Финансирано од Европска Унија

ЕУ со ТЕБЕ

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

МЗМП

ДОКУМЕНТ ЗА ЈАВНИ ПОЛИТИКИ

УЛОГАТА НА СУДСТВОТО И ЈАВНОТО ОБВИНИТЕЛСТВО ВО СИСТЕМОТ НА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРАВОТО НА ПРИВАТНОСТ

УЛОГАТА НА СУДСТВОТО И ЈАВНОТО ОБВИНИТЕЛСТВО ВО СИСТЕМОТ НА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРАВОТО НА ПРИВАТНОСТ

Издавач:
Македонско здружение на млади правници
Центар за правни истражувања и анализи

За издавачот:
Бојана Божиновска Силјановска, Претседателка на МЗМП
Лидија Стојкова Зафировска, Претседателка на ЦПИА

Автор:
Игор Кузевски

Редакција:
Милена Јосифовска, ЦПИА
Сара Марковска, ЦПИА
Маја Атанасова, МЗМП

Лектура:
Дејан Василевски

Графички дизајн:
Релатив

Оваа публикација е изработена во рамките на проектот „**Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн-просторот**“, финансиран од Европската унија. Содржината на публикацијата е единствена одговорност на авторот и на никаков начин не може да се смета дека ги одразува гледиштата на Европската унија.

СОДРЖИНА

ПРЕДГОВОР

Овој документ за јавни политики е подготвен во рамките на проектот: „Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн просторот“, финансиран од Европската унија и имплементиран од Центарот за правни истражувања и анализи (ЦПИА) и Македонско здружение на млади правници (МЗМП). Цел на проектот е да се зајакнат капацитетите на судството и јавното обвинителство во ефикасна заштита на приватноста на граѓаните, како и другите права и основни слободи засегнати од новите технологии во онлајн просторот во согласност со правото и стандардите на ЕУ.

Целта на овој документ за јавни политики е да обезбеди сеопфатен и стратешки пристап за решавање на клучните предизвици за Улогата на судството и јавното обвинителство во системот на заштита на личните податоци и правото на приватност.

Преку овој документ, се настојува да се идентификуваат и анализираат главните проблеми кои бараат интервенција, да се дефинираат приоритетите и да се предложат конкретни решенија кои ќе придонесат за унапредување на политиките за Улогата на судството и јавното обвинителство во системот на заштита на личните податоци и правото на приватност. Посебен акцент се става на инклузивноста во пристапот, каде што заклучоците и препораките ќе бидат заеднички потврдени преку активна дебата со претставници на сите засегнати институции. Ова ќе осигури дека различните перспективи и интереси се земени предвид, создавајќи сеопфатни и балансирани политики.

Со имплементација на предложените мерки, се очекува да се постигне значителен напредок во справувањето со идентификуваните проблеми и да се создадат услови за континуирано подобрување на јавните политики и услуги во областа на улогата на судството и јавното обвинителство во системот на заштита на личните податоци и правото на приватност.

ВОВЕД

Сигурноста и тајноста на личните податоци, како и почитувањето и заштитата на приватноста на граѓаните на Република Северна Македонија се слободата и правата што се гарантираат со Уставот на Република Македонија од 17 ноември 1991 година.

Иако гарантирани со Уставот, овие права практично и реално почнуваат вистински да се гарантираат и да се почитуваат со донесувањето на Законот за заштита на личните податоци од 2005 година.[1]

Но, брзиот технолошки развој и глобализацијата придонесоа и континуирано придонесуваат кон појавата на нови предизвици во однос на заштитата на личните податоци и заштитата на приватноста. Имено, модерните и современите технологии во денешно време овозможуваат обработката на личните податоци да се случува во досега невидени размери и обем, а притоа географската одредница и политичките граници помеѓу државите се сè помалку видливи и во таканаречениот „дигитален свет“ практично исчезнуваат. Со новите предизвици за човековите права и основните слободи, особено правото на приватен живот, постои неизбежна потреба за соодветен „одговор“, со цел подобро да се одговори на овие предизвици за приватноста што произлегуваат од зголемената употреба на новите информатички и комуникациски технологии.

Од овие причини, Европската унија ја усвои Регулативата (ЕУ) 2016/679 на Европскиот парламент и на Советот од 27 април 2016 година за заштита на физички лица во поглед на обработката на лични податоци, за слободно движење на таквите податоци и за укинување на Директивата 95/46/ЕЗ – Општа регулатива за заштита на податоци (GDPR), која во ЕУ почна да се применува во мај 2018 година. Оттогаш, GDPR е глобална референтна точка за заштитата на личните податоци. Имено, GDPR воспостави иновативен систем на управување што има цел да обезбеди усогласено толкување, примена и спроведување на правилата за заштита на личните податоци. Следствено, многу земји ширум светот, вклучително и оние надвор од Европската унија, ги модернизираа(т) своите закони и „правила на игра“ во однос на почитувањето на приватноста и заштитата на личните податоци, особено тогаш кога при обработката на личните податоци се користат нови современи информатички и комуникациски технологии.

