањето треба да биде на лесен и едноставен начин, преку користење на расположливите канали на комуникација и без дополнителни трошоци.

Се препорачува Контролорот да предвиди системска евиденција (постојат различни софтверски алатки, модели и решенија) за дадени и повлечени согласности за обработка за целите на директниот маркетинг што ќе ви овозможи ажуриран преглед на состојбата во секое време.

Пример: Органите на државната власт можат да се потпрат на критериумот „при спроведувањето на нивните надлежности", но тоа не значи дека прашањето за директен маркетинг никогаш не се поставува во поглед на јавниот сектор, на пр., како што е достава на електронска пошта на граѓаните за културни настани, користејќи лични податоци од Регистарот на население.

10. ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

10.1. Определување офицер за заштита на личните податоци

Во согласност со член 41, став 1 од ЗЗЛП од Законот за заштита на личните податоци, потребно е да определите офицер за заштита на личните податоци во следниве случаи:

- Доколку сте орган на државна управа.
- Кога вашата основна дејност се состои од активности за обемна обработка што налагаат редовно и систематско следење на физичките лица (на пр., компанија за обезбедување која има систем за видеонадзор во неколку трговски центри).
- Кога вашата основна дејност вклучува обемна обработка на посебни категории лични податоци (на пр., биометриски податоци, генетски по-

датоци, податоци што се однесуваат на здравјето) или лични податоци поврзани со казнени пресуди и кривични дела (на пр., активностите за обработка на личните податоци во болница се сметаат за обемна обработка наспроти обработката што ја врши лекарот, за поединец, која не се смета за обемна обработка на лични податоци).

Во согласност со горенаведеното, обврската за назначување офицер се однесува на сите државни органи, со исклучок на судовите, но само кога постапуваат во рамките на нивните надлежности. Ова подразбира дека, сепак, судовите се обврзани да определат офицер за заштита на личните податоци кој ќе се грижи за усогласеноста со прописите за заштита на личните податоци, во однос на активностите за обработка на лични податоци кои се надвор од нивните судски надлежности.

Притоа, офицерот за заштита на личните податоци има обврска за тајност и доверливост при извршувањето на неговите/нејзините задачи.

Воедно, потребно е на официјалната интернет-страница на институцијата да бидат објавени контакт-детали за офицерот за заштита на личните податоци, а тие треба да бидат доставени и до Агенцијата за заштита на личните податоци.

10.2. Потребни квалификации

Согласно ЗЗЛП при назначување на вработен на позиција офицер за заштита на личните податоци, потребно е да бидат исполнети пропишаните професионални стручни знаења и квалификации, за лицето да биде назначено на оваа функција.

Поради природата на активностите, од офицерот, дополнително, се очекува да поседува и сет лични и интерперсонални вештини. Од личните потребно е да има: интегритет, иницијативност, организираност, дискреција, истрајност, интерес и мотивација за извршување на оваа функција, како и високо ниво на професионална етика, развивање вештини и спроведување конкретни практики со наметнување промени кога тоа е потребно, и способност за пренесување на знаења и јасна позиција, како и афирмација на позицијата кога е потребно.

Што се однесува, пак, на интерперсоналните вештини, од офицерот се очекува да може да одржува добра комуникација со сите вклучени страни, како и да поседува способност за преговарање и решавање конфликти.

Дејствувањето на офицерот за заштита на личните податоци не смее да предизвика судир на интереси, со извршувањето на други задачи, од причина што на таков начин ќе биде доведено во прашање независното извршување на неговите задачи и должности (вклучително и можни политички или други

влијанија врз извршувањето на нивните должности), ниту, пак, смее во исто време да биде вработено како лице кое учествува во определувањето на целите и начините на обработка на личните податоци (без оглед на фактот дали станува збор за високи менаџерски позиции или за пониски работни позиции).

На пример: За ОЗЛП не може да биде определен управителот на контролорот/обработувачот, ниту администраторот на информацискиот систем.

Законот за заштита на личните податоци, предвидува можност органите на државната управа да определат, за неколку органи во состав на надлежниот орган, да биде надлежен еден офицер за заштита на личните податоци, под услов да биде достапен за секоја од институциите. Овој офицер може да биде ангажиран врз основа на договор на дело за обезбедување на таквите услуги.

Работната група 29 (WP29) при Европскиот одбор за заштита на личните податоци во својот документ „Насоки за офицери за заштита на личните податоци"[9], го наведува следново:

- во случај на државен или јавен орган, офицерот за заштита на личните податоци треба да има солидно познавање на (интерните) административни правила и процедури во рамките на организацијата.

10.3. Улога на офицерот за заштита на личните податоци

Офицерот за заштита на личните податоци претставува клучен играч во системот за управување со личните податоци. Мисијата доделена на офицерот за заштита на личните податоци ја потврдува неговата важна улога во следењето на динамичниот процес на повисоко ниво на усогласеност од областа за заштита на личните податоци и неговата поставеност (со гаранција од раководството за неговата независност) во институцијата, од кого се очекува да балансира меѓу интересите на институцијата и правата на субјектите на лични податоци.

Офицерот за заштита на личните податоци има советодавна и ревизорска улога на контролорот, ја следи усогласеноста на работењето на државниот орган со релевантните прописи и врши континуирана едукација на вработените за темите од областа на заштитата на личните податоци.

Од тие причини, потребно е соодветно и навремено да биде вклучен во сите аспекти од областа на заштитата на личните податоци.

Отповикувањето/разрешувањето на носителот на функцијата офицер за заштита на личните податоци е оправдано, единствено, доколку лицето повеќе не ги исполнува условите за извршување на работните задачи и должности.

[9] Guidelines on Data Protection Officers ('DPOs') (wp243rev.01) https://ec.europa.eu/newsroom/article29/items/612048.

11. ЗАДАЧИ И ОДГОВОРНОСТИ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

При описот на работните задачи од областа на заштитата на личните податоци, во правниот документ (одлука, решение и сл.), за ваше назначување на позицијата офицер за заштита на личните податоци, потребно е државниот орган/институција да се води од оние пропишани во Законот за заштита на личните податоци, односно во самиот опис на работното место на офицерот за заштита на личните податоци да се наведе следното:

Пример: Опис на работните задачи на ОЗЛП

Работни задачи на ОЗЛП
❖ Се грижи за имплементацијата на прописите за заштита на личните податоци и внатрешните акти донесени од страна на контролорот. ❖ Развива стратегија за заштита на личните податоци која е соодветна на конкретниот контролор. ❖ Раководи со организациската единица за заштита на личните податоци – доколку е воспоставена. ❖ Го претставува контролорот (интерно и јавно) за прашањата од областа на заштитата на личните податоци.
На оперативно ниво: ❖ Се грижи за информирање на субјектите на личните податоци за нивните права, како и на контролорот за неговите обврски што произлегуваат од прописите за заштита на личните податоци. ❖ Се грижи за подигнувањето на свеста кај контролорот за заштита на личните податоци. ❖ Организира и спроведува обуки за вработените кои се вклучени во операциите на обработката на лични податоци кај контролорот. ❖ Ги следи усогласеноста и почитувањето на прописите за заштита на лични податоци од страна на контролорот, преку идентификација и евалуација на законските барања, нивна процена и развивање упатства за нивно исполнување од страна на контролорот. ❖ Ги подготвува внатрешните акти на контролорот и ја следи нивната усогласеност со прописите за заштита на лични податоци. ❖ Го следи спроведувањето на техничките и организациските мерки за обезбедување сигурност и тајност при обработката на личните податоци кај контролорот. ❖ Го советува и му дава соодветни препораки на контролорот во насока на исполнување на обврските што произлегуваат од прописите за заштита на личните податоци.

- Активно е вклучен во сите проекти што се однесуваат на имплементацијата на нови ИТ-системи или креирање на нови продукти и сервиси, уште во раните фази од проектот, со цел да се дизајнираат системите или продуктите во согласност со основните начела за заштита на личните податоци.
- Активно е вклучен во креирањето и имплементацијата на процесите што опфаќаат обработка на личните податоци.
- Врши контроли во врска со почитувањето на прописите за заштита на личните податоци врз основа на претходно дефинирани правила за нивно спроведување.
- Дава совети во поглед на проценатa на влијанието на планираните операции за обработка врз заштитата на личните податоци и следењето на извршувањето на оваа процена (Data Protection Impact Assessment).
- Остварува редовни состаноци со највисокото ниво на раководење/менаџмент во врска со прашањата од областа на заштитата на личните податоци.
- Соработува и дејствува како контакт-точка за ДЗЛП (дава поддршка на ДЗЛП при спроведувањето на законските обврски и соработува со ДЗЛП во насока на развивањето и промовирањето најдобри практики за конкретни теми).
- Ја координира комуникацијата на контролорот во постапките што се водат пред Дирекцијата за заштита на личните податоци.
- Остварува контакт со субјектите на личните податоци и се грижи за спроведувањето на постапката и навремено одговарање на нивните барања и приговори упатени до контролорот, а во врска со прашањата од областа на заштитата на личните податоци.
- Ја координира надворешната комуникација за прашањата од областа на заштитата на личните податоци, дејствувајќи како единствена точка за контакт и ја координира надворешната поддршка дадена од страна на консултантски, адвокатски и други правни друштва.

Функциите односно задачите на офицерот за заштита на личните податоци можат генерално да бидат групирани во четири главни категории и тоа: прелиминарна, организациска, советодавна и ревизорска функција.

Преку следните чекори за проверка на спроведувањето на Вашите задачи и одговорности, ќе бидете во можност, на едноставен начин, да имате увид за тоа што се очекува од вашата работна позиција офицер за заштита на личните податоци. Воедно, преку конкретни примери од практиката, ќе можете да пристапите и успешно да ги имплементирате вашите обврски и задачи.

11.1. Прелиминарна функција

За почеток, потребно е да се направи попис на сите лични податоци што ги поседувате и да се документира зошто се потребни личните податоци што ги обработувате. Во таа насока, треба да се определи опкружувањето на

контролорот и да се мапираат активностите за обработка на личните податоци во организацијата, во поширок рамки.

Имено, ќе бидете во можност професионално да ги извршувате своите задачи, само доколку сте запознаени со:

(i) внатрешната распределба и распределбата на задачите и одговорностите, во однос на каква било обработка на личните податоци, во рамки на вашата институција;

(ii) надворешните односи и договори на институцијата со други институции/тела (соработка со др. институции, користење услуги од надворешни добавувачи и трети страни, користење на услуги во „облак" и сл.);

(iii) правната рамка(и), со која вашите задачи се регулирани.

При извршување на овие активности, потребно е да го документирате следното:

- Како се добиени личните податоци?
- Зошто се чуваат личните податоци?
- Дали сè уште се потребни личните податоци?
- Дали се безбедни личните податоци?
- Со кого се споделуваат личните податоци?

Следно што треба да направите е да пристапите кон утврдување на целите на обработката и да гарантирате безбедност на обработката, преку примена на соодветни технички и организациски мерки.

Во оваа фаза, може да дојде до поклопување на активностите од оваа задача со активностите кои се однесуваат на спроведувањето на евиденцијата на активностите за обработка на личните податоци во Задача 1 од Организациската функција – но во оваа фаза, потребно е активностите за обработка на личните податоци да бидат единствено идентификувани, во однос на целта на обработката и употребените технологии.

На тој начин, ќе добиете првична идеја за тоа кои задачи и одговорности ги има секоја организациска единица (сектор, служба, одделение или оддел), во врска со активностите за обработка на личните податоци и, воедно, ќе го идентификувате „сопственикот на деловниот процес" на секоја обработка на лични податоци.

Врз основа на добиените резултати, ќе направите патека на движење на личните податоци во рамки на Вашата институција, со цел да обезбедите поголема контрола на нивната обработка во рамки на работните активности на институцијата.

ПРИМЕР:

- Централен регистар (Закон за Централен регистар);[10]
- Регистар за изречени казнени санкции (Закон за извршување санкции);[11]
- Регистар за забрана за вршење дејност и Регистар за казни на правни лица (Закон за прекршоци);[12]
- Регистар на даночни обврзници (Закон за даночна постапка);[13]
- Регистар за педофили (Закон за посебен регистар за лица осудени со правосилна пресуда за кривични дела за сексуална злоупотреба на малолетни лица и педофилија);[14]
- Регистар за приматели на социјална помош (Закон за социјална заштита);[15]
- Регистар на службени матични книги (Закон за матична евиденција);[16]
- Регистар на недвижен имот (Закон за даноците на имот) итн.[17]

Во централна електронска форма, дел од овие податоци на граѓаните се разменуваат и интероперабилно од страна на различни институции преку Централниот регистар на население (Закон за електронско управување и електронски услуги[18], каде што е дефинирана електронската размена на податоците и начинот на кои таа треба да се спроведува, давањето е-услуги, работењето на посредниците, како и Законот за централен регистар на население[19] и Законот за електронски документи, електронска идентификација и доверливи услуги[20]).

Многубројните прашања што ќе произлезат во оваа прелиминарна фаза не мора веднаш да бидат адресирани и решени – но потребно е соодветно да

---

[10] Закон за Централен регистар (Службен весник на Република Македонија број 50/2001, 49/2003, 109/2005, 88/2008, 35/11, 43/14, 199/14, 97/15, 153/15, 27/16, 83/18 и 311/20).

[11] Закон за извршување на санкциите (Службен весник на Република Северна Македонија бр. 99/19, 220/19 и 236/22).

[12] Закон за прекршоци (Службен весник на Република Северна Македонија бр. 96/19)

[13] Закон за даночна постапка (Службен весник на Република Македонија број 13/2006, 88/2008, 159/2008, 105/2009, 133/2009, 145/10, 171/10, 53/11, 39/12, 84/12, 187/13, 15/15, 97/15, 129/15, 154/15, 23/16 и 35/18 и Службен весник на Република Северна Македонија број 275/19, 290/20 и 247/22).

[14] Закон за посебен регистар за лица осудени со правосилна пресуда за кривични дела за сексуална злоупотреба на малолетни лица и педофилија (Службен весник на Република Македонија бр. 11/2012 и 112/2014).

[15] Закон за социјална заштита (Службен весник на Република Северна Македонија број 104/19, 146/19, 275/19, 302/20, 311/20, 163/21, 294/21, 99/22, 236/22 и 65/23).

[16] Закон за матична евиденција (Службен весник на Република Македонија бр. 8/1995; 38/2002; 66/2007; 98/2008; 67/2009; 13/2013 и 43/2014).

[17] Закон за данок на имот (Службен весник на Република Македонија бр. 61/04, 92/07, 102/08, 35/11, 53/11, 84/12, 188/13, 154/15, 192/15, 23/16 и 151/21).

[18] Закон за електронско управување и електронски услуги (Службен весник на РСМ бр. 98 и бр. 244).

[19] Закон за централен регистар на население (Службен весник на РСМ бр. 98/19 и 275/19).

[20] Закон за електронски документи, електронска идентификација и доверливи услуги (Службен весник на РСМ бр. 101/19 и 275/19).

бидат мапирани активностите за обработка на личните податоци на институцијата во поширока смисла, како клучен чекор кон создавањето регистар на овие активности и сите поединечни активности за обработка на личните податоци, спроведени во рамки на следната задача.

Напомена: *Офицерот за заштита на личните податоци во оваа фаза е во улога на координатор на одговорните лица од надлежните сектори и советодавно лице чија улога е да води низ процесот на усогласеност со регулативата од оваа област.*

11.2. Организациска функција:

Задача 1: Подготовка на евиденција (регистар) на активности за обработка на личните податоци

Согласно член 34 од ЗЗЛП, секој контролор, односно обработувач мора „да води" евиденција на активностите за обработка, наведувајќи различни детали за секоја активност, како што е називот на контролорот и овластеното лице, офицерот за заштита на личните податоци, назив на работниот процес, целта/целите на обработката, категориите субјекти на податоците, категориите лични податоци, преносот во трета земја (доколку има), роковите за бришење, општ опис на техничките и организациските мерки како и категориите корисници на кои се откриени или ќе бидат откриени личните податоци.

Оваа должност да води евиденција на активностите за обработка на личните податоци е тесно поврзана со начелото за отчетност, што го олеснува и ефективниот надзор од страна на Агенцијата за заштита на личните податоци.

Според тоа, евиденцијата е предуслов за усогласеност, како и ефикасна мерка на отчетност.

Секој контролор и обработувач треба да биде обврзан да соработува со надзорниот орган и, на негово барање, да ги стави на располагање записите, односно евиденцијата.

Записот што се води претставува алатка која им овозможува на контролорот и на надзорниот орган да имаат увид во активностите за обработката на личните податоци што ги спроведува една институција.

Во Прилогот бр. 1 од овој Водич, може да најдете предлог-обрасци за евиденција (Регистар) за обработката на личните податоци (тие не се задолжителни, но би ви помогнале при создавањето на вашата евиденција на активностите за обработка на личните податоци и соодветни записи).

Напомена: *Доколку постои какво било сомневање во врска со потребата од евиденција, Контролорот треба да побара совет од вас, а вам тоа ви се препора-*

чува, при давање на советот, тоа да биде во насока на водењето на евиденцијата, место да ризикувате дека институцијата нема да постапи во согласност со член 34 од ЗЗЛП.

Забелешки:

1. На прашањето дали евиденцијата на активностите за обработка на личните податоци е потребно да биде јавна достапна (на интернет или на друг начин) или не, можете подетално да видите во Задача 2, „Преглед на активностите за обработка на личните податоци".

2. Создавањето на евиденцијата како таква сè уште не вклучува процена на усогласеноста на евидентираните активности за обработка на личните податоци: тоа е направено во Задача 2 – но се разбира, евиденцијата треба да биде предмет на редовно менување и ажурирање, односно секогаш кога ќе настанат промени во активностите за обработката на личните податоци да бидат запишани во неа.

Задача 2: Преглед на активностите за обработка на личните податоци

Повеќето институции од јавниот сектор нудат широк спектар услуги. Ова значи дека тие вообичаено чуваат и споделуваат голем обем лични податоци што треба да бидат предмет на одговорна обработка. Податоците се клучни за тоа како институциите од јавниот сектор обезбедуваат услуги за граѓаните, ги подобруваат нивните системи и процеси и со тоа носат подобри одлуки. Сепак, постои недостаток на доверба кога станува збор за управувањето со личните податоци од страна на јавниот сектор, посебно во поглед на електронските јавни услуги, поради големиот број на хакирања за кои бевме сведоци во изминатиот период.

Евиденцијата на активностите за обработката на личните податоци вклучува информации за целите на обработката, категориите субјекти на лични податоци, категориите лични податоци и примателите на лични податоци, преносот на личните податоци, рокот за бришење на личните податоци, како и техничките и организациските мерки што се применуваат.

Овој вид евиденција е одличен начин за воспоставување контрола врз обработката и движењето на личните податоци во рамки на вашата организација. Чувањето на овие информации на едно место го олеснува докажувањето на усогласеноста со Законот за заштита на личните податоци.

Откако сте ја подготвиле евиденцијата на активностите за обработката на личните податоци во својата организација (Задача 1), следниот чекор е да спроведете длабински преглед на овие активности за обработка на личните податоци за да се види дали ги исполнуваат условите од ЗЗЛП, во однос на:

- утврдување на целта за обработката и на ограничувањата;

- валидноста на секоја согласност и документарен доказ за неа или применливоста на која било друга правна основа за обработка (валидноста се утврдува врз основа на постоење правна основа за обработка на личните податоци, согласно член 10, став (1) од ЗЗЛП).