Во овој контекст, и Република Северна Македонија ја модернизираше правната и институционалната рамка за заштитата на личните податоци во 2020 година со донесувањето на новиот Закон за заштита на личните податоци[2], кој почна да се применува во целост од август 2021 година. Со овој закон, практично, правно се овозможија нови можности за зголемување на заштитата на поединците како субјекти на личните податоци и за олеснување на протокот на податоци според стандардите и начелата на овој закон, кој е целосно усогласен со GDPR во однос на неговите решенија. Оттука, Законот за заштита на личните податоци треба да се разбере како флексибилна, заштитна и ефективна алатка, која дозволува да се развиваат и да се имплементираат современи технолошки решенија, но со примена на технички и организациски мерки што ќе обезбедат ниво на безбедност на личните податоци што ќе биде соодветно на ризикот при нивната обработка, како и почитување на начелата поврзани со обработката на личните податоци.

1 Законот за заштита на личните податоци е објавен во „Службен весник на Република Македонија“, бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018. Овој закон веќе не е во сила.

2 Законот за заштита на личните податоци е објавен во „Службен весник на Република Северна Македонија“, бр. 42/2020 и 294/2021.

Од друга страна, Законот за заштита на личните податоци овозможува баланс во однос на техничкиот развој на начин што гарантира и им обезбедува на физичките лица како поединци повеќе применливи права, како што се правото на пристап, правото на исправка, правото на бришење, правото на приговор, правото на преносливост и обврската за зголемена транспарентност на оние што ги обработуваат личните податоци (контролорите и обработувачите).

Доколку контролорите и обработувачите ни ги заштитат овие права, регулаторот, односно Агенцијата за заштита на личните податоци[3], може да спроведе супервизија и согласно фактичката состојба, доколку се исполнети условите, да изрече глоби и други корективни мерки согласно законот, со единствена цел да се обезбеди колку е можно повисоко ниво на заштитата на овие уставно- загарантирани права и слободи – правото на приватност и заштитата на личните податоци при нивната обработка.

Кога се говори за Општата регулатива за заштита на податоците (*GDPR*), а во тој контекст и за Законот за заштита на личните податоци, треба да се истакне дека тие (Регулативата и Законот) постојат, односно се донесени најпрвин да го потврдат фактот дека сè повеќе се врши обработка на личните податоци на автоматизиран, дигитален, електронски начин со примена на современи технолошки решенија во областа на информатичките и комуникациските технологии (ИКТ). Нивната крајна цел треба да биде уредување на начинот, методите и постапките на обработка на личните податоци на начин што ќе биде согласно „новото“ време, не заборавајќи го притоа и традиционалниот начин на обработка на личните податоци. Имено, Законот дури и јасно утврдува дека контролорот во моментот на дефинирање на средствата за обработка, како и при обработката, е должен да предвиди, планира и примени соодветни технички и организациски мерки според најновите технолошки достигнувања. Притоа, земајќи ги предвид, меѓу другото, природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица кои произлегуваат од таквата обработка на личните податоци. Сето ова Законот за заштита на личните податоци го бара со цел ефикасно спроведување на начелата поврзани со заштитата на личните податоци и вклучување на потребните заштитни мерки во процесот на обработка, со цел да се исполнат барањата од овој закон и да се обезбеди заштита на правата на субјектите на личните податоци.

Но, кога ја споменавме Агенцијата за заштита на личните податоци, треба да се нагласи дека грижата за приватноста и заштитата на личните податоци, иако примарно е во нејзина надлежност, таа не зависи и објективно не може да зависи единствено „само“ од Агенцијата за заштита на личните податоци. Имајќи предвид дека станува збор, пред сè, за уставно-загарантирани човекови права и слободи, нивната заштита, покрај Агенцијата, значително зависи и од судовите во Република Северна Македонија што судат врз основа на Уставот и законите и меѓународните договори ратификувани во согласност со Уставот, како и Јавното обвинителство како единствен и самостоен државен орган што ги гони сторителите на кривични дела и на другите со закон утврдени казниви дела. Оттука, решенијата што ги овозможува новото модерно време во контекст на обработката и заштитата на личните податоци и приватноста, со примената на современи технолошки достигнувања при обработката на личните податоци се предизвик и за судовите и за обвинителствата во Република Северна Македонија.