Напомена: *Имајте предвид дека доколку се потпирате на согласност обезбедена од физичките лица како правна основа за обработката на личните податоци, тогаш треба да гарантирате дека се исполнети сите услови пропишани со законот.*

Напомена: *Доколку обработката на личните податоци, пак, вклучува посебни категории лични податоци (на пр., биометриски податоци, генетски податоци, податоци кои се однесуваат на здравјето и сл.), треба да се повикате на правната основа за обработката и на еден од исклучоците за обработка на таквите податоци дадени во член 13 од ЗЗЛП*:

- Релевантност и неопходност на обработените лични податоци, во однос на утврдената цел(и)).
- Квалитет на податоците (точност, ажурираност, итн., на податоците, како и нивно минимизирање и псевдонимизација).
- Информации доставени до субјектот на личните податоци (кога податоците се собираат од субјектот на личните податоци или на барање на субјектот на личните податоци, пр., податоците собрани врз основа на негова согласност за користење колачиња, како посетител на интернет-страница).

Напомена: *Во таа насока, од вас се очекува да ги информирате субјектите, во рамките на вашата политика за приватност/известување за приватност/изјава за приватност за*:

- временскиот период во кој личните податоци се чуваат во форма која може да се идентификува;
- техничката, организациската и физичката безбедност на податоците (вклучувајќи физички пристап, ограничување на пристапите (корисничко име, лозинки, политики итн.)), енкрипција, и сл.);
- прекугранични от пренос на податоци (правни, договорни или други вид односи); итн.

Согласно горенаведеното, недвосмислено ќе бидете во можност да процените дали конкретната активност за обработка на личните податоци, во целост, е во согласност со принципите на законитост и правичност.

Создавањето точна и одржувањето ажурна евиденција на активностите за обработка на личните податоци, која претставува мапа на личните податоци во една институција, истовремено е и корисен документ за институцијата кој ќе придонесе за поголема заштита на личните податоци.

Како што наведовме претходно, не постои предвидена форма на евиденција. Но според нејзината природа на „менливост", попрактично би било да се чува во електронска форма користејќи некоја од алатките на MS Office или можеби некој посебен софтвер за ваква намена.

Во поглед на техничките и организациските мерки, а во согласност со член 28 од ЗЗЛП, контролорот е должен да примени такви мерки на обезбедување што одговараат на нивото на безбедност кое е соодветно на ризиците по правата и слободите на физичките лица. Тука би можеле да се предвидат различни мерки за справување со овие ризици како, на пример: псевдонимизација/енкрипција, стандардни одредби за доверливост, технички мерки за да се обезбеди доверливост, интегритет, достапност на системите и можности за враќање на податоци, и сл. Сепак, ова нуди првичен преглед, од аспект на тоа дали преземените мерки се „соодветни" на *state of art*, трошоците за имплементација и природата, обемот, контекстот и целите на обработката, како и веројатноста и сериозноста за појава на ризик по правата и слободите на физичките лица.

ЗЗЛП не бара од контролорите да ја објават јавно евиденцијата на активностите за обработката на личните податоци на една институција. Меѓутоа, ЗЗЛП, исто така, тоа не го забранува.

Генерално, постојат многу причини зошто евиденцијата на активностите треба да биде јавна:

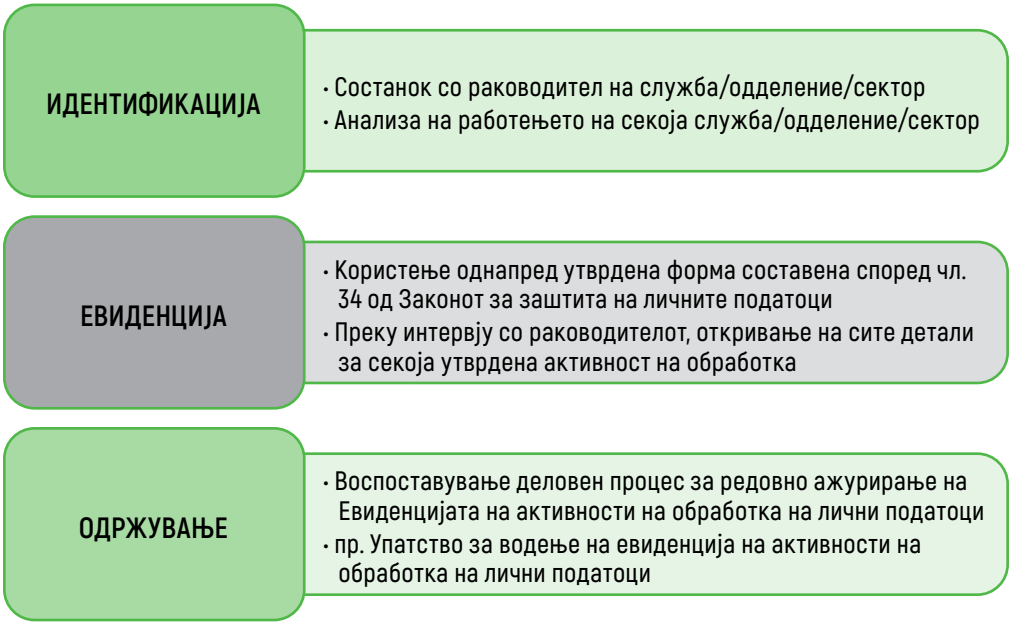
- Придонесува за транспарентноста;
- Помага да се зајакне довербата на јавноста;
- Го олеснува споделувањето знаење;
- Необјавувањето би било чекор назад зад старите правила.

Ова, во најмала рака, е важно за вас како државни институции. Останува можноста, националното законодавство да наметне должност за објавување на евиденцијата.

Во оваа насока, доколку сметате дека активностите за обработка на лични податоци не се усогласени со регулаторните барања, потребно е без одлагање да го известите одговорното лице (сопственик) на деловниот процес за недостатоците и да предложите соодветни мерки за ублажување (доколку е потребно и целосно да се прекине со понатамошна обработка на овие лични податоци).

Доколку, пак, и покрај укажувањата, не се следи вашиот совет, од страна на сопственикот на деловниот процес, ова прашање треба без одлагање да биде адресирано до највисокото раководство (подетално во делот на „Советодавни задачи").

Напомнуваме дека од вас се очекува да водите целосна евиденција за спроведените прегледи, процени и дадени совети.



Слика: Фази од процесот на создавање евиденција на активностите за обработка на личните податоци

Во продолжение пример за евиденцијата на активностите за обработка:

Пример	Систем за видеонадзор
Контролор	Министерство/Општина/Агенција
Категорија субјекти и категорија лични податоци	Видеоснимки од посетителите на институцијата
Цел	Заштита на сопственоста, заштита на животите и здравјето на вработените поради природата на работата што се извршува
Примател	Министерство/Општина/Агенција
Рок за бришење на податоците	30 дена
Технички и организациски мерки	Посебен акт за начинот на вршење видеонадзор
Пренос на лични податоци	/

*Слика 2 – Пример за евиденција на активностите за обработка на личните податоци.

Со завршување на Прелиминарната функција и задача 1 и 2 од Организациската функција, треба да имате одговор на следните прашања:

Чекор 1: Утврдени активности за обработка на личните податоци

- Вид лични податоци кои се обработуваат и за која цел, како и кој и како ги обработува;
- Системи што се користат за обработката на личните податоци.

Чекор 2: Утврдени правни основи за обработка на личните податоци

- Утврден законит начин за собирање и обработка на личните податоци;
- Личните податоци се евидентирани за конкретна цел и се следат насоките за обработка на личните податоци.

Чекор 3: Утврдени деловни процеси што налагаат поголема безбедност (нивно приоретизирање!)

- Услуги, системи, простории и податоци што треба да бидат заштитени, како и нивна меѓусебна поврзаност.

Задача 3: Процена на ризиците во врска со активностите за обработка на личните податоци

Усогласеноста бара да се утврдат релевантните ризици, врз основа на извршениот попис на активностите за обработка на личните податоци и создавањето Евиденција (Регистар) на тие активности (Задача 1), заедно со прегледот на тие активности (Задача 2).

ЗЗЛП не бара стриктно вклучување на офицерот за заштита на личните податоци во спроведувањето на општата процена на ризиците: неговото вклучување го предвидува само во однос на подлабока анализа на ризиците, односно спроведувањето на Проценатa на влијанието на заштитата на личните податоци, кога е идентификуван висок ризик за правата и слободите на физичките лица. Меѓутоа, во практика, се препорачува да се вклучите и вие, генерално, при подготовката на општата процена на ризиците од оваа област.

Ризиците што е потребно да бидат предмет на процена не ги опфаќаат единствено безбедносните ризици, туку и веројатноста и влијанието од нарушувањето на безбедноста при активностите за обработка на личните податоци што можат да се одразат како на правата и слободите на субјектите на личните податоци, така и на други засегнати поединци.

При подготовката на проценатa во врска со ризиците од активностите за обработка на личните податоци, се земаат предвид природата, обемот, контекстот и целите на обработката, карактеристични за вашата институција, односно се користи пристап базиран на ризик (повеќе не се применува ист принцип за сите, односно универзален пристап).

Согласно Правилникот за безбедност на обработката на лични податоци[21] (во понатамошниот текст: Правилник за безбедност), при идентификување и оценување на ризиците (управување со ризици), контролорите ги земаат предвид ризиците што се поврзани со обработката на личните податоци, особено од случајно или незаконско уништување, губење, менување, неовластено откривање или неовластен пристап до податоците што се пренесени, се чуваат или на друг начин се обработуваат. Во таа насока, вие сте одговорни за усогласеноста на нивото на мерките за безбедност на обработката согласно Правилникот за безбедност, при што со ваша помош и советување се очекува да биде обезбедено соодветно ниво на безбедност на овие обработки на лични податоци што се дел од деловните процеси на институцијата.

Проценета мора да го содржи „најмалку" следново:

I. Систематски опис на предвидените активности за обработка и целите на обработката;

II. Процена на неопходноста и пропорционалноста на активностите за обработка на личните податоци во однос на целите;

- Се определуваат мерки предвидени за усогласување и тоа:
  - Мерки што придонесуваат за пропорционалноста и неопходноста од обработката на лични податоци, врз основа на:
    - конкретна, експлицитна и легитимна цел(и);
    - законитост на обработката;
    - соодветни, релевантни и ограничени на потребните податоци;
    - ограничено времетраење на чување.
  - Мерки што придонесуваат за правата на субјектите на личните податоци:
    - Информации доставени до субјектот на лични податоци;
    - Правата на субјектот;
    - Односи со обработувачите;
    - Заштитни мерки околу преносот (и) во трети земји;
    - Претходна консултација со Агенцијата за заштита на лични податоци.

III. Проценка на ризиците за правата и слободите на субјектите на лични податоци:

- се проценува потеклото, природата, особеноста и сериозноста на ризиците или, поконкретно, за секој ризик (неовластен прис-

[21] (Службен весник на РСМ, бр. 122 од 12.5.2020 година).

тап, несакана промена или губење на податоците), во врска со субјектите на личните податоци;

- » се земаат предвид изворите на ризици;
- » се идентификуваат потенцијалните влијанија врз правата и слободите на субјектите на личните податоци, во случај на настани што вклучуваат неовластен пристап, несакана промена или губење податоци;
- » се идентификуваат заканите што можат да доведат до неовластен пристап, несакана промена и губење на податоците;
- » се проценува веројатноста и сериозноста;

IV. Мерките предвидени за справување (митигирање) на ризиците, вклучително и заштитни мерки, безбедносни мерки и механизми за обезбедување заштита на личните податоци, како и докажување на усогласеноста, имајќи ги предвид правата на субјектите на личните податоци и другите засегнати лица.

Во таа насока, Проценатa на ризиците вклучува четири чекори и тоа:

1. Определување на активноста за обработка на личните податоци и нејзината содржина.
2. Разбирање и евалуација на влијанието врз правата и слободите на субјектите на личните податоци.
3. Определување на можните закани и процена на веројатноста за појава на закани.
4. Евалуација на ризик (веројатноста од појава на закана и влијанието доколку се појави).

Оттаму, зборуваме за четири главни области на процена на ризиците, и тоа:

- » Мрежни и технички ресурси (хардверска и софтверска опрема);
- » Процеси/процедури поврзани со активностите на обработка на личните податоци;
- » Различни страни вклучени во активностите на обработка на личните податоци;
- » Деловен сектор и обем на обработка.

(во Прилог број 4 кон овој Водич, можете да најдете предлог-пристап за спроведување на проценатa на ризиците предложен од страна на Европската агенција за вмрежување и информациска сигурност, која се заснова

на меѓународниот ИСО-стандард 27005[22]: Закани од злоупотреба на ранливости на средства што може да предизвикаат штета за организацијата (*Threats abuse vulnarabilities of assets to generate harm for the organisation*, препорачано и од Италијанската агенција за заштита на личните податоци).

Фактори при процена на ризикот

Генерално, кога се проценува одреден ризик, потребно е тој објективно да се оцени, односно да се земат предвид веројатноста и влијанието од појава на овој ризик врз правата и слободите на субјектите на личните податоци.

Проценувањето на ризиците врз правата и слободите на субјектите како резултат на нарушувањето има различен фокус од ризиците што се проценуваат. Проценатa ги вклучува двата типа ризици: ризикот обработката на личните податоци да не се спроведе во согласност со планираното и ризик во случај на нарушување на безбедноста на личните податоци.

Пример:

Проценатa за влијанието на заштитата на личните податоци (во понатамошниот текст: ПВЗЛП) предлага дека употребата на одреден безбедносен софтверски производ за заштита на личните податоци е соодветна мерка за да се обезбеди нивото на безбедност кое е соодветно на ризикот што инаку би го предизвикала обработката на личните податоци, за субјектите на лични податоци. Меѓутоа, доколку ранливоста се појави подоцна, односно за неа би станале дополнително свесни, тоа би ја променила соодветноста на нивото на безбедност на софтверот и, поради тие причини, тоа би требало да биде предмет на повторна процена како дел од тековната ПВЗЛП.

Имено, подоцна се искористува ранливоста на средството и доаѓа до нарушување на безбедноста. Контролорот треба да ги процени специфичните околности на нарушувањето, кои лични податоци се погодени и потенцијалното влијание врз поединците, како и колку е веројатно овој ризик да се материјализира (пр., природата, чувствителноста и обемот на податоците, можноста за идентификација на субјектите на лични податоци, последиците, можноста да бидат вратени изгубените податоци, настанатата штета и сл.).

Како добра практика, при оценувањето, се препорачува да се земат предвид следните критериуми:

1. Видот на нарушувањето кое може да влијае на нивото на ризик

Пример:

Нарушувањето на доверливоста може да е во поглед на откривање медицински податоци на неовластени лица кои може да предизвикаат различни

[22] ISO/IEC 27005 „Information technology - Security techniques - Information security risk management".

последици за поединецот, односно податоците да се изгубат и повеќе да не се достапни.

2. Природата, чувствителноста и обемот на личните податоци

Категоријата на личните податоци чија безбедност е нарушена претставува клучен фактор при проценувањето на ризиците. Колку се почувствителни податоците, толку е поголем ризикот од штетата за засегнатите субјекти на личните податоци, доколку тие на друг начин веќе станале јавно достапни.

На пример, обелоденување на името и адресата на некој субјект веројатно нема да предизвика значителна штета. Меѓутоа, доколку името и адресата на посвоителот е откриена на биолошкиот родител, последиците во поглед на приватноста би можело да имаат значајно влијание и за посвоителот и за детето.

Нарушувањата што вклучуваат здравствени податоци, документи за идентификација или финансиски податоци како што се кредит, детали за платежна картичка и сл., сами по себе не предизвикуваат штета, но доколку се користат во комбинација со други лични податоци, тие можат да бидат искористени за кражба на идентитетот на субјектот на личните податоци.

3. Едноставност при идентификација на поединци

Фактор кој, исто така, е потребно да се процени е и колку страната која има пристап до компромитираните лични податоци би била во можност да идентификува одредени поединци.

Во зависност од околностите, идентификацијата би можела да се направи со директно користење на нарушените лични податоци или, пак, би биле потребни дополнителни активности за да се открие идентитетот на поединецот.

Во таа насока, примената на одредени технички мерки како, на пр., псевдонимизација, ќе овозможи обработка на личните податоци така што активноста на обработката повеќе нема да може да доведе до одреден субјект на лични податоци, без притоа да бидат потребни дополнителни информации за тоа лице. Сето ова, пак, ќе ја намали и веројатноста за појава и на други поединци кои можат да бидат идентификувани, во случај на нарушување на безбедноста. Проценета на секоја активност за обработка е индивидуална, имајќи предвид дека техниките на псевдонимизација, сами по себе, не може да се сметаат дека ги прават податоците целосно неразбирливи, како и дека псевдонимизираните податоци сè уште се сметаат за лични податоци.

4. Сериозност на последиците за субјектите на личните податоци

Доколку нарушувањето се однесува на личните податоци за ранливи категории субјекти, тоа ќе предизвика и поголема штета.

Доколку личните податоци се во рацете на лица чии намери се непознати или евентуално злонамерни, тоа ќе влијае на нивото на потенцијален ризик. На тој начин, се доведува во прашање доверливоста, од причина што личните податоци се откриени на трето лице или друг примач, и тоа како резултат на грешка.

На пример, кога личните податоци се испраќаат случајно на погрешен оддел во организацијата или на најчесто користената надворешна организација – добавувач. Притоа, контролорот може да побара од примачот или да ги врати или безбедно да ги уништи добиените податоци. Во двата случаи, потребно е контролорот да биде во постојан контакт со третата страна за да биде свесен за нивните постапки, историјата и други релевантни детали за примачот. Доколку примачот е доверлив, тоа може да доведе до намалување или целосно избегнување на последиците од нарушувањето, но тоа не значи и дека нема да дојде до нарушување. Но, повторно, ова е предмет на индивидуална процена.

Сепак, контролорот сè уште треба да ги чува информациите во врска со нарушувањето како дел од општата должност за водење на евиденција за нарушувањата.

Треба да се земе предвид и времетраењето на последиците за поединците, особено доколку влијанието е значајно, а ефектите се долгорочни.

Посебни карактеристики на субјектот на личните податоци

Нарушувањата може да влијаат на личните податоци за одредена категорија субјекти, пр., деца или други ранливи субјекти, кои притоа може да бидат изложени на поголем ризик. И други фактори за субјектот можат да влијаат на самото нарушување.

Посебни карактеристики на контролорот на личните податоци

Природата и улогата на контролорот и неговите активности може да влијаат на нивото на ризик за поединци како резултат на конкретно нарушување на безбедноста на личните податоци. На пример, медицинска установа која обработува посебни категории лични податоци претставува поголема закана за субјектите, во случај да настане повреда на нивните лични податоци.

Број засегнати лица

Генерално, колку е поголем бројот на засегнатите лица, толку е поголемо влијанието на нарушувањето. Сепак, самото нарушување може да има сериозно влијание дури и на една личност, во зависност од природата на личните податоци и контекстот во кој податоците се компромитирани. Затоа од особена важност е да се разгледаат веројатноста и сериозноста на влијанието врз засегнатите страни.

Врз основа на спроведената процена и утврдените ризици, од вас се очекува да дадете приоритет и да се фокусирате на прашањата што претставуваат повисок ризик за правата и слободите на субјектите чиишто лични податоци ги обработува вашата институција.