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

Имено, брзиот информатичко-комуникациски развој сам по себе како „алатка“ за побрзо решавање на одредени појави и прашања во општеството, нужно доведува до зголемување на ризикот од можно загрозување или нарушување на дел од основните човекови и граѓански права и слободи гарантирани со Уставот на Република Северна Македонија, конкретно заштитата на личните податоци и правото на приватност, а во насока кон забрзување на развојот на државата. Но, со ова никогаш не треба да се дозволи постигнувањето на една цел – развој, ефикасност, ефективност и економичност..., да предизвика кршење или ограничување на човековите права и слободи. Следствено, кога усвојуваме и ја прифаќаме примената на современите информатичко-комуникациски технологии чија намена е на модерен, современ начин да ни го олеснат функционирањето на одредени процеси, а на кои многу веројатно е дека не им е примарна обработката на личните податоци (иако ќе имаме и такви случаи), треба да внимаваме тоа да се прави на начин што ќе биде соодветен, односно со примена на мерки што ќе обезбедуваат безбедност на личните податоци. Впрочем, само така може да се остане во духот на европските вредности и да се осигури дека примената на информатичко-комуникациските технологии ќе биде на начин што ќе обезбеди дека нема да бидеме „принудени“ да избираме помеѓу ефикасниот и ефективен развој од една страна и заштитата на личните податоци и правото на приватност како основни човекови права и слободи од другата страна, бидејќи објективно можат да се постигнат и двете.

Во таа насока, особено во денешното модерно време, предизвикот за судовите и обвинителствата во Република Северна Македонија е кога постапуваат во рамките на нивните судски и обвинителски функции и надлежности, да обезбедат баланс, помеѓу почитувањето и заштитата на личните податоци и правото на приватност од една страна, визави современиот технолошки, информатичко-комуникациски развој, од друга страна. За да се постигне ова ќе биде потребно не само познавање на правото туку и сè повеќе разбирање на модерните технолошки достигнувања од аспект на тоа дали тие обезбедуваат ефикасно спроведување на начелата за заштита на личните податоци со цел да се обезбеди заштита на правата на субјектите на личните податоци. Имено, треба да се има предвид дека не е секогаш технички изводливо сè што, согласно денешниот современ технолошки развој, е едновремено и општествено и етички прифатливо или, уште повеќе, законски дозволено. Во таа насока, улогата на судовите и јавните обвинителства во системот на заштита на лични податоци и приватноста е исклучително многу значајна и претставува предизвик на кој тие мораат да одговорат соодветно, и тоа кога се јавуваат во улога на контролор и при практикување на своите изворни правосудни надлежности.

1. ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРИВАТНОСТА

АЛАТКА ЗА ЕФИКАСНО СУДСТВО И ОБВИНИТЕЛСТВО

Прифаќајќи дека судовите и јавните обвинителства имаат значајна улога во системот на заштита на лични податоци и приватноста во продолжение се наведени предизвиците со кои се соочуваат тие, почнувајќи со уставно-правната рамка во оваа област.

1.1. ШТО ВЕЛИ УСТАВОТ?

Уставот уредува дека се гарантираат сигурноста и тајноста на личните податоци и дека на граѓаните им се гарантира заштита од повреда на личниот интегритет што произлегува од регистрирањето информации за нив преку обработката на податоците.

Понатаму, Уставот уредува дека на секој граѓанин му се гарантира почитување и заштита на приватноста на неговиот личен и семеен живот, на достоинството и угледот.

Уставот уредува дека судската власт ја вршат судовите, кои се самостојни и независни и судат врз основа на Уставот и законите и меѓународните договори ратификувани во согласност со Уставот, при што расправата пред судовите и изрекувањето на пресудата се јавни, а јавноста може да биде исклучена во случаи утврдени со законот.

Понатаму, Уставот уредува дека Јавното обвинителство ги врши своите функции врз основа на Уставот и законите и меѓународните договори ратификувани во согласност со Уставот, при што во Законот за јавното обвинителство[4] е утврдено дека Јавното обвинителство е единствен и самостоен државен орган што ги гони сторителите на кривични дела и на други казниви дела утврдени со законот, а врши и други работи утврдени со законот.

Говорејќи за Уставот од аспект на основните слободи и права на човекот и граѓанинот, треба да се нагласи дека сите органи на државната власт практикувањето на своите функции и надлежности треба да го вршат на начин што нема да ги ограничи или да ги загрози загарантираните човекови права и слободи.

1.2. ШТО ВЕЛИ ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ?