За обработката која претставува висок ризик за правата и слободите на физичките лица, потребно е да го известите одговорното лице или лицата задолжени за управување со ризици (доколку има определено) и да предложите мерки за ублажување или алтернативно дејство. Доколку Вашиот совет не се следи, потребно е да го упатите до највисокото раководство.

За сите овие активности, водете целосна евиденција и чувате записи.

Овие записи „ќе покажат дека обработката е извршена во согласност со регулативата за заштита на личните податоци" – односно дека тие ризици навистина биле оценети и дека преземените мерки се соодветни за нивно управување, а во насока на „должноста да се демонстрира усогласеност" со ЗЗЛП.

Дополнително, од вас се очекува да утврдите кои области се предмет на внатрешна или надворешна ревизија/контрола/проверка, каква обука/едукација/тренинг треба да се организира за вработените и на кои активности за обработка на личните податоци во рамки на деловните процеси вработените треба да посветат посебно внимание.

ПРИМЕРИ:

Личните податоци собрани за една цел (изработка на картичка за пристап) се користат и за друга цел (објава на фотографијата на социјални медиуми), односно цел за која нема соодветна правна основа и/или субјектите на личните податоци не се информирани за планираната секундарна обработка, што би било уште посериозно, во случај да постои обелоденување на податоците на трета страна;

Појаснување: Ова може да резултира така што субјектите на личните податоци да не бидат информирани (или да не се согласат) за секундарната обработка што, пак, би имало негативни последици за нив (на пр., на работното место или кај апликации за добивање социјална или финансиска помош и сл.). Исто така, сосема е веројатно дека личните податоци добиени за една цел се недоволно точни, односно релевантни за употреба во сосема поинаков контекст.

Задржување и/или користење на личните податоци (откако веќе не се потребни за првобитната намена за која биле собрани) во псевдонимизирана или анонимизирана форма (за понатамошна употреба за нова, споредна намена).

Појаснување: Со оглед на зголемениот ризик од повторна идентификација

на наводно целосно анонимизирани податоци, на секое понатамошно задржување и употреба на вакви податоци потребно е да се гледа како да претставува ризик за правата и слободите на субјектите на личните податоци (што може да доведе до „висок ризик" што бара подготовка на процена на влијанието врз заштитата на личните податоци). Во таа насока, треба да ги проверите ризиците од аспект на можноста за повторна идентификација на лицето за која било специфична употреба и да предвидите засилени мерки за нивно ублажување, па сè до забрана за понатамошна нивна обработка.

Користење ирелевантни, неточни или застарени податоци

Појаснување: Можни слични негативни последици како што беа појаснети во претходниот пример

Непосветување на потребното внимание во поглед на „интересите или основните права и слободи на субјектот на лични податоци кои бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете".

Несоодветно информирање на субјектите на личните податоци за сите детали за кои тие мора да бидат информирани при што субјектите нема да имаат информација околу тоа за кои цели се обработуваат нивните лични податоци, колку време ќе се чуваат тие лични податоци, дали ќе се пренесуваат на трети страни и сл.

Појаснување: Ова може да резултира така што субјектите на личните податоци да не можат целосно да ги остварат своите права, односно интересите или основните права и слободите на субјектот на личните податоци кои треба да бидат заштитени.

Пренос на лични податоци во трета земја каде не е обезбедено „соодветно ниво" на заштита на личните податоци, не се применети соодветни заштитни мерки или сет задолжителни корпоративни правила, односно не влегува во некое од наведените отстапувања за специфични ситуации дефинирани во ЗЗЛП. Ова вклучува користење „услуги во облак" (cloud computing) која користи сервер (или сервери) што локациски се сместени во трети земји.

Појаснување: Имајте предвид, дека „услугите во облак" (cloud computing) носат со себе специфични ризици што би требало да бидат внимателно третирани од страна на контролорите. Од причина што инхерентно носат високи ризици, доколку се користи ваков тип услуга, потребно е за нив да се подготви соодветна процена на влијанието врз заштитата на личните податоци.

По завршување на оваа задача, треба да бидете во можност да одговорите на следното:

Чекор 4: Ги имате анализирано потенцијалните ризици, односно:

4.1. Идентификувани се ризиците: (утврдено е дали безбедноста на личните податоци е подложна на ризици како што се природни катастрофи, недоволно дефинирани одговорности во рамките на организацијата, или потенцијални технички проблеми и сл.);

4.2. Проценети се можните последици:

- Сериозноста на последиците во случај на инцидент.
- Утврдени сценарија и дали тие влијаат врз податоците што треба посебно да бидат заштитени (податоци за здравјето или детали од досието на вработено лице и сл.)

4.3. Проценета е веројатноста:

- да се случи некој инцидент;
- искуството на институцијата кое може да ја олесни проценатa на сериозноста на штетата од настанување на ваков настан;
- на потребните информации за да се утврди можната штета.

4.4. Утврден е степенот на ризик:

- Ризици што подразбираат висок степен на влијание и висок степен на веројатност.
- Ризици што би предизвикале помала штета и постои помала веројатност да се појават.

Во согласност со Правилникот за безбедност на обработката на личните податоци, во поглед на примената на техничките и организациските мерки, даваме одредени насоки и упатства по кои може да се водите и да постапувате во своето работење: (Прилог 7 од овој Водич)

Задача 4: Управување со активностите за обработка на личните податоци за кои е веројатно дека ќе резултираат со „висок ризик“ за слободите и правата на субјектите, врз основа на спроведена процена на влијанието врз заштитата на личните податоци.

Општата процена на ризиците, опишана во Задачата 3, се применува и за активностите на обработка на личните податоци што претставуваат „висок ризик за правата и слободите на физичките лица“.

ЗЗЛП јасно наведува дека ова особено е случај кога се применуваат нови технологии. Од тие причини, потребно е контролорот да изврши проценка на влијанието врз заштитата на личните податоци, пред да продолжи со понатамошна обработка на личните податоци.

Агенцијата за заштита на личните податоци има донесено, во форма на подзаконски акти – Правилник за процесот на процена на влијанието на заштити-

тата на личните податоци[23], Листа на видовите активности за обработка за кои се бара процена на влијанието врз заштитата на личните податоци[24], како и Листа на видовите активности за обработка за кои не се бара процена на влијанието врз заштитата на личните податоци[25].

Подготовката на проценатa за влијанието на заштитата на личните податоци (во понатамошниот текст: ПВЗЛП) претставува корисна алатка за управување со ризиците за правата и слободите на субјектите на личните податоци, додека управувањето со ризиците во други области (на пр., информациска сигурност) е фокусирано, пред сè, на ризиците од информациска сигурност со кои се соочува организацијата.

Целите на ПВЗЛП се идентификување и процена на високите ризици за правата и слободите на физичките лица, вклучени во активностите за обработката при користењето нови технологии, земајќи ги предвид природата, обемот, контекстот и целите на обработката, изворите на ризик, како и мерките што може да се преземат за да се ублажат овие ризици, соодветни во поглед на достапната технологија и трошоците за имплементација. Воедно, потребно е да се евидентираат наодите, евалуацијата и преземените мерки (или непреземени, со наведување на причините за таа активност) за да може да се „покаже усогласеност" со барањата на ЗЗЛП, во согласност со принципот на „отчетност" во однос на оценетата обработка.

Член 39, став 3 од ЗЗЛП пропишува дека „високите ризици" за правата и слободите на физичките лица, може да произлезат, особено, од:

- Автоматизирана обработка, вклучително и профилирање, врз чија основа се донесуваат одлуки што произведуваат правно дејство, односно значително влијаат врз физичкото лице;
- Обработка во голем обем на посебна категорија лични податоци или на лични податоци што се однесуваат на казнени осуди и казнени дела од член 14 од ЗЗЛП; или
- Систематско набљудување на јавно достапни простории во големи размери.

Автоматска обработка, вклучително и профилирање:

Автоматизираното одлучување засновано на профилирање може да доведе до нефер одлуки (бидејќи не постои личност која е идентична со друг поединец и ниту еден систем не ги поседува сите податоци за една личност) или недемократски одлуки што можат да вклучат и дискриминаторски исход; употребата на посебна категорија лични податоци, исто така, може

[23] (Службен весник на РСМ, бр. 122 од 12.5.2020 година)
[24] (Службен весник на РСМ, бр. 122 од 12.5.2020 година)
[25] (Службен весник на РСМ, бр. 122 од 12.5.2020 година)

да доведе до дискриминација (без разлика дали е намерно или не); употребата на навидум незначајни лични податоци за продажба може да открие интимни здравствени проблеми или бременост; и систематското следење на луѓето на јавните места може да има застрашувачки ефект врз остварувањето на основните права како што се правата на слобода на изразување, здружување, протест и сл.

Ризиците може да се комбинираат и меѓусебно да го зајакнат своето дејство како, на пример, при употребата на технологијата за препознавање лица за следење на јавни места од страна на полицијата, со цел „идентификување" и предвидување лошо однесување.

Притоа, за овие ризици да се материјализираат, не е потребна повреда на личните податоци: ризиците произлегуваат од инхерентниот ризик (наследен ризик) на самите активности за обработка на личните податоци, дури и доколку обработката се врши во согласност со нивните специфики и без да дојде до нарушување на безбедноста.

Повеќе примери можете да најдете во Прилог бр. 4 од овој Водич.

Користење услуги од надворешни лица

При проценатa на ризиците, доколку обработката на личните податоци за потребите на органите на државната власт вклучува посебна категорија лични податоци во техничко-правна смисла на Законот („посебни категории податоци") или чувствителни во поопшти термини, како што се финансиски податоци или податоци за попис, таа може да се спроведе во соработка со надворешни лица.

Во поглед на спроведувањето детална проверка на надворешните лица (трети страни, обработувачи, надворешни даватели на услуги, добавувачи и сл.), потребно е пред влегување во договорен однос за секое надворешно лице да се направат:

- проверка дали е усогласено со законските одредби за заштита на личните податоци;
- проверка дали е или било под истрага за нарушување на безбедноста на личните податоци;
- идентификација на неговите други клиенти;
- негативни референции или генерално негативни објави што можат да влијаат на неговата репутација;
- проверка дали е сертифициран според ISO27001, PCI DSS или некој друг стандард од областа на информациската сигурност (посебно за обработувачот);

» ревидирање на документацијата за безбедност и заштита на личните податоци;

» спроведување теренски посети и контроли (ова се предвидува во планот за оперативни непосредни и посредни контроли, согласно резултатите од спроведената процена на ризиците и нивна приоретизација);

» идентификување на седиштето;

» кратка анализа од запознавањето со синџирот на набавка и неговите подизведувачи.

Видеонадзор и анализа на ризик:

Шведската државна управа за заштита на лични податоци ја казни општината Скелефтеа со 200.000 SEK (17.000 евра) поради прекршување на GDPR. Оцената на државната агенција е дека гимназијата во Скелефтеа додека вршела пилот-тест на системот за препознавање лица ги прекршила личните податоци на 22 ученици. Иако идејата била системот да се користи за полесно следење на присуството на учениците, GDPR ги класифицира таквите податоци како посебна категорија лични податоци, со посебни ограничувања за нивна употреба.

Со порастот на следењето на луѓето преку видеонадзор се намалува слободата на движењето и однесувањето на луѓето и нивната приватност, особено оној кој се спроведува на работните места.

При проценатa на ризиците водете се од исполнувањето на следните обврски поврзани со видеонадзорот:

» Јасен доказ кој е одговорен за видеонадзорот, преку обезбедување известување кое ги содржи следните задолжителни елементи: дека се врши видеонадзор, името/називот на контролорот кој го врши видеонадзорот, како и начинот на кој може да се добијат информации за тоа каде и колку време се чуваат снимките од системот за видеонадзор.

» Придржување до правилата за тоа кои податоци и во колкав обем можат да се прибираат и да се чуваат (вклучително и целта за поставувањето на видеонадзорот, рокот на чување на снимените материјали и сл.).

» Ограничена правна основа (заштита на животот или здравјето на луѓето, заштита на сопственоста, заштита на животот и здравјето на вработените поради природата на работата или обезбедување контрола над влегувањето и излегувањето од службените или деловните простории само за безбедносни цели).

» Примена на технички и организациски мерки (поставеност на камера за исполнување на целите на видеонадзорот, овластување за гледање снимки, евиденција на авторизиран/неавторизиран пристап, заштита со корисничко име и лозинка и сл.).

» Рок на чување (максимално 30 дена, освен ако со друг закон не е предвиден подолг рок).

» Забрана за снимање одредени простории (надзор во гардероби, соблекувални, санитарни јазли и други слични простории).

» Интерен акт – Правилник за начинот на вршење на видеонадзорот со кој ќе се регулира, на пр., овластувањето за пристап до снимките, автоматизираниот систем на записи (логови), транспарентноста, системот заштитен со лозинка, обуката на вработените, итн.

» Донесена и објавена Изјава/Известување за приватност.

Примери:

Видеонадзор на работно место и јавен простор

Многупати кога одите на состанок, ќе видите дека одредени канцеларии и простории се под видеонадзор чија цел, во основата, треба да биде заштитата на луѓето, имотот и бизнисот. Многу често, компаниите без процена на ризикот, на сопствена иницијатива, инсталираат систем за видеонадзор, со што се врши повреда во доменот на заштитата на личните податоци. Треба да се нагласи дека ваквиот видеонадзор е суштински неупотреблив бидејќи видеоматеријалот од него би бил лесно оспорен во секоја постапка и, во суштина, претставува голем ризик за институцијата што го користи за снимање вработени, посетители и трети лица спротивно на законските одредби, односно ги чува и архивира нивните лични податоци.

На прашањето зошто се снимаат канцеларии или други јавни простори, одговорот кој често се слуша е „така кажале претпоставените".

Работодавецот треба да ја почитува приватноста на сите вработени додека се на работното место, односно начелото на пропорционалност, во однос на целта заради која се поставува видеонадзорот. Новата технологија и постојаниот видеонадзор можат негативно да влијаат на здравјето и физичката состојба на работниците и на работната способност.

Согласно горенаведеното, во поглед на вклученоста на заинтересираните страни во подготовката на проценатa на ризиците, вашиот совет е од клучно значење.

Затоа, контролорот, во соработка со вас, ќе направи процена приспособена на потребите на институцијата, а потпирајќи се на меѓународното иску-

ство за процена на ризик, на пр., во согласност со стандардот ISO 31000 Risk Management.

Главната цел на записот од спроведената процена е да има докази дека е извршена соодветна, длабинска ПВЗЛП, во согласност со ЗЗЛП, преку исполнување на горенаведените критериуми.

Подетално појаснување на факторите што укажуваат на веројатност да резултираат со „висок ризик" и за кои задолжително е потребна подготовка на ПВЗЛП, може да најдете во Прилог бр. 4 кон овој Водич.

Напомена:

Достава на Известување до Агенцијата за заштита на личните податоци:

- » Потребно е електронски да се евидентира во Евиденцијата на збирки на лични податоци со висок ризик, со корисничко име и лозинка на пристап до системот;
- » По исклучок, за оние кои се веќе регистрирани во Централниот регистар на збирки на лични податоци, потребно е да се достави Известување во електронска форма преку интернет-страницата на АЗЛП, заради негово евидентирање.
- » Формата и содржината на образецот за известувањето е пропишана во одредбите на Правилникот за известување за обработка на лични податоци со висок ризик.

По завршување на оваа задача, треба да можете да одговорите на следните прашања:

Чекор 5: Ги имате избрано соодветните технички и организациски мерки

- Техничките и организациските мерки се избрани врз основа на ризиците што треба да имаат приоритет во решавањето поради високиот степен на сериозност и веројатност
- Водејќи се од најновите технолошки достигнувања, мерките што треба да се разгледаат за минимизирање на овие ризици
- Мерките што можат да се спроведат во разумен обем (претставуваат рационален трошок), на пример, набавка на машина за уништување хартиени документи (техничка мерка) и спроведување соодветни работни инструкции за уништување хартиени документи (организациска мерка).

Чекор 6: Го имате оценето преостанатиот ризик

- Утврдените ризици што не можат да бидат целосно избегнати со примена на технички и организациски мерки
- Степенот на сериозност и веројатност на преостанатите ризици

Чекор 7: Ги имате консолидирано мерките

- Направена е соодветна комбинација на мерките
- Мерките се соодветни на посебните околности во вашата организација

Чекор 8: Ги имате спроведено избраните мерки

- Дефинирани (или избор на) мерките што најпрвин ќе бидат применети (во согласност со нивото на мерките – стандардно или високо)
- Утврдена е страната која е одговорна за нивното спроведување
- Спроведените мерки што довеле до посакуваниот резултат како резултат на спроведената процена на ризикот

Задача 5: Управување со нарушувањето на безбедноста на личните податоци

Идејата за известување за нарушување на безбедноста на личните податоци не е новина сама по себе. Обврската за известување веќе беше вклучена во Директивата за е-приватност[26]. Меѓутоа, таа должност беше ограничена на давателите на електронски комуникации, мрежи и услуги. GDPR ја користи истата дефиниција за „нарушување на безбедноста на личните податоци" како што е онаа содржана во Директивата за е-приватност, но без ограничувањето кое се однесува на нарушувањето на безбедноста што доведува до случајно или незаконско уништување, губење, промена, неовластено откривање или пристап до лични податоци пренесени, складирани или поинаку обработени.

Доколку направиме паралела, обврска за известување до Агенцијата за заштита на лични податоци во случај на повреда на личните податоци беше предвидена и со стариот Закон за заштита на личните податоци (кој е надвор од сила).

Со актуелната регулатива за заштита на личните податоци се предвидува:

- Општо известување на релевантниот надзорен орган за секое нарушување на безбедноста на личните податоци што може да резултира со ризик за правата и слободите на поединци; и
- Должност за информирање на субјектите на податоците за таквите нарушувања, во случаите кога тоа е веројатно да резултира со „висок ризик" за правата и слободите на физичките лица.

Притоа, сретнуваме различни видови повреда на личните податоци („нарушување на доверливоста"; „нарушување на интегритетот"; „нарушување на достапноста").

Пример за нарушување на безбедноста на личните податоци претставува ситуација во која уредот на контролорот кој содржи копија од базата на податоци за клиентите е изгубена или украдена.

Дополнителна ситуација на нарушување може да биде онаа каде единствената копија од базата на податоци е енкриптирана од страна на злонамерен софтвер кој ги заклучува податоците на контролорот додека не се плати от-

[26] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

куп, или е енкриптирана од контролорот со помош на клуч што повеќе не е негова сопственост.

Примерите за губење на достапноста вклучуваат и ситуации во кои случајно се избришани податоците од страна на неовластено лице. Доколку контролорот не може да го врати пристапот до податоците, на пример, од резервна копија, тогаш ова се смета за трајно губење на нивната достапност.

Губењето на достапноста, исто така, може да се случи и доколку дошло до значително нарушување на нормалното функционирање на организацијата, на пример, се случи прекин на струја или напад итн., (denial of service) што ги прави недостапни личните податоци.

И привремено губење на достапноста може да претставува повреда на личните податоци.

Во продолжение уште неколку примери:

Во болниците, доколку не се достапни податоците за здравствената состојба на пациентите, дури и привремено, тоа може да претставува ризик за правата и слободите на физичките лица; на пример, операциите може да бидат откажани и животите да бидат изложени на ризик.

Спротивно на тоа, во случај системите на медиумска компанија да бидат недостапни неколку часа (на пр., поради прекин на струја), доколку таа со тоа е спречена да доставува билтени на своите претплатници, ова веројатно нема да претставува ризик за правата и слободите на физичките лица.