Законот за заштита на личните податоци (ЗЗЛП) уредува дека Агенцијата за заштита на личните податоци е самостоен и независен државен орган, надлежен да врши надзор над законитоста на преземените активности при обработката на личните податоци на територијата на Република Северна Македонија, како и заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци. ЗЗЛП појаснува дека Агенцијата е надлежна за извршување на задачите и на овластувањата доделени согласно законот. Но, не е надлежна да врши надзор над судовите кога постапуваат во рамките на нивните судски функции, освен за надзор над законитоста на преземените активности при другата обработка на лични податоци што се врши од страна на судовите согласно со законот.

4 Законот за јавното обвинителство е објавен во „Службен весник на Република Северна Македонија“, бр. 42/2020.

Но, ЗЗЛП уредува дека во однос на транспарентноста на информациите, комуникацијата и начините на остварување на правата на субјектите на личните податоци постои исклучок, односно дека со законот што се применува за контролорот или обработувачот можат да се ограничат овие права кога таквото ограничување ќе биде во согласност со суштината на основните права и слободи и претставува неопходна и пропорционална мерка со цел да се обезбеди заштита на независноста на судовите и судските постапки.

Понатаму, ЗЗЛП уредува дека кога при користење на нови технологии за некој вид обработка, според природата, обемот, контекстот и целите на обработката, постои веројатност таа да предизвика висок ризик за правата и слободите на физичките лица пред да биде извршена обработката, контролорот е должен да изврши процена на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци. Притоа, предвидува дека проценатa на влијанието врз заштитата на личните податоци се бара особено во случај на обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела.

Меѓу другото, ЗЗЛП утврдува и обврска за определување на овластено лице, односно офицер за заштита на личните податоци во случај кога обработката се врши од страна на орган на државната власт, освен за судовите кога постапуваат во рамките на нивните надлежности, но тие се должни да определат офицер за друга обработка на личните податоци што се врши согласно со законот.

ЗЗЛП утврдува и право на ефективна судска заштита за секој субјект на лични податоци, како против одлуките на Агенцијата за заштита на личните податоци, така и против конкретен контролор или обработувач, притоа не доведувајќи ги во прашање кои било достапни управни или вонсудски средства за правна заштита, вклучувајќи го и правото на поднесување барање до Агенцијата за заштита на личните податоци, тогаш кога смета дека се повредени неговите права утврдени со ЗЗЛП, како резултат на обработката на неговите лични податоци спротивно од овој закон.

Анализата на содржината на наведените норми несомнено покажува дека примарната улога во заштитата на личните податоци и приватноста ја има Агенцијата за заштита на личните податоци, но дека и таа подлежи на контрола од страна на судовите, односно се обезбедува ефективна судска заштита како против правнообврзувачката одлука на Агенцијата, така и непосредно против конкретен контролор или обработувач. Оттука, несомнено е значајна и важна улогата на судовите, но и на обвинителствата кога станува збор за заштитата на личните податоци и приватноста. Во овој контекст ќе ги разгледаме и нивните улоги во оваа област, и тоа низ две перспективи:

- Во улога на контролор согласно ЗЗЛП, каде што Агенцијата за заштита на личните податоци има надлежност да ја врши својата супервизорска функција без ограничувања; и

- Кога судовите како носители на судската власт постапуваат во рамките на нивните судски функции и согласно Уставот се целосно самостојни и независни, при што Агенцијата за заштита на личните податоци нема директни овластувања и надлежност да врши супервизија.

2. СУДОВИТЕ И ОБВИНИТЕЛСТВАТА - КОНТРОЛОРИ

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

Согласно посочените уставно-правни норми, несомнено е дека судовите и обвинителствата во Република Северна Македонија (треба да) имаат целосна независност и автономност во извршувањето на нивните функции и надлежности. Но, независноста на судовите и обвинителствата никако не треба да се разбере како можност за целосна дискреција во постапувањето во однос на информациите што во себе содржат и лични податоци. Имено, иако се независни, тие и понатаму се дел од органите на државната власт во поширока смисла на зборот. Оттука, кога станува збор за заштитата на личните податоци и за нив (судовите и обвинителствата) важат и треба да важат сите „правила на игра“ како и за другите државни органи, односно како и за сите други контролори. Впрочем, ова јасно неколкупати го нагласува и Законот за заштита на личните податоци. На пример, Законот за заштита на личните податоци утврдува дека контролорот и обработувачот се должни да определат офицер за заштита на личните податоци во секој случај кога обработката се врши од страна на орган на државната власт, освен за судовите кога постапуваат во рамките на нивните надлежности. Судовите се должни да определат офицер за другата обработка на личните податоци што се врши согласно со законот или, пак, кога Законот за заштита на личните податоци утврдува дека Агенцијата за заштита на личните податоци не е надлежна да врши надзор над судовите кога постапуваат во рамките на нивните судски функции, но дека е надлежна да врши надзор над законитоста на преземените активности при другата обработка на лични податоци што се врши од страна на судовите согласно со законот.