Нападот со откупнина може да доведе до привремено губење на достапноста, доколку податоците можат да се вратат од резервна копија. Сепак, доколку се случи неовластен влез (упад) во мрежата, известувањето може да се бара доколку инцидентот е квалификуван како повреда на доверливоста (односно напаѓачот има неовластен пристап до лични податоци), а ова несомнено претставува ризик за правата и слободите на физичките лица.

ЗЗЛП пропишува дека АЗЛП треба да биде известена не подоцна од **72 часа** откако контролорот дознал за нарушувањето на безбедноста на личните податоци. Исклучок од ова е доколку не постои веројатност нарушувањето на безбедноста на личните податоци да создаде ризик за правата и слободите на физичките лица.

Доколку контролорот доцни со доставата на известувањето до АЗЛП, потребно е да достави образложение за причините за доцнењето.

Доколку станува збор за обработувач, тој е должен да го извести контролорот веднаш откако дознал за нарушувањето на безбедноста на личните податоци.

ЗЗЛП, исто така, пропишува дека:

- контролорот ги документира сите нарушувања на личните податоци, вклучително и фактите во врска со нарушувањето на личните податоци, неговите ефекти и преземените мерки за справување со нарушувањето. Оваа документација ќе му овозможи на надзорниот орган да ја потврди усогласеноста со оваа обврска.

Имајте предвид дека последното барање се однесува на сите нарушувања на безбедноста на личните податоци: тоа не е ограничено на нарушувањата за кои Агенцијата за заштита на личните податоци треба да биде известена, односно записот мора да вклучува и за какво нарушување на личните податоци се работи дури и (според мислењето на Контролорот да) „не е веројатно дека ќе резултираат со ризик за правата и слободите на физичките лица".

Напомена: Во Прилогот бр. 5 дадени се примери и дополнително појаснување во врска со нарушувањето на безбедноста на личните податоци.

Што се однесува, пак, на субјектите на личните податоци, ЗЗЛП наведува дека субјектите треба да се известат „без непотребно одложување", што значи што е можно поскоро.

Главната цел на известувањето до субјектите е да се дадат конкретни информации за чекорите што треба да ги преземаат за да се заштитат себеси. Како што е наведено погоре, во зависност од природата на нарушувањето и ризикот што го носи, навремената комуникација ќе им помогне на субјектите да преземат чекори за нивна заштита од какви било негативни последици што можат да настанат од нарушувањето. Во таа насока, со ЗЗЛП предвидени се задолжителни елементи на известувањето, како и исклучоци од обврска за ниво известување.

Пример:

Сигурно сте се нашле во ситуација намерно или ненамерно да дознаете зошто колега од работа е на боледување. Ана Петровска отворила боледување со шифрата на болеста Х и информациите од Секторот за човечки ресурси се пренесуваат така што и останатите вработени се запознаваат со шифрата на болеста прикажана на формуларот за спреченост за работа, односно дека колешката Ана има болки во грбот или тонзилитис. Информациите за болестите се особено чувствителни (посебна категорија) лични податоци и со нив треба да се постапува на посебен начин, па препораката би била тие податоци да се анонимизираат, а „истекувањето" на овие податоци веднаш да се пријави на офицерот за заштита на личните податоци кој треба да ги види причините за загубата на податоците и за тоа да ја извести Агенцијата за заштита на личните податоци (по процена можеби и субјектот за заштита на лични податоци), најдоцна 72 часа по настанување на инцидентот.

Задача 6: Поддршка и промовирање „Техничка и интегрирана заштита на личните податоци“

Како што беше наведено и во претходните фази и задачи, вие, како офицер за заштита на личните податоци, потребно е да бидете консултирани за прашањата од областа на заштитата на личните податоци што произлегуваат во рамките на организацијата, вклучително и за насоките во поглед на подготовката на општите политики и сл.

Согласно член 29 од ЗЗЛП, потребно е контролорот да ги спроведе оние технички и организациски мерки што се неопходни за конкретни активности на обработка на личните податоци, односно се приспособени за секоја посебна цел на обработка. Таа обврска се однесува на обемот на собраните лични податоци, степенот на нивната обработка, периодот на нивно чување и пристапноста до нив.

Општиот концепт на терминот *техничка и интегрирана заштита на лични податоци* може да се подели на „7 основни принципи“ што ја нагласуваат потребата да се биде проактивен при следењето на приватноста, односно барањата од фазата на дизајнирање, па за времетраењето на целиот животен циклус на личните податоци, да бидат „вградени во дизајнот и архитектурата на ИТ-системите и деловните практики... без намалување на функционалноста...“, со приватноста како стандардна поставка, безбедноста (end-to-end security) во текот на целиот процес, вклучително и безбедното уништување на податоците и силната транспарентност која е предмет на независна верификација. Принципот на приватност е изведен како втор од основните принципи, утврдување дека техничката и интегрирана заштита обезбедува дека личните податоци се автоматски заштитени во сите ИТ- системи или деловни практики. Едноставно, субјектот автоматски го ужива основното право на приватност и заштитата на личните податоци.

Јавната администрација е повикана да се води во примената на овие принципи на одговорен начин, подготвена да го покаже нивното спроведување, доколку е потребно, на надлежниот надзорен орган.

Техничката и интегрирана приватност со право може да се поврзе со проценката на влијанието на заштитата на податоците (од Задача 4); во насока на констатацијата дека вашата улога е централна во процесот за заштитата на личните податоци и е од клучно значење во пристапот на приватноста по дизајн. Поради тие причини, потребно е да бидете вклучени уште од самиот почеток, односно кога институцијата го планира системот за обработка на лични податоци, така што ќе можете да ги поддржувате сите релевантни чинители и тоа: раководители, сопственици на деловни процеси и одделите за ИТ и технологија. Сетот вештини што се очекува да ги поседуваат овие чинители треба да одговара на барањата, односно да вклучува целосно

едуцирање и обучување за соодветните методологии и технологии (доколку има потреба, преку дополнителна обука на работното место) и целосно вклучување при дизајнирањето, развојот, тестирањето и приспособувањето на сите производи „чувствителни на приватност", услуги и активности на институцијата (вклучително и јавните набавки).

Посебно треба да внимавате да ја советувате својата институција во постапките за јавни набавки да поттикнува учество на апликанти кои можат да „покажат" дека нивниот производ или услуга е целосно усогласен со ЗЗЛП, односно е вградена „техничка и интегрирана заштита на податоци". Во таа насока, треба да им се даде конкурентска предност на овие апликанти пред оние за чии производи или услуги не може да се покаже дека ги исполнуваат барањата.

Задача 7: Односи со трети страни (заеднички контролори, контролор–контролор, контролор–обработувач како и клаузули за пренос на лични податоци)

Со цел да се усогласи со ЗЗЛП, а особено со цел да се „покаже" таквата усогласеност, контролорите треба да ги регулираат односите со третите страни, а особено:

- да се потпишат договори помеѓу јавните органи или тела, особено доколку станува збор за „заеднички контролори" на одредени активности за обработка на личните податоци;
- да се подготват релевантни договори со други контролори и обработувачи (како што се стандардните договорни клаузули пропишани од страна на Агенцијата за заштита на личните податоци[27]); и
- да се изготват стандардни или поединечно одобрени договори за пренос на личните податоци[28].

Главната цел е дека сите овие одговорности што се однесуваат на „докажувањето на усогласеноста" се обврска на контролорот. Но, во практика, од Вас се очекува непосредно да бидете тесно вклучени во овие активности.

Задача 8: Постапување по барањата на субјектите на личните податоци

Субјектите на личните податоци може да контактираат со офицерот за заштита на личните податоци во врска со сите прашања поврзани со обработката на нивните лични податоци и за остварување на нивните права според ова Регулатива.

---

[27] Одлука за утврдување на стандардни договорни клаузули помеѓу контролорите и обработувачите (Службен весник на РСМ, бр. 280 од 15.12.2021 година).

[28] Стандардни договорни клаузули за пренос на лични податоци во трети земји (Службен весник на РСМ, бр. 280 од 15.12.2021 година).

Субјектите на личните податоци кои сакаат да остварат кое било од нивните права – права на пристап, исправка, бришење („право да се биде заборавен"), ограничување на обработката, преносливост на податоците, право на приговор и во врска со автоматското одлучување и профилирање – или кои било други општи прашања или поплаки што се однесуваат на заштитата на личните податоци, вообичаено прво се обраќаат до офицерот. Вработените во институцијата треба да бидат информирани дека во случај да добијат некое такво барање, задолжително за тоа да го информираат офицерот за тој да биде вклучен во постапката за остварување на правата на субјектите на лични податоци.

Затоа е потребно да има објавено податоци за контакт на офицерот од страна на институцијата која го назначила и дека контролорот мора да обезбеди „дека офицерот за заштита на податоци е вклучен, соодветно и навремено, во сите прашања што се однесуваат на заштитата на личните податоци." Од тие причини, доколку субјектот на податоците треба се обрати на друго лице во организацијата, пр., генералниот советник или извршниот директор, тие треба да го пренесат барањето до офицерот.

Дополнително, вашиот независен статус треба да обезбеди дека барањето, прашањето или поплаката се решава од ваша страна – или од страна на надлежни вработени, под ваш надзор – на соодветен начин, без пристрасност во корист на институцијата или против субјектот на личните податоци. Во секој случај, потребно е самите да го составите или да го проверите одговорот до субјектот на личните податоци кој е подготвен од страна на друг вработен. Ова особено треба да вклучи дека доколку субјектот на личните податоци не е задоволен од одговорот, тој или таа може да се обрати до офицерот.

Ова е затоа што субјектите на личните податоци имаат право да достават приговор до Агенцијата за заштита на личните податоци. Поточно, Агенцијата е овластена да:

- „постапува со поплаки поднесени од субјект на податоци... и истражува, до степен соодветно на предметот на поплаката и да го извести подносителот на жалбата за напредокот и исходот од истрагата..."

Притоа, би било логично, исто така, да бидете подготвени да одговорите на барањата и поплаките и од репрезентативни организации (пр., граѓански организации), наместо само од субјектите на личните податоци.

Од аспект на досегашната практика, треба да се очекува дека Агенцијата за заштита на личните податоци (како EDPS во однос на институционалните офицери на ЕУ) ќе ги охрабри субјектите на личните податоци секогаш да се обратат најпрвин до контролорот, односно до офицерот, за да видат

дали предметот може да биде истражен и разрешен, без вклучување на Агенцијата, под услов офицерот да се консултира со Агенцијата, доколку е потребно. Повеќе за соработката со АЗЛП во точка 11 – Соработка со Агенцијата за заштита на личните податоци.

Ова ја зајакнува вашата посебна позиција, која претставува мост меѓу контролорот и регулаторот (АЗЛП).

Задача 9: Следење на функциите за усогласеност односно повторување на активностите од организациските функции, на тековна основа

Терминот „следење" јасно покажува дека ова претставува тековна активност.

Вие сте одговорни за следењето на усогласеноста со прописите од областа на заштитата на личните податоци.

Вие како офицер сте, исто така, одговорни за подигнување на свеста во рамките на институцијата, особено меѓу вработените кои се директно вклучени во активностите за обработка на личните податоци.

Како што вели EDPS:

„Обезбедувањето усогласеност особено започнува со подигнувањето на свеста. ...Офицерот игра важна улога во развивањето знаења за прашањата за заштита на податоците внатре во институцијата/телото."

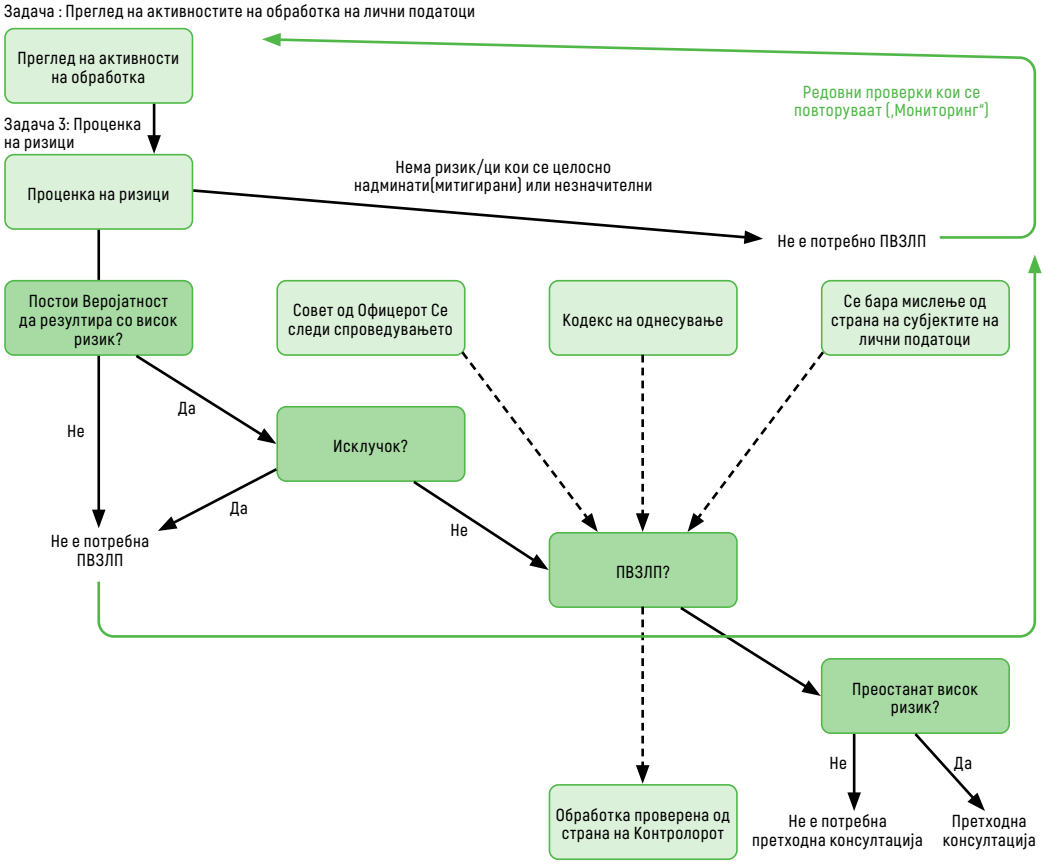
Подигнувањето на свеста „стимулира ефикасен превентивен пристап наместо репресивен надзор за заштита на податоци".

Имено, потребно е следењето на усогласеноста да биде потврдена од страна на надворешна ревизија или внатрешна ревизија, односно лично од ваша страна во улога на офицер, или во соработка со други клучни функции како што е ОСИС (Одговорно лице за сигурност на информативниот систем).

Усогласеноста со заштитата на личните податоци е одговорност на контролорот на личните податоци, а не на офицерот. Но, од вас се очекува, на редовна основа, особено да:

- собирате информации за да се идентификуваат активностите за обработка на личните податоци,
- да ја анализирате и проверувате нивната усогласеност, и
- да информирате, советувате и издавате препораки до контролорот или обработувачот.

Како што беше нагласено и во задача 4, во однос на ПВЗЛП, потребно е да се управува со ризиците за правата и слободите на физички лица, односно ризиците треба соодветно да бидат идентификувани, анализирани, проценети, евалуирани, третирани (на пр., ублажени) и следени.



Вашите записи треба да ја одразуваат реалноста на активностите за обработка во вашата институција.

Ова подразбира дека личните податоци се редовно ажурирани, особено кога вашата институција планира промени во активностите за обработка, за што треба да проверите дали записот е потребно да биде ажуриран. Се препорачува формално да ја вклучите оваа проверка во вашиот процес на управување со промени. Независно од планираните промени, се препорачува да се спроведуваат редовни прегледи, со цел да се утврдат и оние кои можеби останале незабележани, а потребно е да бидат ажурирани.

11.3. Советодавна функција

Советодавната задача, генерално, се одвива на неколку нивоа:

- Пренесување на Вашата стручност до раководството за да може да се обезбеди усогласеност при спроведувањето на активностите за обработка на личните податоци;

- Ширење на културата и правилата за заштита на личните податоци до сите вработени/ангажирани лица кои обработуваат лични податоци во рамките на организацијата. На тој начин, ќе бидете во можност да ги идентификувате клучните прашања каде се бара ваша интервенција или систематски пристап, на пример, за секоја/секое:

✓ Предлог-одлука за креирање или надградба на постојната обработка (особено за да се обезбеди усогласеност со начелата за техничка и интегрирана заштита на личните податоци;

✓ Разгледување на потребата од процена на влијанието врз заштитата на личните податоци и нејзина реализација (со документирање на вашето мислење во Извештајот за спроведената ПВЗЛП);

✓ Следење на евиденцијата на активностите за обработка на личните податоци;

✓ Давање мислење и ажурирање на внатрешните правила или политики за заштита на личните податоци;

✓ Предлог-мерки што треба да се преземат за нарушување на безбедноста како и за известувањето на надзорниот орган и субјектот на личните податоци;

✓ Информирање на субјектите на лични податоци за нивните права.

✓ Притоа дејствувајте во насока на подигнување на свеста и поддржување на вработените од секој сектор/оддел/организациона единица во постапката на обработка на личните податоци:

✓ преку градење култура на заштита на личните податоци (на пр., одржување на интерни едукации/тренинзи/обуки за основните начела за заштита на личните податоци и сл.);

✓ преку спроведување активности за комуникација и подигање на свеста за теми релевантни за организацијата (употреба на постери и практични водичи достапни на интернет, потсетување на безбедносните правила, лажни кампањи за „фишинг“, други форми на социјален инженеринг, итн.);

✓ преку ваше претставување како внатрешна точка за контакт за секое прашање во однос на заштитата на личните податоци, и преку посредници (пр., вработени со добра репутација и препознатливост, во улога на амбасадори за подигнување на свеста за заштитата на личните податоци), доколку е потребно.

✓ Вашата мисија е токму информирање, советување и надзор. Вие директно не сте одговорни за усогласеноста на организацијата, водењето евиденција, спроведувањето процена на влијанието на

заштитата на личните податоци или известувањата за повреда на личните податоци. Сепак, вашата позиција е да бидете клучен играч чии вештини ќе му бидат корисни на раководното лице на организацијата за да му помогнете во процесот на усогласување со обврските што произлегуваат од прописите за заштита на личните податоци.

11.4. Ревизорска функција

Офицерот за заштита на личните податоци треба да биде овластен, сам или со помош на други, да врши ревизија/контрола на контролорот со прописите за заштита на личните податоци. За таа цел, контролорот треба да му ги обезбеди/даде сите потребни информации и документи на офицерот.

Самата постапка и начинот на спроведувањето на ревизиите/контролите треба да биде документирана во интерен акт на контролорот.

Во зависност од приоритетите, целта на контролите/ревизиите се состои од:

- Проверка на точноста на информациите содржани во евиденцијата на активностите за обработка имплементирани од институцијата (попис на активностите за обработка, целта за обработката, субјектите на податоците, природата на обработените податоци, примачите и можните преноси надвор од ЕУ/Европски економски простор, рокот на чување, безбедносните мерки и сл.);
- Проверки на усогласеноста на најчувствителните активности за обработка, земајќи ги предвид спроведените процени на влијанието (особено во однос на спроведувањето на мерките наменети за намалување на веројатноста и сериозноста на ризиците);
- Имплементација на алатки и периодични контроли (анализа на привилегиите, контрола на авторизиран/неавторизиран пристап (логови), проверка на усогласеноста со роковите за чување податоци итн.);
- Следење на ефективноста на техничките и организациските мерки за заштита на личните податоци што организацијата се обврзала да ги спроведе.
- Правилникот за безбедност[29], за некои од ревизиите/контролите утврдува точна динамика за нивно спроведување. За останатите за кои нема утврдено точна динамика, вие како офицер, односно контролор треба да утврдите динамика за спроведување, која ќе биде

[29] (Службен весник на РСМ, бр. 122 од 12.5.2020 година).

базирана на проценатa на ризикот. Ревизиите/контролите пропишани во Правилникот се следните:

- Контрола на евиденцијата за секој пристап (logs) – **најмалку еднаш месечно**.
- Периодична контрола над работата на администраторот на информацискиот систем.
- Годишна контрола (ревидирање) на документот „Список (преглед) со рокови на чување на личните податоци"
- Контрола на привилегиите за пристап – **најмалку квартално**.
- Контрола на документацијата за технички и организациски мерки – **најмалку еднаш годишно**.
- Годишна внатрешна контрола.

Конечно, со оглед на бројот и обемот на вашите задачи, се препорачува да подготвувате годишен план на теваши активности, земајќи го предвид очекуваното време за спроведување и да ги земете предвид новите случувања, но и да се посвети време за непредвидени настани; и редовно да се ревидира и ажурира овој план.

12. СОРАБОТКА СО АГЕНЦИЈАТА

Офицерот има задача да одговори на барањата на Агенцијата за заштита на личните податоци и тоа во рамките на областа која е во нејзина надлежност, да соработува, на сопствена иницијатива или на иницијатива на Агенцијата.

Од Вас се очекува да соработувате со Агенцијата за заштита на личните податоци, како „олеснувач" во комуникацијата (одговарајќи на барањата за време на супервизија на самото место, постапување по прием на поплака, консултации во рамките на спроведувањето на проценатa на влијанието, известување за повредата на правото на заштита на личните податоци итн.).

Исто така, постои можност да се консултирате со Агенцијата за сите прашања што се однесуваат на заштитата на личните податоци или самата функција – офицер за заштита на личните податоци.

Супервизиите што ги спроведува Агенцијата, на самото место, можат да бидат со и без претходна најава. Притоа, без разлика на тоа дали супервизијата е најавена или не, офицерот треба да биде присутен кога таа се спроведува во просториите на контролорот.

Однос меѓу офицер за заштита на личните податоци и Агенцијата за заштита на личните податоци

Во идеална ситуација, улогата на офицерот за заштита на личните податоци е да обезбеди усогласеност во рамките на институцијата, односно да советува или дејствува превентивно во рана фаза, со цел избегнување евентуална интервенција од страна на надзорниот орган. Во исто време, Агенцијата за заштита на личните податоци може да понуди значајна поддршка на офицерот во извршувањето на неговата функција.

Затоа се поддржува идејата за развој на синергија меѓу офицерот и Агенцијата, која би придонесла за постигнувањето општа цел за ефикасна заштита на личните податоци во институциите.

Обезбедување усогласеност

Обезбедувањето усогласеност започнува со подигнувањето на свеста. Вие играте важна улога во развивањето на знаењето за прашањата за заштита на личните податоци во рамките на институцијата. Во таа насока, надзорниот орган го поздравува превентивното дејствување наместо репресивниот надзор.

Исто така, од Вас се очекува да давате совети во рамките на вашата институција, практични препораки за подобрување на заштитата на личните податоци или толкување во врска со примената на Регулативата. Оваа советодавна функција е поздравена од Агенцијата за заштита на личните податоци која

ги советува сите домашни институции/тела за прашањата што се однесуваат на обработката на личните податоци. Воедно, на одредени поопшти теми, обезбедуваат и насоки за институциите/телата.

Претходни проверки

Мислењата издадени од Агенцијата за заштита на личните податоци во рамките на претходните консултации, и издадените претходни овластувања, се, исто така, повод за Агенцијата во насока на следење и обезбедување усогласеност со ЗЗЛП.

Имено, добрата практика од EDPS[30] покажува дека пред конечното усвојување на мислењето на Агенцијата за претходната проверка, може да достави привремен нацрт до офицерот со информации за планираните препораки, што отвора простор за дискусија за ефикасноста и последиците од планираните препораки, со цел тие да бидат ефикасни и практични.

Спроведување

Во делот на имплементацијата на одредени мерки за заштита на личните податоци се појавува синергија меѓу офицерот и Агенцијата, во однос на донесувањето санкции и постапување по однос на поплаките и прашањата.

Како што веќе беше споменато, офицерот има ограничени овластувања за извршување. Агенцијата ќе придонесе за обезбедување усогласеност со ЗЗЛП, преку преземање ефективни мерки во поглед на претходните консултации или овластувања, односно поплаките и други прашања.

Мерките можат да бидат ефективни доколку се добро насочени и остварливи. На вас се гледа како на стратешки партнер во поглед на одредувањето на добро насочена примена на мерката.

Постапувањето по жалби и прашања од ваша страна на локално ниво е охрабрено, особено во однос на првата фаза од истрагата и решавањето, пред да се повика Агенцијата.

Исто така, може да се консултирате со Агенцијата секогаш кога се сомневате во постапката или содржината на жалбите. Ова, сепак, не ги спречува субјектите на личните податоци да ѝ се обратат директно на Агенцијата.

Ограничените овластувања на офицерот, од друга страна, подразбираат дека во некои случаи жалбата или барањето мора да се ескалира до Агенцијата. Затоа Агенцијата обезбедува значајна поддршка во областа на извршувањето. За возврат, може да се потпре на вас, во поглед на обезбедување информации и следење на усвоените мерки.

Мерење на ефективноста

[30] EUROPEAN DATA PROTECTION SUPERVISOR

Што се однесува на мерењето на ефективноста на спроведувањето на барањата за заштита на личните податоци, вие сте корисен партнер за да се оцени напредокот во ова област. На пример, кога станува збор за мерење на перформансите на внатрешен надзор, Агенцијата охрабрува да развивате свои критериуми за спроведување квалитетен надзор (професионални стандарди, конкретни планови за институција, годишна програма за работа и сл.). Овие критериуми, за возврат, ќе ѝ овозможат на Агенцијата, каде што е поканета да го стори тоа, да ја оцени работата на офицерот, но ќе ѝ овозможи и да ја измери состојбата на имплементација на ЗЗЛП во рамките на институцијата.

Исто така, веројатно е дека како офицер во јавниот сектор ќе бидете повикани од Агенцијата да придонесете во консултациите што ги одржува и да обезбеди свој активен придонес кога се подготвува формално мислење за предложени или нацрт-закони во областа на заштитата на личните податоци што се однесува на делот кој го работи офицерот.

Ова често е од клучно значење, особено во однос на сложените системи за обработка каде е потребно длабинско познавање на ИТ-архитектурата и внатрешните процеси за на правилен преглед.

Национален портал за е-услуги (uslugi.gov.mk)

Националниот портал за е-услуги (во понатамошниот текст: Порталот) претставува електронска платформа, достапна на https://uslugi.gov.mk, преку која на граѓаните на РСМ им се овозможува да добијат информации за јавните услуги и да користат е-услуги од надлежни органи и други институции што даваат е-услуги преку Порталот.

Порталот е воспоставен и управуван од Министерството за информатичко општество и администрација (во понатамошниот текст: МИОА) кое е одговорно за достапноста и техничкото функционирање на Порталот, како и системите со кои е поврзан. Преку Порталот, Давателот на електронските услуги ги користи барањата за давање административна услуга по електронски пат утврдени во согласност со Закон, додека Давателот на електронски услуги ги известува корисниците за извршените услуги.

Правната основа за функционирање на Порталот ја дава Законот за електронско управување и електронски услуги, каде што е дефинирана електронската размена на податоците и начинот на кои таа треба да се спроведува, давањето е-услуги, работењето на посредниците и друго.

Други важни закони за работењето на Порталот се Законот за централен регистер на население и Законот за електронски документи, електронска идентификација и доверливи услуги што обезбедуваат извршување електронски

услуги со користење на едноставни средства за работа на корисникот, вклучително и лицата со попреченост.

За содржината на информациите за одредена услуга, како и за давањето на самите е-услуги, одговорен е исклучиво надлежниот орган или друг субјект – давател на услугата.

Што се однесува, пак, на личните податоци, како офицер имате обврска да се грижите за начинот на собирање, обработка и давање на личните податоци, во согласност со законот.

Во таа насока, треба да се даваат совети за имплементирањето и да се следи исполнувањето на минималните технички барања, политики и стандарди за обезбедување пристап до електронските услуги на давателот на електронски услуги, донесени од страна на МИОА.

Во поглед на електронската форма на документите, од надлежните органи, тие се издаваат врз основа на пропишани стандарди од страна на министерот за информатичко општество и администрација.

Обработката на барањето во електронска форма се врши преку Порталот, каде давателот на електронски услуги ги користи податоците за корисникот содржани во регистарот на население и прописите за заштита на личните податоци. По исклучок, доколку во регистарот на населението не се содржани потребните податоци, тие се обезбедуваат од изворот на податоците од каде што веќе се собрани.

Сите добиени и доставени документи во електронска форма се чуваат во информацискиот систем на давателите на електронски услуги, во согласност со законот.

Офицерот за заштита на личните податоци треба да биде вклучен во процесот на дефинирање на меѓусебниот однос кој го имаат институциите, особено кога се работи за електронската размена на податоци и документи.

Од органите на државната власт се очекува да применат мерки за безбедност на информацискиот систем кој го користат за комуникација по електронски пат, со примена на посебни стандарди и правила[31] пропишани од МИОА.

Се препорачува, офицерот да биде дел од тимот одговорен за поврзувањето на платформата за интероперабилност од страна на институцијата и да биде редовно информиран за нејзините евентуални промени.

[31] Платформа за интероперабилност.

Вештачката интелигенција и обврските на ОЗЛП

Вештачката интелигенција (ВИ) покренува важни и итни прашања. ВИ е веќе со нас – менувајќи ги информациите што ги добиваме, изборите што ги правиме и начините на кои функционира нашето општество. Во годините што доаѓаат ќе игра уште поголема улога во тоа како државните органи и јавните институции функционираат и како граѓаните комуницираат и учествуваат во демократскиот процес.

Ова воведува нови предизвици за ОЗЛП, од кого ќе се очекува да го анализира и разбере начинот на којшто работат системите за ВИ и потенцијалните импликации на овие технологии, при што тој нема да има избор освен да остане во чекор со трендот.

Во продолжение се одговори на некои од прашањата што можат да произлезат од горенаведеното и што ќе ви помогнат вам како офицери во случај вашата институција да имплементира систем базиран на ВИ.

1. Дали ЗЗЛП ги регулира вештачката интелигенција и машинското учење?

Да, ЗЗЛП ги регулира ВИ и машинското учење. ЗЗЛП ги регулира сите форми на технологија кои обработуваат лични податоци. Како регулатива базирана на ризик, ЗЗЛП се залага за начела што се применуваат без разлика на контекстот во кој се обработуваат личните податоци.

2. Дали автоматската обработка секогаш вклучува ВИ или машинско учење?

Не, има многу случаи каде автоматската обработка не вклучува ВИ или машинско учење. Активностите за обработка на личните податоци често се „автоматизирани" без вклучување на ВИ или машинско учење. На пример, систем за управување со документи (eng. Document Management System) вклучува автоматска обработка на лични податоци, без неопходно вклучување на ВИ или машинско учење.

3. Дали ВИ и машинското учење секогаш вклучуваат обработка на личните податоци?

Не, системите за ВИ и машинското учење некогаш не вклучуваат обработка на личните податоци. Тие можат да се користат за различни цели што може да немаат поврзаност со личните податоци, како што се, предвидување на временска прогноза, каде влезните податоци се содржат од атмосферски мерења од сензори или податоци за оптимизирање на употребата на пестициди и нутритиенти. Притоа, има повеќе инстанции каде системите за ВИ и машинско учење не обработуваат лични податоци.

4. Дали некои од членовите на ЗЗЛП специфично се применуваат на ВИ и машинско учење?

ЗЗЛП се применува на целата обработка на лични податоци; притоа, секогаш кога систем за ВИ или машинско учење се користи за обработка на личните податоци се применува ЗЗЛП.

5. Јас сум ОЗЛП. Дали треба да бидам загрижен/а за растењето на ВИ и машинско учење?

Како офицер за заштита на личните податоци треба да бидете загрижени за растот на ВИ и машинското учење, бидејќи овие технологии можат да водат до автоматско донесување одлуки што потенцијално може да имаат сериозни импликации врз правата и слободите на субјектите на личните податоци. На пример, ВИ може да биде употребена за автоматска одлука во врска со претходен скрининг на кандидати за вработување. Разбирањето на начинот на кој функционираат алгоритмите ви помага да идентификувате потенцијални ризици (поврзани со заштитата на личните податоци) и да имплементирате соодветни заштитни мерки, каде што е неопходно.

Без разлика на големината на институцијата, вие, како ОЗЛП, ќе бидете афектирани од интеграцијата на ВИ и машинско учење во ИТ-системите на вашата институција. На пример, следните апликации користат ВИ или планираат да го користат во иднина:

- Microsoft Office планираат да имаат ВИ и машинско учење почнувајќи оваа година (2023);
- Многу софтвери за човечки ресурси, пресметка на плати, продажба и сл., веќе користат ВИ и машинско учење, а оние што немаат веќе имаат во план да имплементираат;
- Четботови што користат лични податоци на физички лица за да дадат персонализирани одговори.

Како ОЗЛП, вие и вашиот тим треба да направите процена на влијанието врз заштитата на личните податоци (ПВЗЛП) за сите нови активности за обработка. Со нејзиното спроведување, од особена важност е да се разберат импликациите и ограничувањата на системите за ВИ, особено доколку постојат какви било предрасуди. Потенцијалот системот за ВИ да генерира неточни резултати, исто така, се зема предвид.

Како ОЗЛП, кој работи за организација кој имплементира систем за ВИ, вие треба да имате улога во процедурата за управување со ризик на системите за ВИ. Бидејќи едно од барањата на ЗЗЛП е да се имплементира техничка и интегрирана заштита на лични податоци, една од задачите на ОЗЛП е да ги идентификува, намали или ублажи познатите и предвидливи ризици преку соодветен дизајн и развој на кој било систем за ВИ кој обработува лични податоци.

6. Кои се клучните разговори што треба да ги водам интерно во орга-

низацијата за да се спремиме за брзиот развој на ВИ и машинското учење?

Офицерот за заштита на личните податоци треба да работи заедно со другите засегнати страни во институцијата, како што се ИТ-професионалците, правните експерти како и одговорните на секторите/службите за да формираат мрежа за комуникација преку ВИ. Оваа мрежа за комуникација ќе обезбеди дека употребата на технологијата на ВИ и системите за ВИ во институцијата се транспарентни, отчетни и фер, но, најважно од сè, дека употребата на ВИ е усогласена со ЗЗЛП.

Во продолжение се неколку чекори што ОЗЛП и членовите во мрежата за комуникација можат да ги преземат за да се спремат за зголемената употреба на системите за ВИ во организацијата:

- ✓ Разбирање на технологијата за ВИ: Вие како ОЗЛП треба да имате добро познавање на технологијата за ВИ која се користи од стана на вашата организација. Ова познавање е потпомогнато од страна на засегнатите страни што се дел од вашата мрежа за комуникација, а се со цел да се разберат технологиите за ВИ специфични за одделите каде се користат, вклучително и начинот на кој функционираат, кои податоци ги собираат и обработуваат и какви видови одлуки можат да носат самите системи за ВИ.
- ✓ Специфицирање и соодветно документирање на целите за обработка поврзани со системите за ВИ: ова е многу важно и за фазата на дизајн и за фазата на развој на новиот систем за ВИ, а се со цел да се имплементираат начелата од ЗЗЛП како што се минимален обем на податоци и техничка и интегрирана заштита на личните податоци, особено за системите за ВИ што обработуваат посебна категорија лични податоци како што се податоците за здравствената состојба.
- ✓ Вршење процена на влијанието врз заштитата на личните податоци (ПВЗЛП): вршењето на ПВЗЛП е процес кој помага да се идентификуваат и минимизираат ризиците врз личните податоци. ПВЗЛП мора да се изврши без разлика дали обработката на личните податоци ќе резултира со висок ризик врз правата и слободите на субјектите на личните податоци. ОЗЛП треба да работи во соработка со засегнатите страни (членовите во мрежата за комуникација) за да ги идентификува потенцијалните влијанија врз приватноста на физичките лица и нивните права. Клучен дел од ПВЗЛП за системите за ВИ е да се проверат какви било пристрасности во алгоритамот кои можат да доведат до дискриминација.
- ✓ Преглед на договорите за обработка на лични податоци: Вие како ОЗЛП треба да ги прегледате сите договори за обработка на личните

податоци со провајдерите на ВИ за да обезбедите дека тие вклучуваат соодветни заштитни мерки за обработката на личните податоци од страна на системите за ВИ.

- ✓ Имплементирање соодветни безбедносни мерки: Вие како ОЗЛП треба да обезбедите дека се имплементирани соодветни безбедносни мерки за да се заштитат личните податоци од неовластен пристап, губење или уништување при користење на системите за ВИ.
- ✓ Мониторинг и ревизија на системите за ВИ: Вие како ОЗЛП треба да ги управувате и ревидирате системите за ВИ на редовна основа за да обезбедите дека тие функционираат како што е предвидено и дека ризиците врз личните податоци се ефективно управувани.

Ефектот на вештачката интелигенција врз човековите права

Неприкосновеното и вродено достоинство на секој човек ја сочинува основата за универзалниот, неделив, неотуѓив, меѓусебно зависен и меѓусебно поврзан систем на човекови права и основни слободи. Затоа, почитувањето, заштитата и унапредувањето на човековото достоинство и правата како што е утврдено со меѓународното право, вклучително и меѓународното право за човекови права, е од суштинско значење во текот на животниот циклус на системите за вештачка интелигенција. Човековото достоинство се однесува на признавањето на внатрешната и еднаква вредност на секое човечко суштество, без разлика на расата, бојата, потеклото, полот, возраста, јазикот, религијата, политичкото мислење, националното потекло, етничкото потекло, социјалното потекло, економската или социјалната состојба, раѓањето или инвалидитетот и која било друга основа.

Ниту едно човечко суштество или човечка заедница не треба да биде повредено или подредено (без разлика дали физички, економски, социјално, политички, културно или ментално) во текот на која било фаза од животниот циклус на системите за ВИ. Во текот на животниот циклус на системите за ВИ, квалитетот на живеењето на луѓето треба да се подобрува, додека дефиницијата за „квалитет на живеење" треба да се остави отворена за поединци или групи, сè додека не постои повреда или злоупотреба на човековите права и фундаменталните слободи или достоинството на луѓето во смисла на оваа дефиниција.[32]

Лицата можат да комуницираат со системи за вештачка интелигенција во текот на нивниот животен циклус и да добиваат помош од нив, како што се грижата за ранливи луѓе или луѓето во ранливи ситуации, вклучително, но

[32] https://unesdoc.unesco.org/ark:/48223/pf0000381137

не ограничувајќи се на деца, постари лица, лица со попреченост или болни. Во рамките на таквите интеракции, лицата никогаш не треба да се објективизираат, ниту, пак, треба да се поткопа нивното достоинство на друг начин или да се нарушат или злоупотребуваат човековите права и основни слободи.