Оттука, почитувајќи ги независноста и самостојноста на судовите и обвинителствата и основната функција што ја имаат во спроведувањето на правото и правдата, со цел да се обезбеди дека правата на граѓаните се соодветно заштитени, како и да обезбедат спречување, откривање и сузбивање на кривичните и други казниви дела и прекршоци, главниот предизвик што го имаат тие е што сето ова треба да го спроведат во законска утврдена временска рамка со кратки рокови, ограничени ресурси што ги имаат на располагање и во услови на голем обем на работа. Притоа, треба да обезбедат и примена на соодветни технички и организациски мерки што ќе обезбедат обработка на личните податоци согласно прописите за заштита на личните податоци.

Сето ова не значи дека заради ваквата состојба и предизвиците, судовите и обвинителствата треба да имаат „посебни“ правила во постапувањето при обработката на личните податоци. Напротив, Законот за заштита на личните податоци и за нив утврдува должност за примена на соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот и сериозноста за правата и слободите на физичките лица. Имено, ако се земе предвид дека во рамките на судско-обвинителската надлежност овие органи собираат и обработуваат многу често и посебни категории на личните податоци, тогаш тие секако треба да применуваат (по)високо ниво на мерки за безбедност при собирањето, споделувањето и обработката на личните податоци, а со цел да обезбедат дека тие нема да бидат достапни или обработени од надворешни, неовластени лица. Оттука, во вакви услови, кога

судовите и обвинителствата во остварувањето на своите изворни надлежности неминовно меѓусебно комуницираат и разменуваат чувствителни информации што во себе содржат и лични податоци, земајќи го предвид притоа и недостатокот или ограничените ресурси (човечки, технички, финансиски), како главен предизвик го имаат токму следното прашање:

- како да се обезбеди ефикасно спроведување на правото и правдата, а притоа да се дизајнираат и да се применат современи технолошки достигнувања и мерки, согласно расположливоста на ресурсите за трошоците за спроведување, а имајќи ги предвид природата, обемот, контекстот и целите на обработката на личните податоци, како и ризиците со различен степен на веројатност за сериозноста врз правата и слободите на физичките лица.

Одговорот на ова прашање е комплексен и тој во себе мора да содржи повеќеслоен, скалест пристап.

Најпрвин и најмалку што може да се направи е да се обезбеди проактивна и редовна комуникација на судовите и обвинителствата со Агенцијата за заштита на личните податоци. Притоа, ова секогаш треба да биде иницирано од страна на судовите и обвинителствата, на што од стручно искуство и пример може да се потврди дека голема е веројатноста да има позитивен одговор од Агенцијата. На овој начин, преку споделување на предизвиците и непосредна комуникација со Агенцијата, има можност постојано да се зголемува свеста кај сите вработени во правосудните органи. Тоа секако ќе биде преку споделување на сопствени и меѓународни искуства од страна на Агенцијата, бидејќи таа има континуиран и практично директен, непосреден пристап до сите релевантни информации и институции од областа на заштитата на личните податоци. Секако, тука значен чекор и пример може и треба да биде спроведувањето обуки од страна на Агенцијата приспособени на потребите на судовите и јавните обвинителства. Имено, една од надлежностите на Агенцијата, согласно Законот за заштита на личните податоци, е подготвување и спроведување обуки за вработените кај контролорите, односно обработувачите, како и за офицерите за заштита на личните податоци. Притоа, овие обуки треба да се дизајнираат и да се организираат со цел офицерите, но и другите вработени (вклучувајќи ги и судиите и обвинителите), да се стекнат со знаења од областа на заштитата на личните податоци. А офицерите за заштита на личните податоци да се стекнат со знаења и вештини во однос на практиките и прописите за заштита на личните податоци и со способност да ги извршуваат работите што за нив произлегуваат согласно Законот за заштита на личните податоци. Конечно, обуки може и треба да се спроведуваат континуирано, па тие, покрај Агенцијата, можат да бидат спроведувани и во рамките на програмите на Академијата на судии и јавни обвинители. Притоа, ако се има предвид дека, согласно Законот за заштита на личните податоци, офицерот за заштита на личните податоци има законска обврска, меѓу другото, да го информира и да го советува контролорот (во случајов судовите, односно обвинителствата) и вработените кои вршат обработка соодветно на нивните обврски според одредбите од овој закон, како и дека треба директно да врши работи на подигнување на свеста и обучување на вработените кои учествуваат во операциите на обработка, тогаш секако како неопходна се јавува и потребата од обука за обучувачи на офицерите, за да можат да се оспособат со знаења и вештини за пренесување на знаењето и информациите од областа на заштитата на личните податоци. На овој начин ќе се постигне самоодржливост и предвидливост во рамките на судовите и обвинителствата, а со тоа и ниво на свест кај сите вработени кои се вклучени во операциите на обработка на личните податоци и минимизирање на ризиците од можни, несакани „протекувања“ на чувствителни информации што во себе содржат и лични податоци.