Човековите права и основни слободи мора да се почитуваат, штитат и промовираат во текот на животниот циклус на системите за вештачка интелигенција. Државните институции, приватниот сектор, граѓанското општество, меѓународните организации, академската заедница мора да ги почитуваат рамките за човекови права во процесите околу животниот циклус на системите за ВИ. Новите технологии треба да обезбедат нови средства за застапување, одбрана и остварување на човековите права, а не за нивно кршење.

Приватноста, како право суштинско за заштита на човековото достоинство и човечката автономија, мора да се почитува, заштити и промовира во текот на животниот циклус на системите за ВИ. Важно е податоците за системите за ВИ да се собираат, користат, споделуваат, архивираат и бришат на начини кои се во согласност со меѓународното право, притоа почитувајќи ги релевантните национални, регионални и меѓународни правни рамки.

Треба да се воспостават соодветни рамки за заштита на податоците и механизми за управување со пристап од повеќе засегнати страни на национално или меѓународно ниво, заштитени со судски системи и обезбедени во текот на животниот циклус на системите за ВИ.

ВИ вклучува можности, но и ризици за човековите права што треба да бидат заштитени, а не загрозени од самите системи на ВИ. Овие препораки за ВИ и човековите права обезбедуваат насоки за начинот на кои негативното влијание на системите на ВИ на човековите права можат да бидат превенирани или ублажени, фокусирајќи се на 10 клучни области на дејствување.

1. *Процена на влијанието на човековите права*

Потребно е да се воспостави правна рамка која ја дефинира процедурата за државните институции да можат да вршат процена на влијанието на човековите права (во понатамошниот текст: ПВЧП) на системите за ВИ стекнати, развиени и/или користени од страна на тие институции. ПВЧП треба да биде имплементирано и/или користено слично како другите форми на процена на влијанието што се вршат од страна на државните институции, како што е проценатa на влијанието на заштитата на личните податоци. Надзорното тело може да пропише кои типови системи за ВИ се предмет на ПВЧП, но тие пропишани системи за ВИ мора да ги опфатат сите системи за ВИ кои имаат потенцијал да влијаат врз човековите права во кој било стадиум од животниот циклус на системот за ВИ.

Како дел од правната рамка на ПВЧП, од државните институции треба да се бара да извршат самооценување на постојните и предложените системи за

ВИ. Ова самооценување треба да го процени потенцијалното влијание на системот за ВИ врз човековите права земајќи ги предвид природата, контекстот, опсегот и целта на системот. Доколку државната институција сè уште нема набавено или развиено систем за ВИ, оваа процена мора да биде извршена пред купувањето и/или развојот на тој систем.

ПВЧП мора, исто така, да вклучува надворешна ревизија на системите за ВИ, било од независно тело или надворешен ревизор со релевантна експертиза, за да може да помогне во откривањето, мерењето и/или мапирањето на влијанието врз човековите права и ризиците кои би настанале.

Самооценувањето и надворешната ревизија не треба да се ограничат само на евалуација на моделите или алгоритмите зад системите на ВИ, туку треба да вклучуваат и евалуација на тоа како одлучувачите можат да ги собираат или влијаат на влезните параметри како и да ги интерпретираат излезните параметри на таквиот систем. Потребно е, исто така, да се вклучи и процена на тоа дали системот за ВИ останува под значителна човечка контрола низ животниот циклус.

Во околности кога самооценувањето или надворешната ревизија открива дека системот за ВИ претставува реален ризик од кршење на човековите права, ПВЧП мора да ги утврди заштитните мерки и механизмите што се предвидени за спречување или ублажување на тој ризик. Во околности кога таков ризик бил идентификуван во врска со систем за ВИ кој е веќе ставен во употреба од страна на државните институции, неговата употреба треба веднаш да биде суспендирана додека не се имплементираат горенаведените заштитни мерки и механизми. Онаму каде што не е можно значајно да се ублажат идентификуваните ризици, системот за ВИ не треба да биде ставен во употреба или да се користи од која било државна институција. Онаму каде што самооценувањето или надворешната ревизија открива повреда на човековите права, државната институција мора веднаш да дејствува за да ја отстрани повредата и да донесе мерки за спречување или ублажување на ризикот доколку повторно се случи таква повреда.

ПВЧП, вклучувајќи ги наодите од истражувањето или заклучоците од надворешната ревизија, мора да биде достапен на јавноста во лесно достапен и машински читлив формат.

Државните институции не треба да набавуваат системи за ВИ од трети страни во околности кога третата страна не е подготвена да се откаже од ограничувањата за достава на информации (на пр., доверливост или трговски тајни) и кога таквите ограничувања го попречуваат процесот на: спроведување на ПВЧП (вклучително и спроведувањето на надворешна ревизија) и објавување на ПВЧП.

Државните институции треба редовно да спроведуваат ПВЧП, и тоа не само

каде што државните институции набавуваат и/или развиваат системи на ВИ. ПВЧП треба, во најмала рака, да се преземе при секоја нова фаза од животниот циклус на системот за ВИ и на слични значајни промени.

2. *Јавни консултации*

Употребата на системи за ВИ од страна на државните институции треба да биде управувана од стандардите за отворена набавка, применети во транспарентен процес, во кој сите релевантни засегнати страни се поканети да дадат свој придонес.

3. *Обврски за олеснување на имплементацијата на стандардите за заштита на човековите права во приватниот сектор*

Потребно е државата да имплементира мерки во согласност со Европската конвенција за човекови права[33], за актерите на ВИ (пр., креаторите на ВИ, провајдерите и др.) да може да ги имплементираат тие принципи (начела) низ нивното работење.

4. *Информации и транспарентност*

Треба да биде препознаена употребата на систем за ВИ во кој било процес на донесување одлуки кој има значително влијание врз човековите права. Не само што е потребно употребата на системите за ВИ да биде јавно објавена (користејќи јасни и достапни термини), поединците, исто така, мора да бидат способни да разберат како се донесуваат одлуките и како тие одлуки се верификувани.

Ако системот за ВИ се користи за интеракција со поединци во контекст на јавните услуги, особено правдата и здравствената заштита, потребно е корисникот да биде известен и комуницира без одложување на можноста за барање помош или заштита од страна на стручно лице.

Мора да биде овозможена ревизија врз системот за ВИ, а во врска со барањата за транспарентност. Ова може да биде или во форма на јавно објавување информации за системот за кој станува збор, неговите процеси, директни и индиректни ефекти врз човековите права и преземени мерки за идентификување и ублажување на негативните влијанија врз човековите права или во форма на независна, сеопфатна и ефективна ревизија. Во сите случаи, достапните информации треба да овозможат значајна процена на системот за ВИ. Ниту еден систем за ВИ не треба да биде сложен до степен до кој не овозможува човечки преглед и проверка. Системите што не можат да бидат предмет на соодветни стандарди за транспарентност и одговорност не треба да се користат.

5. *Независен надзор*

[33] European Convention on Human Rights.

Надзорните тела треба да бидат независни од државните институции и приватните компании што развиваат, стават во употреба или на друг начин ги користат системите за ВИ и тие мора да бидат опремени со соодветни и адекватни интердисциплинарни експертизи, надлежности и ресурси за извршување на нивната надзорна функција.

Независните надзорни тела треба проактивно да ја истражуваат и следат усогласеноста на системите за ВИ со човековите права, да добиваат и постапување по жалби од засегнатите лица, да вршат периодични прегледи на способностите и технолошкиот развој на системите за ВИ. Тие треба да ја имаат моќта да интервенираат во ситуации кога тие идентификуваат (ризик од) прекршување на човековите права.

6. *Еднаквост и недискриминација*

Во сите околности, ризиците од дискриминација мора да се спречат и ублажат со посебно внимание за групите што имаат зголемен ризик врз нивните права, а тие се под влијание на ВИ.

Ова ги вклучува жените, децата, постарите лица, економски загрозените лица, лицата со попреченост и „расни", етнички или религиозни групи.

7. *Заштита на личните податоци и приватноста*

Развојот, обуката, тестирањето и употребата на системите за ВИ што се потпираат на обработката на личните податоци мора целосно да го обезбедат правото на почитување на приватниот и семејниот живот според член 8 од Европската конвенција за човекови права, вклучително и „правото на информирано самоопределување" во однос на нивните податоци.

Обработката на податоците во контекст на системите за ВИ ќе биде пропорционална во врска со легитимната цел што се остварува преку таквата обработка. Во сите фази треба да постои правична рамнотежа помеѓу интересите што се остваруваат преку развојот и ставањето во употреба на системите за ВИ и правата и слободите на физичките лица.

Обработка на личните податоци во која било фаза на животниот циклус на системот за ВИ мора да се заснова на принципите наведени подолу од Конвенцијата 108+[34], а особено:

i. мора да постои легитимна основа за обработка во согласност со Законот за заштита на личните податоци во соодветните фази на животниот циклус на системот за ВИ;

ii. личните податоци мора да се обработуваат законски, правично и на транспарентен начин;

[34] Convention 108+ for the protection of individuals with regard to the processing of personal data.

iii. личните податоци мора да се собираат за експлицитни, специфицирани и легитимни цели и да не се обработуваат на начин кој е некомпатибилен со тие цели;

iv. личните податоци мора да бидат соодветни, релевантни и да не бидат прекумерни во однос на целите за кои се обработени;

v. личните податоци мора да бидат точни и, каде што е потребно, да се ажурирани;

vi. личните податоци треба да се чуваат во форма која дозволува идентификација на субјектите на личните податоци не подолго отколку што е потребно за целите за кои се обработуваат тие податоци.

8. *Слобода на изразување, слобода на собирање и здружување и ̄право на работ̄ење*

Во контекст на нивната одговорност да ги почитуваат, штитат и исполнуваат сите човекови права и основните слободи, треба да се земе предвид целиот спектар меѓународни стандарди за човекови права што можат да бидат вклучени со употребата на ВИ.

- Слобода на изразување: Треба да се размисли за преземање соодветни мерки за регулирање на технолошките монополи за спречување на негативните ефекти од концентрацијата на експертизата и моќта на ВИ врз слободниот проток на информации.
- Слобода на собирање и здружување: Треба да се стави посебен акцент на влијанието што може да го има употребата на системите за ВИ врз слободата на собирање и здружување, особено во контексти каде што овие слободи тешко се остваруваат офлајн.
- Право на работа: Внимателно треба да биде следен потенцијалот на ВИ да ја забрза автоматизацијата и со тоа негативно да влијание на можноста за работа. Треба да се прават редовни процени за да се следат бројот и видовите создадени и изгубени работни места поради развојот на вештачката интелигенција.

9. Средства за постигнување на правда

Системите за ВИ мора секогаш да останат под човечка контрола, дури и во околности каде што машинското учење или слични техники овозможуваат системот за ВИ да донесе одлука независно од специфичната човечка интервенција. Мора да се воспостават јасни линии на одговорност за кршење на човековите права што може да се појават во различни фази од животниот циклус на системот за ВИ. Одговорноста и отчетноста за кршењето на човековите права што се случуваат во развојот, ставањето во употреба или употребата на системите за ВИ секогаш мора да бидат во рацете на физичкото

лице, дури и во случаи кога мерката со која се кршат човековите права не била директно применета од одговорно лице.

10. *Познавање на ВИ*

Знаењето и познавањето на ВИ треба да се промовира во државните институции, независни надзорни тела, судството, како и во јавноста.

Оние кои се вклучени директно или индиректно во развојот или примената на системите за ВИ треба да го имаат потребното знаење и познавање за тоа како функционира системот за ВИ и да бидат информирани за неговото влијание врз човековите права. Со цел таквите актери да бидат информирани за влијанието на нивните системи врз човековите права, тие, исто така, мора да бидат свесни за спектарот на стандардите што се донесуваат на човековите права.

Државата треба да инвестира во подобрувањето на нивото на писменост кај јавноста, а во врска со ВИ, преку силни напори за подигање на свеста, обука и едукација, вклучително и (особено) во училиштата. Ова не треба да се ограничи само на едуцирањето во врска со начинот на којшто функционира ВИ, но и за нејзиното потенцијално влијание – позитивно и/или негативно врз човековите права. Треба да се направат посебни напори за да се допре до маргинализираните групи и оние кои се обесправени во однос на ИТ-писменоста.[35]

Во Прилог 7 е дадена предлог листа за проверка за горенаведените области на дејствување.

[35] https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

ДЕЛ 4 – ПРИЛОЗИ

ПРИЛОГ 1 – ПРЕДЛОГ-ЕВИДЕНЦИЈА НА АКТИВНОСТИТЕ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ (КОНТРОЛОР И ОБРАБОТУВАЧ)

ПРИМЕРОК ФОРМАТ ОД ЕВИДЕНЦИЈАТА ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ НА КОНТРОЛОРОТ

Напомена: *Имајте предвид дека потребно е да се подготви посебен запис за секоја посебна активност за обработка на личните податоци.*

Дел 1 – Информации за контролорот

ДЕТАЛИ ЗА КОНТАКТ НА КОНТРОЛОРОТ: Име, адреса, е-пошта Телефон
ДЕТАЛИ ЗА КОНТАКТ ЗА ЗАЕДНИЧКИ КОНТРОЛОР[36]:* Име, адреса, е-пошта Телефон
ДЕТАЛИ ЗА КОНТАКТ ЗА ПРЕТСТАВНИК:* Име, адреса, е-пошта Телефон
(*) Доколку е применливо ДЕТАЛИ ЗА КОНТАКТ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ: Име, адреса, е-пошта, телефон

Дел 2 - Основни податоци за активностите за обработка на личните податоци

Име на активност	
Одговорна единица („сопственик на деловен процес“)	
Цел на обработка	

[36] Имајте предвид дека сè потешко е целосно да се разликуваат обработувачите од контролорите. Често, обработувачите (кои дејствуваат во согласност со добиените насоки од контролорот, кој ги определи средствата и целите) сега преземаат многу повеќе одговорности и можат да станат „заеднички контролори“. Ова е особено случај во однос на давателите на облак услуги – од кои нудат „Вештачка интелигенција и машинско учење (AI/ML) преку Machine-Learning-as-a-Service (MLaaS)“.
Во согласност со дискусиите во прелиминарната задача, аранжманите помеѓу субјектите вклучени во вакви сложени аранжмани треба да бидат јасно и правилно евидентирани. Формуларите што ги запишуваат активностите за обработка, потребно е да бидат приспособени на конкретните аранжмани.

Категории субјекти на лични податоци	
Категории лични податоци	
Категории корисници на кои се откриени или ќе бидат откриени личните податоци	
Дали податоците се пренесени во трета земја или на меѓународна организација?	
Во случај на пренос на лични податоци: кои соодветни заштитни мерки се обезбедени?	
Рок за бришење	
Општ опис на имплементираните технички и организациски (безбедносни) мерки	
Законска основа*	

*Законската основа не е задолжителна, но најдобрата практика покажува дека е добро да се наведе во евиденцијата.

ПРИМЕРОК ФОРМАТ ОД ЕВИДЕНЦИЈАТА ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ НА ОБРАБОТУВАЧОТ

Имајте предвид дека мора да постои посебен запис за секоја активност за обработка на лични податоци, за секој посебен контролор.

Информации за обработувачот и кој било подобработувач(и)

ДЕТАЛИ ЗА КОНТАКТ НА ОБРАБОТУВАЧОТ: Име, адреса, е-пошта, телефон
ДЕТАЛИ ЗА КОНТАКТ ЗА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛП: Име, адреса, е-пошта, телефон
ДЕТАЛИ ЗА КОНТАКТ ЗА ПОДОБРАБОТУВАЧОТ:* Име, адреса, е-пошта, телефон
(*) Доколку е применливо ПОДАТОЦИ ЗА КОНТАКТ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛП: Име, адреса, е-пошта, телефон

(*) доколку е применливо

ДЕТАЛИ ЗА КОНТАКТ НА КОНТРОЛОРОТ: Име, адреса, е-пошта, телефон
ДЕТАЛИ ЗА КОНТАКТ ЗА ЗАЕДНИЧКИТЕ КОНТРОЛОРИ: Име, адреса, е-пошта, телефон

ДЕТАЛИ ЗА КОНТАКТ НА ПРЕТСТАВНИКОТ:* Име, адреса, е-пошта, телефон
(*) Доколку е применливо ПОДАТОЦИ ЗА КОНТАКТ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛП: Име, адреса, е-пошта, телефон

Забелешка: Односот меѓу контролорот и обработувачот и меѓу обработувачот и секој подобработувач, мора да се засноваат на писмен договор за исполнување на барањата за обработка на личните податоци.

Обработувачите треба да чуваат копии од соодветните договори со пополнетиот образец.

Образец за обработувачот – Основни податоци за активностите за обработка на личните податоци

Категорија (вид) обработка што се спроведува за контролорот во однос на обработката, вклучително и:	
– категории субјекти на лични податоци	
– категории лични податоци	
Дали податоците се пренесени во трета земја или на меѓународни организација?	

Во случај на пренос на личните податоци: кои соодветни заштитни мерки се обезбедени?	
Општ опис на техничките и организациските мерки	
Дали обработката вклучува употреба на (а) подобработувач(и)? Доколку да, наведете целосни детали и копија од релевантните договор(и).	

ПРИЛОГ 2 – ПРЕДЛОГ-ДЕТАЛИ ЗА МАПИРАЊЕ НА АКТИВНОСТИТЕ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ

II.1. Податоци и извори на податоци

1. Кои лични податоци или категории лични податоци се собираат и користат за оваа активност за обработка?	Означете со √ доколку е применливо	Кога, како и од кого се добиени личните податоци? На пр.: (субјект на лични податоци) » при вработување на лицето » при вклучување во истражување....
Име и презиме		
Датум на раѓање		
Адреса		
Телефонски број (приватен/службен)		
E-mail (приватен/службен)		
Додадете дополнителни податоци, доколку е применливо:*		

2. Дали податоците што ги собирате и чувате во врска со активноста <u>вклучуваат или индиректно откриваат</u> некоја од следните посебни категории лични податоци („чувствителни податоци“)?	Означете со √ доколку податоците се стриктно собрани и искористени за активноста; Означете со √ и додајте („индиректно“) ако податокот е индиректно откриен (објасни доколку е неопходно)	Кога, како и од кого се добиени податоците? На пр.: (субјект на лични податоци) » при вработување на лицето » при вклучување во истражување....
Расно или етничко потекло		
Политички мислења или припадности		
Религиозно или филозофско верување		
Членство во синдикат		
Генетски податоци		
Биометриски податоци		
Податоци за личното здравје		
Информации за кривични пресуди или прекршоци		
3. Останати податоци што се однесуваат на специфична обработка	Означете со √ доколку е применливо	Кога, како и од кого се добиени личните податоци? На пр.: (субјект на лични податоци) » при вработување на лицето » при вклучување во истражување....

ЕМБГ		
Податоци за долгови/кредити		
Податоци за малолетници		
4. Доколку е познато или утврдено: Колку долго се чуваат личните податоци? Што се случува потоа?*		
* Наведете период или настан, на пр., „7 години“ или „До 5 години по престанокот на вработувањето“. Објаснете и што се случува со податоците, на пр., бришење/уништување или доколку тие се чуваат во анонимизиран облик. Забелешка: Доколку постојат различни периоди за чување за различни податоци, ве молиме наведете.		