Следно што треба да се направи со цел да се обезбеди соодветна обработка на личните податоци е да се изврши мапирање на сите процеси на кои се врши обработка на личните податоци во рамките на судовите и обвинителствата. Овој процес треба да обезбеди информации за законската основа за чување и обработка на личните податоци, за рокот и причините за чување на личните податоци, категориите на лични податоци што се предмет на обработката и категориите на субјекти на личните податоци, како и податок за тоа каде, примарно, во рамките на конкретен суд или обвинителство, се чуваат и се обработуваат податоците или, пак, можеби се чуваат централизирано, а пристап имаат сите судови и обвинителства. И во овој случај, односно пример, секако Агенцијата може да помогне со своето знаење и искуство, но треба да се нагласи дека целиот процес мора да биде воден и спроведен од судовите, односно обвинителствата. Доброто мапирање на податоците е „половина завршена работа“, бидејќи овозможува да се утврди што точно се случува во однос на обработката на личните податоци во рамките на еден контролор, а и надвор од него, ако одреден процес во име на контролорот го врши обработувач, на пример во делот на ИКТ-решенијата. На овој начин ќе може да се идентификува дали, на пример, има премалку или, пак, премногу бази на податоци (што е секогаш поверојатно) за спроведување на законот, односно во врска со законот, како тие податоци се достапни во рамките на конкретен суд или обвинителство, дали се достапни само за правосудниот орган или можеби и надвор од него (на пример, на обработувач), дали се достапни на национално, државно ниво со централизиран пристап или, пак, локално во рамките на конкретен контролор, дали има контролиран пристап до базите на податоци и како се обезбедува контролираниот пристап. Сето ова е исклучително важно затоа што во практиката често се случува да имаме премногу податоци, а тие понекогаш да резултираат со премалку информации и притоа сето ова да не биде во согласност и со начелото на минимален обем на податоци утврдено со Законот за заштита на личните податоци, согласно кое личните податоци треба да бидат соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат согласно законот.

Понатаму, следен предизвик за судовите и обвинителствата е правилното (а не само проформа), спроведување анализа на ризик, која во себе најмалку што треба да опфати е:

- список (преглед) на сите процеси со кои се врши обработка на лични податоци (за кој говоревме претходно);
- процена на ризиците за секој процес на обработка на лични податоци;
- спроведување и проверка на планираните мерки; и
- спроведување на периодични безбедносни проверки.

Откако сето ова ќе се спроведе правилно, ќе може да се воспостави објективна политика за систем за заштита на личните податоци како стратешки документ за секој контролор, со утврдени начела за безбедност и заштита на личните податоци. Врз основа на тоа, понатаму ќе можат да се (ре)дизајнираат и да се донесат/дополнат подетални политики и процедури со опишани технички и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичката инфраструктура во рамките на судовите и обвинителствата. Притоа, тука треба да се нагласи потребата, но и должноста за дизајнирање и примена на техничката и интегрираната заштита на личните податоци (англ. *Data protection by design and by default*) како една од клучните мерки утврдени со Законот за заштита на личните податоци, која треба да биде применета и од страна на судовите и обвинителствата, и тоа уште во моментот на дефинирањето на средствата за обработка, како и во текот на обработката. Со ова ќе се обезбеди ефикасно спроведување на начелата за заштита

на личните податоци, како што е сведувањето на минимален обем на податоците и вклучување на потребните заштитни мерки во процесот на обработка со цел да се исполнат барањата од Законот за заштита на личните податоци и да се обезбеди заштита на правата на субјектите на личните податоци.