II.2. Обелоденување податоци

5. На кои трети лица се обелоденуваат горенаведените податоци? И за кои цели? Забелешка: Ова, исто така, важи и за податоците што стануваат достапни, особено директно, електронски Повторни обелоденувања што вклучуваат преноси кон трета земја	Трето лице примач, место и земја на основање	Цел(и) на обелоденување(и)
СИТЕ ПОДАТОЦИ НАВЕДЕНИ ВО II.1.		
ИЛИ: Следниве податоци: (Копирај ги податоците од 1 и 2 погоре)		

Доколку е потребно, додајте дополнителни редови		

II.3. Правна основа за обработка

6. Правна основа за обработка на податоците	Означете ја релевантната правна основа и дадете појаснување во следната колона, доколку е применливо	Појаснување
Субјектот на личните податоци дал согласност за обработката		
Обработката е неопходна за договорниот однос меѓу вашата организација и субјектот на личните податоци (или со цел да се преземат понатамошни чекори на барање на субјектот на личните податоци пред да се склучи договорот – на пр., вработување)		
Обработката е неопходна за усогласеност со законската обврска* на пример, Закон за работни односи – ве молиме наведете го предметниот закон		
Обработката е неопходна за да се заштитат суштинските интереси на субјектот на личните податоци или на друга личност		

Обработката е неопходна за извршување задача од јавен интерес * * Наведете го изворот на задачата (обично закон од кој произлегува)		
6.1. СОГЛАСНОСТ (детали)		
Доколку податоците се обработени врз основа на согласност на субјектите на личните податоци, како и кога е добиена оваа согласност? Напомена: Доколку согласноста е дадена во хартиена или електронска форма, наведете копија од соодветниот текст		
Колку долго се чува овој доказ?		
Дали е пропишан начин на кој може субјектот да ја повлече согласноста?		

II.4. Информирање на субјектите на личните податоци

[Напомена: Оваа информација не е задолжителна, но корисна е при оценувањето и ревидирањето на внатрешните (интерни) политики за заштита на податоците]

7. Информирање на субјектите на личните податоци	Наведете Да/Не (или „не е применливо“) Забелешка: Доколку е релевантно, можете да наведете „Очигледно е во контекстот“ и/или „Субјектот на податоците веќе ги поседува овие информации“	Објаснете кога и како ова е направено Ве молиме дајте копии од какви било информации, известувања или врски
Дали субјектите на личните податоци се информирани за обработката? И доколку одговорот е потврден, кога и како?		
Дали вашата организација е контролорот на обработката на личните податоци за конкретната активност?		
Доколку е применливо, дали информацијата содржи детали за вашиот претставник во ЕУ?		
Дали информацијата содржи детали за контакт на офицерот за заштита на личните податоци		
Дали информацијата содржи главна цел на обработката		
Дали информацијата содржи понатамошна цел за која вашата организација сака (или можеби е заинтересирана) да ги обработува податоците		

Дали информацијата содржи дали податоците се добиени директно од субјектите на личните податоци, кој е изворот и дали тие вклучуваат јавно достапни информации (како, на пример, јавни регистри)?		
Дали информацијата ги содржи примателите или категориите приматели на личните податоци?		
Дали информацијата содржи дали податоците се (ќе бидат) пренесуваат/ни во земја надвор од ЕУ/Европски економски простор (на пр., до услуги во „облак" каде серверот се наоѓа во САД)? Забелешка: Ова, исто така, важи и за податоците што се достапни (особено директно, онлајн) на субјектите кои не се дел од ЕУ-/ЕЕА-земји.		
Дали информацијата содржи дали податоците се пренесени, кои заштитни мерки се предвидени, и каде субјектите на личните податоци можат да добијат копии од нив? Забелешка: Заштитните мерки можат да бидат предвидени во договорите за пренос на личните податоци или преку приватни шифри или печати за приватност.		
Дали информацијата содржи колку време се чуваат податоците?		

Дали информацијата ги содржи правата на субјектите на личните податоци да бараат пристап, исправка или бришење на нивните лични податоци; да побараат нивните податоци не бидат предмет на понатамошна обработка, да приговараат на обработката итн.		
Дали информацијата содржи право субјектите да поднесат жалба до Агенцијата за заштита на личните податоци?		
Дали информацијата содржи податок дали, за сите или дел од податоците што се обработуваат врз основа на добиена согласност, се информирани субјектите на личните податоци?		
Дали информацијата содржи дали субјектите можат да ја повлечат нивна согласност во кое било време (и како да го направат тоа без тоа да влијае на законитоста на претходната обработка)?		
8. Доколку субјектите на личните податоци е потребно да бидат предмет на автоматско одлучување или профилирање, дали тие се информирани за следново;		Наведете кус преглед на применетата логика при автоматското одлучување или профилирање.
Дека ќе се примени таквото одлучување или профилирање?		
Генерално, која е „логиката" за профилирањето?		

Какво значење има автоматското одлучување или профилирање и кои се последиците од ваквиот начин на одлучување или профилирање?		

II.5. Прекуграничен пренос на податоци (пренос на податоци во трети земји)

9. Дали личните податоци се пренесени во трета земја [не е ЕУ/ЕЕА] (или сектор во трета земја) или на меѓународна организација која е потребно да обезбеди „соодветно" ниво на заштита?	Наведете Да/Не и земја/и за кои станува збор. Ако преносот е само на дел, но не сите податоци, наведете за секоја категорија податоци	Објаснете ја целта на преносот, на пр.,: како дел од активностите на вашата организација (на пр., при користење софтвер базиран на облак), или како дел од обелоденувањето на податоците на трето лице (ве молиме наведете ја таа страна/и)
СИТЕ ПОДАТОЦИ НАВЕДЕНИ ВО II.1.		
-		
-		
Доколку е потребно, додајте дополнителни редови		

10. Дали некои од податоците се пренесени во трети земји (не се ЕУ/Европски економски простор) или меѓународна организација која нема обврска да обезбеди „соодветно" ниво на заштита?	Наведете Да/Не и земјата/ите во прашање. Доколку преносот е на само дел, но не на сите податоци, наведете за секоја категорија податоци.	Објаснете ја целта на преносот, на пр.,: како дел од активностите на вашата организација (на пр., при користење софтвер базиран на облак), или како дел од обврската за обелоденување на податоците на трето лице (наведете ја/ги третата страна/и)	Каква заштита или исклучок користите за да го поткрепите овој пренос? *Забелешка: Обезбедете копија од кој било релевантен документ

Забелешка: Доколку податоците се пренесуваат за различни цели на различни примачи во различни земји, ве молиме одговорете на прашањата посебно за секој пренос.			
СИТЕ НАВЕДЕНИ ПОДАТОЦИ ВО II.1.			
ИЛИ: Следните податоци: (Копирај ги податоците од 1 и 2, погоре)			
-			
-			
-			
Доколку е потребно, додајте дополнителни редови			
ЗАБЕЛЕШКА: Според ЗЗЛП, преносите во земји кои не биле задолжени да обезбедат „соодветно ниво“ на заштита може да се случат само доколку се поставени „соодветни заштитни мерки“, како што е наведено во левата колона, подолу, или ако се применува отстапување, како што е наведено во десната колона			

Заштитни мерки според ЗЗЛП: 1. Меѓународен инструмент меѓу јавните органи; 2. Обврзувачки корпоративни правила; 3. Одобрени стандардни клаузули за пренос на податоци; 6. Одобрени ад хок клаузули.	Исклучоци, доколку соодветни заштити не се достапни: 7. Согласност; 8. Договор меѓу контролорот и субјектот на личните податоци; 9. Договор помеѓу контролорот и трето лице; 10. Неопходно заради важни причини од јавен интерес; 11. Потребни за правни побарувања; 12. Неопходно за заштита на суштинските интереси на субјектот на лични податоци или други; 13. Преносот се врши од регистар достапен за јавноста.
Дали постојат правила за да се постапува по основ на која било пресуда на суд или трибунал и која било одлука на управен орган на трета земја што може да му послужи на контролорот или кој било обработувач, а кој бара контролорот или обработувачот да спроведат пренос или откривање на личните податоци? (не е задолжително, но се препорачува заради евиденција, да се пополни)	Наведете Да/Не и ако да, ве молиме дајте копија од насоките
Забелешка: Наведете Да/Не и ако да, ве молиме дајте копија од насоките	Обезбедете детали:
Дали се чуваат личните податоци наведени во II.1. хартиено или во електронски формат?	
Каде (физички) се складирани податоците? (во канцелариите? На серверите на контролорот? На серверите на поврзаната организација? На сервери на трета страна (на пр., давател на услуги во облак)?	

Кои мерки се применуваат за заштита од неовластен пристап до физичкиот простор каде што податоците се складирани/достапни? Дали постои политика за безбедност на податоците која го регулира ова? (Доколку постои, ве молиме обезбедете копија)	
Каков хардвер се користи при обработката на личните податоци? Кој е одговорен за управувањето и безбедноста на овој хардвер?	
Дали (кои било од) податоците се чуваат на преносен/и медиуми/уреди? Во чија сопственост се медиумите/уредите?	
Може ли некој од луѓето со пристап до податоците да користат лични уреди за пристап или да ги обработуваат податоците? Доколку да, дали постои политика за заштита на користењето на сопствените уреди? Потребно е да обезбедите копија од политиката.	
Дали сите лица овластени да пристапат до лични податоци подлежат на обврската за доверливост (било да е тоа според закон или професионален сет норми или согласно договорните обврски)? Ве молиме наведете детали или копии од сите релевантни правни или договорни клаузули	
Кој софтвер/апликации се користат за обработка на податоците? (на пр., пакет за десктоп на „Мајкрософт офис“, централно управувана апликација, услуга во „облак“, итн.)	

Дали овој софтвер се управува локално или централно? Доколку обработката е централна, кој е централниот ентитет? Ако тоа не сте вие, има ли формален однос меѓу тој субјект и вашата организација во однос на употребата на софтверот? Ве молиме наведете копија од овој документ.	
Дали софтверот е базиран во „облак"? Доколку да, кој е давател на услугите, и каде е законски базиран тој провајдер? А каде е/се серверите физички лоцирани? Дали податоците во „облакот" се криптирани? Како (односно користејќи каква технологија за енкрипција)? Ве молиме дајте копија од договорот врз чија основа се одвива оваа обработка.	
Кој е одговорен (т.е. кој е „администратор") на овој софтвер? (Вие? Некој друг внатре во вашата организација? Некој во субјектот со кој сте поврзани? Трета страна?)	
Дали податоците се во секое време/ во кои било околности електронски пренесени до друг медиум, систем или уред?	
Ако се пренесуваат електронски, дали е ова направено: - преку интернет? Ако е така, дали податоците биле енкриптирани? На кој начин (т.е., користејќи каква технологија за енкрипција)? - со помош на FTP? Како е ова обезбедено? - со помош на VPN? Како е тоа обезбедено? - друго (наведете)	

ПРИЛОГ 3: Пристап усвоен од ENISA (Европска агенција за кибербезбедност) која се надоврзува на меѓународно прифатениот стандард ISO 27005: „Заканите ги злоупотребуваат ранливостите на средствата што доведува до предизвикување штета на организацијата[37]“ ;

Елементите на ризик и нивните односи може да се прикажат на следниов начин:

Дефинирањето на различните нивоа на влијание може да бидат групирани во четири нивоа и тоа:

Ниво на влијание	Опис
Ниско	Субјектите може да наидат на неколку помали непријатности, што ќе бидат надминати без проблем (потрошено време за повторно внесување информации, нервози, иритации итн.).
Средно	Субјектите може да наидат на значителни непријатности, што ќе можат да ги надминат и покрај неколкуте тешкотии (дополнителни трошоци, одбивање пристап до деловни услуги, страв, недостаток на разбирање, стрес, мали физички заболувања, итн.).
Високо	Субјектите може да наидат на значителни последици кои треба да бидат способни да ги надминат иако со сериозни тешкотии (погрешно присвојување на средства, ставање црна листа од страна на финансиски институции, материјална штета, губење работа, покана, влошување на здравјето и сл.).
Многу високо	Субјектите кои може да наидат на значајни, па дури и неповратни последици, кои можеби нема да бидат надминати (неспособност за работа, долготрајна психолошка или физичка болест, смрт, итн.).

За секоја област за оценување, се поставуваат пет прашања, на кои барем еден позитивен одговор укажува на ризик, како што е наведено во табелата.

Лицето кое го проценува безбедносниот ризик може, од овие одговори, да ја утврди веројатноста за појава на заканата. Овој резултат потоа може да се комбинира со оцената за влијанието за да се дојде до севкупниот ризик за конкретна активност за обработка на личните податоци.

[37] Извор: ENISA Threat Landscape Report 2016, Figure 4: The elements of risk and their relationships according to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscapereport- 2016. See also its 2017 report, https://www.enisa.europa.eu/publications/enisa-threatlandscape- report-2017.

ЧЕТИРИТЕ ГЛАВНИ ОБЛАСТИ ЗА ОЦЕНУВАЊЕ ВО ОДНОС НА БЕЗБЕДНОСТА НА ПОДАТОЦИТЕ:

Мрежа и технички ресурси	**Процеси и процедури**	**Вклучени страни и лица**	**Безбедност и нарушување**
1. Дали дел од обработката на личните податоци се спроведува преку интернет?	6. Дали улогите и одговорностите во однос на обработката на личните податоци се нејасни односно недоволно јасно дефинирани?	11. Дали обработката на личните податоци се спроведува од страна на неопределен број вработени?	16. Дали сметате дека вашата индустрија е подложна на напади во дигиталниот простор?
2. Дали е можно да се обезбеди пристап до внатрешниот систем за обработка на лични податоци преку интернет (на пр., За одредени корисници или групи корисници)?	7. Дали користењето на мрежата, системот и физичките ресурси во рамките на организацијата е двосмислено или не е јасно дефинирано?	12. Дали кој било дел од активностите за обработка на личните податоци се спроведува од страна на изведувач/трета страна (обработувач на податоци)?	17. Дали вашата организација има претрпено напад во дигиталниот простор или друг вид безбедносен (сигурносен) инцидент/нарушување во последните две години?
3. Дали системот за обработка на личните податоци е меѓусебно поврзан со друг надворешен или внатрешен ИТ-систем или услуга, кој припаѓа на вашата организација?	8. Дали е дозволено вработените да донесат и користат сопствени преносни уреди за да се поврзат со системот за обработка на личните податоци?	13. Дали обврските на странite/лицата вклучени во обработката на личните податоци е двосмислена или не јасно наведена?	18. Дали имате применo какво било известување и/или поплаки во однос на безбедноста на ИТ-системот (кој се користи за обработка на личните податоци), во последната година?

4. Дали неовластени лица можат лесно да пристапат до средината каде се обработуваат личните податоци?	9. Дали на вработените им е дозволено да префрлат, собираат или на друг начин да пренесуваат лични податоци, надвор од просториите на организација?	14. Дали вработените кои се вклучени во обработката на личните податоци не се запознаени со прашања поврзани со информациска сигурност на податоците?	19. Дали евиденцијата на активностите за обработка опфаќа голем обем субјекти и/или лични податоци?
5. Дали системот за обработка на личните податоци е дизајниран, спроведен или се одржува без следење на најдобрите релевантни практики?	10. Може ли обработката на личните податоци да се спроведе, без соодветна ревизорска трага (логови)?	15. Дали лицата/страните вклучени во обработката на податоците ја занемаруваат процедурата на безбедно чување и/или уништување на личните податоци?	20. Дали постојат најдобри безбедносни практики специфични за вашиот бизнис-сектор кои не биле адекватно применети?

ВЕРОЈАТНОСТ ЗА ПОЈАВА НА ЗАКАНА (1):

Област на процена	Број „ДА“ одговори на прашањата погоре	Ниво	Бодови
Мрежа и технички ресурси	0-1 2-3 4-5	Ниско Средно Високо	1 2 3
Процеси и процедури	0-1 2-3 4-5	Ниско Средно Високо	1 2 3
Страни и вклучени лица	0-1 2-3 4-5	Ниско Средно Високо	1 2 3
Безбедност и нарушување	0-1 2-3 4-5	Ниско Средно Високо	1 2 3

Горенаведените резултати се внесуваат во следната збирна табела:

ВЕРОЈАТНОСТ ЗА ПОЈАВА НА ЗАКАНА (2):

Вкупен износ	Ниво за веројатност за појава на закани
4-5	Ниско
6-8	Средно
9-12	Високо

Конечно, овие резултати потоа може да се комбинираат со резултатите од „Ниво на влијание“ за да се прикаже севкупниот ризик, како што следува:

ЦЕЛОСНА ПРОЦЕНА НА РИЗИК

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)

ПРИЛОГ 4 – Примери за нарушување на безбедноста на личните податоци и кој да се извести (Од упатствата на WP29)

Пример	Известете го супервизорскиот авторитет?	Известете ги субјектите на личните податоци?	Забелешки/пораки
i. Контролорот зачувал резервна копија од архивата на личните податоци која е енкриптирана со клуч. Клучот е украден за време на неовластен пристап.	Не	Не	Сè додека податоците се енкриптирани и постојат резервни копии на податоците што се зачувани со единствен клуч кој не е компромитиран и податоците може да се обноват во прифатлив период, ова може да не се третира како нарушување кое треба да се пријави. Меѓутоа, доколку единствениот клуч е подоцна компромитиран, потребно е известување.
ii. Контролорот одржува онлајн сервис. Како резултат на кибернапад на тој сервис, украдени се лични податоци. Контролорот има клиенти во земји членки на ЕУ.	Да, пријавете во АЗЛП, доколку има веројатност од последици врз личните податоци на субјектите што го користат тој сервис.	Да, пријавете на засегнатите субјекти, во зависност од природата на личните податоци и доколку веројатноста и сериозноста на последиците по субјектите е висока.	

iii. Кратко губење струја во траење од неколку минути, при што клиентите не се во можност да пристапат до своите податоци	Не	Не	Ова не е известување за нарушување на безбедноста на личните податоци, но е сигурносен инцидент при што тој треба да се забележи во соодветна евиденција за инциденти.
iv. Контролор страда од ransomware напад кој резултира со енкрипција на сите податоци. Нема достапни резервни копии и податоците не можат да бидат повторно вратени. За време на истрагата, станува јасно дека функционалноста на откупниот софтвер (ransomware) била да ги заклучи (криптира) податоците, и дека не е констатиран друг малициозен софтвер присутен во системот.	Да, пријавете до АЗЛП, доколку постои веројатност за последици, за субјектите на личните податоци имајќи предвид дека станува збор за губење на нивната расположливост.	Да, пријавете на субјектите на личните податоци, во зависност од природата на личните податоци што се засегнати и укажете на можниот ефект од недостаток на расположливоста на податоците, како и на сите останати слични последици	Доколку имало достапна резервна копија и податоците би можеле да се обноват навреме, ова не би требало да биде пријавено на АЗЛП или на субјектите на личните податоци, бидејќи не дошло до трајно губење на доверливоста. Сепак, доколку АЗЛП добие информација за инцидентот на друг начин, може да спроведе истрага за да се процени усогласеноста со барањата за безбедност
v. Личните податоци на голем број студенти се погрешно испратени до погрешна електронска пошта која содржи 1000+ приматели.	Да, пријавете до АЗЛП.	Да, известете ги субјектите на личните податоци, во зависност од опсегот и видот на личните податоци што се опфатени, како и на сериозноста на можните последици	

ПРИЛОГ 5 – Контролна листа за офицерот за заштита на личните податоци во поглед на усогласеноста на работењето на контролорот со Законот за заштита на личните податоци и соодветните подзаконски акти од областа на заштитата на личните податоци

Име на контролорот: _____

Офицер за заштита на лични податоци (име и презиме, електронска пошта, и сл.): _____

Година: _____

(Се препорачува оваа контролна листа да се пополнува на годишно ниво, на крајот од секоја календарска година од страна на офицерот за заштита на личните податоци, со цел да се следи исполнувањето на обврските што произлегуваат од прописите за заштита на личните податоци)

Напомена: Листата прашања може ориентациски да послужи за да се добие преглед на моменталната усогласеност на контролорот со релевантната регулатива од областа на заштитата на личните податоци.

1. Дали контролорот има назначено офицер за заштита на лични податоци, со соодветен интерен правен акт (одлука, решение и сл.) со кој е назначен на оваа позиција, а кој ги поседува потребните квалификации во согласност со ЗЗЛП?

а) ДА

б) НЕ

в) Забелешка:

2. Дали офицерот директно одговара на раководството на контролорот?

а) ДА

б) НЕ

в) Забелешка:

_____

3. Дали офицерот има редовна комуникација со раководството на контролорот?

а) ДА

б) НЕ

в) Забелешка:

_____

4. Дали офицерот ги има на располагање потребните ресурси за вршење на својата функција (работен простор, опрема, непречен и директен пристап до неопходните документи, и сл.)?

а) ДА

б) НЕ

в) Забелешка:

---

5. Дали офицерот за заштита на личните податоци врши и други работни задачи што можат да доведат до потенцијален судир на интереси?

а) ДА

б) НЕ

в) Забелешка:

---

6. Дали офицерот учествува на обуките организирани и спроведени од страна на Агенцијата за заштита на личните податоци, како и други стручни едукации?

а) ДА

б) НЕ

в) Забелешка:

---

7. Дали контролорот ги објавил контакт-податоците на офицерот за заштита на личните податоци, и доставил известување до Агенцијата за заштита на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

8. Дали контролорот располага со интерни акти за заштита на лични податоци? (пр., Политика/Изјава за приватност, Политика за користење колачиња, Правилник за начинот на вршење видеонадзор, Процедура за права на субјектите на лични податоци и сл.)

а) ДА

б) НЕ

в) Забелешка:

---

9. Дали контролорот подготвува процена на влијанието на планираните активности за обработка на податоците врз заштитата на личните податоци (Data Protection Impact Assessment)?

а) ДА

б) НЕ

в) Забелешка:

---

10. Дали контролорот за соодветните активности за обработка на личните податоци има донесено интерни акти со кои се пропишува план и соодветно се уредуваат техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци; определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење документи и информатичко-комуникациската опрема, уредување на процедурата за пријавување, реакција и санирање инциденти; пропишување на процедурата за начинот на правење сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци; како и процедура за начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите и сл.)

а) ДА

б) НЕ

в) Забелешка:

---

11. Дали контролорот, при активностите за обработка на личните податоци во рамки на деловните процеси, ги спроведува пропишаните технички и организациски мерки?

(Напомена: Да се наведе поединечно за секоја активност за обработка на личните податоци)

а) ДА

б) НЕ

в) Забелешка:

---

12. Дали се идентификувани ризиците во однос на тајноста и заштитата на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

13. Дали е воспоставена и дали редовно се ажурира евиденцијата (Регистарот) на активностите за обработка на личните податоци? Дали евиденцијата содржи: назив на активноста за обработка, цел на обработката, правна основа за обработка на личните податоци, рокови за бришење, дали личните податоци се пренесуваат во трети земји и сл.)

а) ДА

б) НЕ

в) Забелешка:

---

14. Дали кај контролорот има регистрирано нарушување на безбедноста за заштита на личните податоци, и дали е соодветно евидентирана повредата, вклучително и за причините за повредата, последиците и преземените мерки за нејзино отстранување?

а) ДА

б) НЕ

в) Забелешка:

---

15. Дали кај контролорот се случила повреда која би можела да доведе до ризик по правата и слободите на физичките лица и дали за тоа е известена Агенцијата за заштита на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

16. Дали контролорот пренесува податоци за поединци во други држави или меѓународни организации, во согласност со законот?

а) ДА (да се наведат кои податоци, каде, на кого, правна основа за преносот)

б) НЕ

в) Забелешка:

---

17. Дали се склучени договори за обработка на личните податоци меѓу контролорот и обработувачот со детални правила и постапки за обезбедување соодветно ниво на заштита на личните податоци за време на нивната обработка? (стандардни клаузули)

а) ДА

б) НЕ

в) Забелешка:

---

18. Дали контролорот обработува посебна категорија лични податоци (податоци со кои се открива расно или етничко потекло, политичко мислење, верско или филозофско уверување или членство во синдикат, како и генетски податоци, биометриски податоци, за цели на единствена идентификација, податоци за здравствената состојба или податоци за сексуалниот живот или сексуална ориентација на физичкото лице)? И дали за тоа се консултира офицерот?

а) ДА (да се наведат кои податоци, каде, на кого, правна основа за преносот)

б) НЕ

в) Забелешка:

---

19. Дали контролорот обработува податоци за кривични пресуди и санкции и дали за обработката на овие лични податоци применува посебни мерки за заштита на правата и слободите на поединците на кои се однесуваат овие лични податоци?

а) ДА (да се наведе во составот на институцијата во која активност за обработка на лични податоци се обработуваат овие податоци, правна основа и за која цел)

б) НЕ

в) Забелешка:

---

20. Дали контролорот има обработувач/и, кој во негово име врши обработка на лични податоци и со нив е уреден односот со договор или со друг правно обврзувачки акт?

а) ДА (да се наведе кои активности за обработка на лични податоци се доделени на обработувач/и и со кој акт е уреден овој однос)

б) НЕ

в) Забелешка:

---

21. Дали контролорот открива лични податоци на примателi (физичко или правно лице, односно орган на државна власт?

а) ДА (да се наведе кои податоци, идентитет на примачот, правна основа и цел на откривање на лични податоци)

б) НЕ

в) Забелешка:

---

22. Дали доколку станува збор за заеднички контролори постои цел и начин на обработка на личните податоци и дали за таа обработка имаат меѓусебен договор?

а) ДА (да се наведе во рамки на која активност, кој е сопственик на деловниот процес и со кој договор е уреден)

б) НЕ

в) Забелешка:

---

23. Дали офицерот подготвува план за одржување едукација (обука) за заштита на личните податоци, приспособени на потребите на вработените на институцијата (основни, напредни, специјализирани и сл.)

а) ДА

б) НЕ

в) Забелешка:

---

24. Дали офицерот организира и спроведува редовна комуникација со сите вработени, трети страни со кои соработува и сл., со цел подигнување на свеста за заштита на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

25. Дали постои пропишана процедура со чија согласност офицерот е вклучен со свое стручно мислење при подготовката и развојот на нови продукти, услуги и ИТ-системи?

а) ДА

б) НЕ

в) Забелешка:

---

26. Дали офицерот е вклучен со мислење во поглед на обезбедувањето согласност од субјектите на личните податоци, за обработка на нивните лични податоци?

а) ДА

б) НЕ

в) Забелешка:

---

27. Дали офицерот е консултиран при обработката на посебните категории лични податоци?

а) ДА

б) НЕ

в) Забелешка:

---

28. Дали офицерот спроведува ревизии/контроли/проверки на почитувањето на прописите за заштита на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

29. Дали постои годишен план за спроведување ревизии/контроли/проверки донесен од страна на офицерот и дали доколку е применливо, тој е спроведен за претходната година?

а) ДА

б) НЕ

в) Забелешка:

---

30. Дали контролорот постапил по наодите и препораките, во дадените рокови за постапување? (да се наведе што сè уште не е затворено)

а) ДА

б) НЕ

в) Забелешка:

---

31. Дали е постапено по наодите од надворешни контроли? (да се наведе што сè уште не е затворено)

а) ДА

б) НЕ

в) Забелешка:

---

32. Дали се спроведуваат периодични контроли во согласност со документацијата за техничките и организациските мерки?

Напомена: Потребно е посебно да се одговори на секоја од горенаведените опции:

а) ДА

б) НЕ

в) Забелешка:

---

33. Дали контролорот постапил по наодите од Извештајот за периодична проверка и ги известил офицерот и одговорните лица на контролорот?

а) ДА

б) НЕ

в) Забелешка:

---

34. Дали кај контролорот е извршен инспекциски надзор од страна на Агенцијата за заштита на личните податоци? Дали се утврдени со решение повреди или неправилности, односно дали се дадени одредени препораки? Доколку да, дали е постапено по нив?

а) ДА

б) НЕ

в) Забелешка:

---

35. Дали во случај на пренос на лични податоци надвор од земји на ЕУ и ЕЕП, офицерот презема активности за поведување постапка за добивање соодветно одобрение за пренос од страна на Агенцијата за заштита на лични податоци?

а) ДА

б) НЕ

в) Забелешка:

---

36. Дали вработените имаат добиено овластување за обработка на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

37. Дали вработените имаат потпишано изјава за тајност и заштита на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

38. Дали контролорот има воспоставено и дали редовно ја ажурира евиденцијата на овластените лица за обработка на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

39. Дали вработените се запознаени со документацијата за техничките и организациските мерки и дали таа е достапна за нив?

а) ДА

б) НЕ

в) Забелешка:

---

40. Дали се доставуваат Извештаи за неправилност/и од вработените до офицерот?

а) ДА

б) НЕ

в) Забелешка:

41.Дали контролорот ја известил Агенцијата за обработка (на лични податоци) со висок ризик ?

а) ДА

б) НЕ

в) Забелешка:

---

42. Дали контролорот информира во случај на нарушување на безбедноста односно повреда на личните податоци?

а) ДА

б) НЕ

в) Забелешка:

---

43. Дали субјектите на личните податоци имаат право на пристап до информациите што се однесуваат на соодветна обработка на нивните лични податоци и дали овие информации се лесно достапни за засегнатите субјекти?

а) ДА

б) НЕ

в) Забелешка:

---

44. Дали е подготвен образец на барање за остварување на правата на субјектите на личните податоци и процедура како субјектите на личните податоци можат да ги остварат своите права?

а) ДА

б) НЕ

в) Забелешка:

---

45. Дали вработените се запознаени со интерните акти како субјектите на личните податоци можат да пристапат до сопствените лични податоци?

а) ДА

б) НЕ

в) Забелешка:

---

46. Дали е предвидена постапка која осигурува дека приговорите и забелешките во врска со обработката на личните податоци ќе бидат разгледани без одлагање?

а) ДА

б) НЕ

в) Забелешка:

---

45. Дали е предвидена постапка која осигурува дека во случај кога се врши директен маркетинг, субјектите на личните податоци се информирани за нивните права?

а) ДА

б) НЕ

в) Забелешка:

К О М Е Н Т А Р И

ПРИЛОГ 6 – ЛИСТА ЗА ПРОВЕРКА ЗА ПРИМЕНА НА ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ ВО СОГЛАСНОСТ СО ПРАВИЛНИКОТ ЗА БЕЗБЕДНОСТ И НАЈДОБРИТЕ ПРАКТИКИ ОД ЕУ

Листа мерки		Мерка	
1.	Подигнување на свеста на корисниците	Информирање и подигнување на свеста на индивидуите за начинот на управување со податоците	☐
2.	Автентикација	Дефинирање единствен идентификатор (логин) за секој корисник	☐
		Усвојување политика за кориснички лозинки според препораките на АЗЛП	☐
		Задолжителна (форсирана) промена на лозинката за секој корисник при нејзино ресетирање.	☐
		Лимитирање на бројот неуспешни обиди за најава на корисниците	☐
3.	Управување со пристапи	Дефинирање профили	☐
		Отстранување застарени кориснички привилегии за пристап	☐
		Спроведување годишна контрола (ревизија) на пристапи и привилегии	☐
4.	Логирање пристапи и управување со инциденти	Имплементирање на систем за логирање (logging)	☐
		Информирање на корисниците за имплементацијата на системот за логирање	☐
		Заштита на опремата користена за логирање и на самите логови	☐
		Имплементација на процедури за известување при нарушување на безбедноста на личните податоци	☐

5.	Безбедност на работните станици	Утврдување процедура за автоматско заклучување на работните станици по изминат период	☐
		Употреба на редовно ажурирање на антивирусот	☐
		Инсталирање „огнен ѕид“ (firewall)	☐
		Добивање согласност од корисниците при интервенција на нивната работна станица	☐
6.	Безбедност на обработката на личните податоци на преносните (мобилни) уреди	Утврдување механизми за енкрипција за преносните (мобилни) уреди	☐
		Спроведување редовни резервни копии и синхронизации	☐
		Дефинирање мерка за отклучување на паметните телефони (лозинка, пин итн.)	☐
7.	Заштита на внатрешната мрежа	Ограничување на мрежниот сообраќај, но само неопходниот да биде активен	☐
		Безбеден далечински пристап преку VPN	☐
		Имплементација на WPA2 или WPA2-PSK протокол за WI-Fi-мрежи	☐
8.	Обезбедување на серверите	Дозвола на пристап до алатките и администраторскиот интерфејс само на квалификувани лица	☐
		Инсталирање клучни надградби без одолжување	☐
		Обезбедување достапност до податоците	☐
9.	Обезбедување на интернет-страницата/страниците	Користење на TLS-протокол и проверка на неговата имплементација	☐
		Проверка дека лозинките и идентификаторите не се префрлаат преку URL	☐
		Проверка дека она што се бара корисниците да внесат ги исполнува нивните очекувања	☐
		Вметнување банер за согласност за користење колачиња за оние кои не се неопходни за користење на услугата	☐

10.	Обезбедување континуитет	Вршење редовни сигурносни копии	☐
		Чување на медиумите каде што сигурносната копија на безбедно место	☐
		Имплементирање безбедносни мерки за пренесување на сигурносните копии	☐
		Имплементирање и редовно тестирање на планот за континуитет во работењето	☐
11.	Безбедно архивирање	Имплементирање одредени методи за пристап до архивираните податоци	☐
		Безбедно уништување застарени архиви	☐
12.	Надгледување на одржувањето и уништувањето на податоците	Водење евиденција на одржувањето во некој вид регистар	☐
		Имање одговорно лице од организацијата да ја надгледува работата на трети страни	☐
		Бришење на податоците од сите хардвери пред тие да се уништат	☐
13.	Управување со обработувачи	Стандардни договорни клаузули	☐
		Дефинирање на начинот и условите за уништување на податоците	☐
		Начин на постапување со личните податоци (ревизии, посети и сл.)	☐
14.	Обезбедување размена на податоци со други организации	Енкриптирање на податоците пред праќање	☐
		Обезбедување дека информацијата ќе стигне само до оној кој треба да ја прочита	☐
		Испраќање на тајниот клуч (лозинка или сл.) преку друг канал	☐
15.	Физичка безбедност	Примена на рестриктивен пристап до одредени локации (систем сала, архива и сл.)	☐
		Инсталација на аларми и нивна редовна проверка	☐
16.	Надгледување на софтверскиот развој	Нудење параметри што ја почитуваат приватноста на крајните корисници	☐
		Тестирање на анонимизирани или измислени податоци	☐

17.	Користење криптографија	Користење признати алгоритми, софтвери и библиотеки	☐
		Чување на тајните информации и криптографски клучеви на безбеден начин	☐

ПРИЛОГ 6 – Листа за проверка за клучните области на дејствување во врска со ВИ и човековите права

Процена на влијанието врз човековите права	**Правете го ова**
	Преземете чекори за воведување закони и регулативи што бараат ПВЧП да се спроведува за системите за ВИ кои биле или можат да бидат набавени, развиени и/или ставени во функција од страна на државните институции. Навремено спроведете ПВЧП за сите системи за ВИ што веќе се ставени во функција/веќе се користат од страна на државните институции во моментот кога е усвоена релевантната правна рамка за ПВЧП. Во противно ПВЧП мора прво да се спроведе пред набавката и/или развојот на системот за ВИ од страна на државната институција. Континуирано следете ги влијанијата на системот за ВИ врз човековите права низ нивниот животен циклус и спроведувајте редовни ПВЧП во секоја нова фаза од животниот циклус и кога има промени во контекстот, опсегот, природата и целта на системите.
	Не правете го ова
	Не заборавајте да се консултирате и да добиете информации од релевантни засегнати страни, вклучително и организациите за граѓанско општество и оние со релевантна експертиза за ВИ и човекови права, кога воведувате правна рамка за ПВЧП. Немојте да спроведувате ПВЧП на нетранспарентен начин и не користете или олеснувате ја употребата на законите за доверливост, приватност, деловна тајна, државна тајна или интелектуална сопственост за да го спречите спроведувањето или објавувањето на ПВЧП. Немојте да набавувате, развивате, ставате во употреба или користите систем за ВИ кој има потенцијал да се меша во човековите права во околности кога (i) не бил предмет на ПВЧП или (ii) ПВЧП открива дека системот за ВИ претставува реален ризик за кршење на човековите права и не се применети мерки или механизми за спречување или ублажување на идентификуваните ризици.

Јавна консултација	**Правете го ова**
	Применувајте стандарди за отворени набавки и транспарентен процес за употреба на системи за ВИ. Вклучете ги сите засегнати страни во јавните консултации, вклучително и засегнатите групи или заедници, минимално за време на фазите за набавка и фазите за спроведување на ПВЧП.
	Не правете го ова
	Не обезбедувајте јавни консултации без да преземете соодветни мерки за да ги направите значајни, вклучително и навремено претходно објавување на сите релевантни информации поврзани со системот за ВИ.
Информираност и транспарентност	**Правете го ова**
	Обезбедете ги сите потребни информации за да можат поединците да разберат кога и како се користат системите за ВИ, особено кога станува збор за јавните услуги.
	Не правете го ова
	Немојте да користите системи за ВИ кои се сложени до степен што не можат да бидат предмет на човечки преглед и контрола во согласност со соодветните стандарди за транспарентност и одговорност (отчетност).

Заштита на лични податоци и приватност	**Правете го ова**
	Направете преглед и процена на постојните закони за заштита на личните податоци за да утврдите дали тие доволно го штитат правото на почитување на приватниот живот и правото на заштита на личните податоци во контекст на системите за ВИ. Проактивно преземете чекори за да се осигурите дека приватните и државните институции вклучени во развој, ставање во употреба и користење на системите за ВИ ги почитуваат правата на субјектите на личните податоци и ги исполнуваат нивните обврски во согласност со применливите закони за заштита на личните податоци.
	Не правете го ова
	Немојте да правите големи и непропорционални исклучоци за оние кои развиваат, стават во употреба или користат системи за ВИ. Не дозволувајте развој или употреба на системи за ВИ кои се потпираат на обука или тестирање збирки податоци кои биле собрани или на друг начин обработени со кршење на правото на почитување на приватниот живот и правото на заштита на личните податоци. Не дозволувајте развој или употреба на системи за ВИ што обработуваат лични податоци било како влезни или излезни податоци, со што се крши правото на почитување на приватниот живот и правото на заштита на личните податоци.

За крај

Преку изборот на темите од регулативата за заштита на личните податоци во овој Водич, се обидовме да разработиме наслови што сметаме дека се посебно актуелни и чести за успешно спроведување на задачите и одговорностите што се очекуваат од вас, како офицер за заштита на личните податоци.

Препорачуваме за дополнителни насоки, како и одредени корисни содржини, кои би нашле непосредна практична примена во работењето, да ја користите официјалната страница на Агенцијата за заштита на личните податоци, посебно во делот наменет за контролорите, како и документот „Насоки за офицери за заштита на личните податоци" донесен од Европскиот одбор за заштита на личните податоци.

Успешна работа и работете на градење квалитет, култура и препознатливост на позицијата – офицер за заштита на личните податоци во вашите институции.