Што значи ова и како изгледа во практиката? – На пример: при воспоставување на нов процес или нови операции на обработка на лични податоци или нов современ начин на обработка на личните податоци, треба да се има предвид следното – дали станува збор за централизирана/децентрализирана архитектура, кои и какви средства ќе се користат за поврзување или понатамошна употреба на податоците, дали и како се обезбедува безбеден пристап до чувствителни категории на податоци, кои безбедносни технички и организациски мерки се предвидени и донесени и дали (ќе) се применуваат, дали е обезбеден пристап на физичките лица (на пример, до судските досиеја), проверки на ИТ-системите, дали и како се бришат податоците, односно уништуваат по остварување на целта, односно истекување на рокот во рамките на кој податоците биле собрани и обработувани итн. На овој начин ќе се обезбеди едновремена примена на сите начела поврзани со обработката на личните податоци, а со тоа и почитување на прописите за заштита на личните податоци.

Како да се постигне сето ова е следното (суштинско) прашање.

Краткиот одговор е преку доследно применување на начелата поврзани со обработката на личните податоци. Начелата поврзани со обработката на личните податоци утврдени со Законот за заштита на личните податоци предвидуваат дека личните податоци се:

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

Притоа, Законот за заштита на личните податоци утврдува дека контролорот, односно во случајов судовите и обвинителствата се одговорни за усогласеноста во почитувањето на начелата поврзани со обработката на личните податоци и се должни да ја демонстрираат усогласеноста (отчетноста).

За да се постигне вистинска, сеопфатна усогласеност, покрај соработката со Агенцијата за заштита на личните податоци и мапирањето на сите процеси на кои се врши обработка на личните податоци и анализата на ризик, за кои говоревме погоре, важно е сите процеси, односно операции на обработка и технички и организациски мерки да бидат соодветно документирани. На тој начин, ќе може да се демонстрира и усогласеноста, а со тоа и отчетноста од страна на судовите и обвинителствата во врска со заштитата на личните податоци, и тоа како пред Агенцијата за заштита на личните податоци, така и пред оние чии податоци се обработуваат – субјектите на личните податоци (физичките лица).

Секако, ова подразбира дека треба да се документира Политиката за систем за заштита на личните податоци како прв стратешки документ на судовите и обвинителствата, потоа мапираните процеси со преглед на процесите на кои се врши обработка на лични податоци, за да се документираат потоа сите технички и организациски мерки што се применуваат од страна на судовите и обвинителствата.

На пример:

- Дали и како се врши автентикацијата на овластените лица и како се обезбедува контролата на пристап до податоците?
- Дали има сегрегација на должности и одговорности помеѓу вработените или секој вработен може да пристапи без да се има никаква контрола?
- Дали има обезбедена евиденција за секој пристап (логови)?
- Дали се документираат активностите за обука и подигнување на свеста на раководството и вработените за приватноста, заштитата на личните податоци и безбедносните ризици во судовите и обвинителствата?

Со документирањето на процесите и донесувањето на неопходната документација за технички и организациски мерки, не завршува работата во делот на заштитата на личните податоци и приватноста. Имено, треба да се разбере дека, како што судовите и обвинителствата во остварувањето на своите надлежности континуирано вршат обработка на личните податоци, така останува континуирана и потребата од постојана работа во оваа област, и тоа, всушност, претставува главниот предизвик за сите контролори, не само за судовите и обвинителствата (случај примерен за сите контролори во Република Северна Македонија).

Дали може и како да се надмине и соодветно да се одговори на овој предизвик?

Секако дека може. Улогата на офицерот за заштита на личните податоци е исклучително значајна.

Оттука, зошто само едно лице да биде определено за офицер за заштита на лични податоци, а не повеќе? Од страна на судовите и обвинителствата треба да бидат разбрани дека се лица на кои се должни да им обезбедат поддршка при извршувањето на нивните задачи, и тоа со ресурси неопходни за извршување на тие работи и пристап до личните податоци и операциите на обработка, како и одржување на нивното стручно знаење.

Од друга страна, неопходно е офицерите континуирано да ги информираат и да ги советуваат судиите, односно јавните обвинители и другите вработени кои вршат обработка на личните податоци соодветно на нивните обврски, а во согласност со прописите за заштита на личните податоци.

Исто така, офицерот треба да ја следи усогласеноста со прописите за заштита на личните податоци, како и со политиките и документацијата усвоена од конкретниот суд или обвинителство во однос на заштитата на личните податоци.

Најмногу треба континуирано да се работи на подигнувањето на свеста и обучување на вработените кои учествуваат во операциите на обработка на личните податоци, вклучувајќи ги и судиите и јавните обвинители. Оваа улога и обврска интерно, како што веќе нагласивме, пред сè, е на офицерот за заштита на личните податоци. Но, покрај ова, треба да се искористи и улогата и надлежноста на Агенцијата за заштита на личните податоци, како и испорачувањето на редовни обуки во рамките на програмите на Академијата на судии и јавни обвинители.

Секако, тука не треба да се заборават и контролите и ревизиите што треба да се вршат внатрешно во рамките на судовите и обвинителствата, а тогаш кога супервизија ќе врши Агенцијата за заштита на личните податоци, тоа да не биде разбрано како „инспекција“, туку како истражување од Агенцијата. Истражувањето опфаќа проверка, давање насоки и превенција на судовите и обвинителствата, а со единствена цел да се обезбеди законитост на преземените активности при обработката на личните податоци и нивната заштита.

Кога наведовме дека во обезбедувањето континуитет во работењето во областа на заштитата на личните податоци улогата на офицерот за заштита на личните податоци е значајна, треба да се нагласи дека неговата/нејзината улога не е единствена. Напротив, главната одговорност ја има и останува единствено кај контролорот, односно судот или обвинителството. На пример: во прописите за заштита на личните податоци е определено дека контролорот (судовите и јавните обвинителства) во Политиката за системот за заштита на личните податоци ги утврдува и начелата за безбедност и заштита на личните податоци.

Понатаму, пропишано е дека, врз основа на Политиката за системот за заштита на личните податоци[5], контролорот донесува подетални политики и процедури во кои се опишани техничките и организациските мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичката инфраструктура, во кои особено треба да бидат опфатени:

- идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);
- општ опис на техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци соодветно на ризикот;
- активности за обука и подигнување на свеста на раководството и вработените за приватноста и безбедносните ризици во контролорот;
- дизајнирање, развивање и одржување на софтверските програми за обработка на личните податоци, а особено од аспект на техничка и интегрирана заштита на личните податоци (*Data protection by design and by default*);
- начинот на обезбедување автентикација на овластените лица во информацискиот систем;
- начинот на обезбедување контрола на пристап до информацискиот систем;

5 Политиката за системот за заштита на личните податоци како задолжителен документ е утврдена со Правилникот за безбедност на обработката на личните податоци објавен во „Службен весник на Република Северна Македонија“, бр. 122/2020.

- начинот на обезбедување евиденција за секој пристап до информацискиот систем [на пример до: оперативните системи, заштитниот ѕид (*firewall*), серверот дизајниран специјално за употреба како сервер за датотеки (*file server*), базите на податоци, системот (софтверот) за управување со документи (*DMS System*), софтверот за управување со врски со клиенти (*CRM Software*) и сл.];
- начинот на управување со инциденти (инциденти што ја нарушуваат доверливоста, интегритетот или достапноста на личните податоци);
- начинот на обезбедување на опремата на контролорот на која се врши обработка на личните податоци;
- начинот на обезбедување на преносливите медиуми;
- начинот на заштита на внатрешната мрежа на контролорот;
- начинот на обезбедување на серверите и интернет-страницата на контролорот;
- начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци;
- начинот на обработка на личните податоци што се псевдонимизирани;
- начинот на обработка на личните податоци што се криптирани;
- обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко-комуникациската опрема;
- начинот и процесите за пријавување, реакција и санирање инциденти;
- начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци;
- начинот на уништување на документите, како и за начинот на уништување, бришење и чистење на медиумите;
- физичка безбедност;
- начинот на ангажирање и контрола на надворешни субјекти (обработувачи);
- динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола; и
- други мерки што контролорот ги применува врз основа на анализата на ризикот.

Од листата на активности и мерки, јасно произлегува дека не само што тоа не е обврска единствено на офицерот за заштита на личните податоци туку објективно тој/таа и не може сам/а да ги изврши и да ги спроведе овие мерки. На контролорот (судовите и обвинителствата) е да обезбеди дека донесената документација е соодветно изменета и дополнета кога ќе се направат промени во информацискиот систем и во информатичката инфраструктура, а најмалку еднаш годишно да се изврши нејзино оценување, евалуација и ажурирање. Ова подразбира дека офицерот за заштита на личните податоци може да има еден вид координативна и контролна улога, но никако да не се разбере дека тој/таа треба сам/а да врши оценување, евалуација и ажурирање. Уште повеќе, контролорот секогаш, кога се прават промени во информацискиот систем и во информатичката инфраструктура, треба да се води од примената на техничка и интегрирана заштита на личните податоци (англ. D*ata protection by design and by default*), со што уште на почетокот „*by design*“ и „*by default*“ ќе обезбеди спроведување на

начелата за заштита на личните податоци, а со тоа особено обработка на минимален, неопходен обем на податоците со вклучување на потребните заштитни мерки во процесот на обработката. Имено, само така, преку автоматизација на процесите на обработка на личните податоци и со јасна поделба на должностите и одговорностите, ќе може да се одговори на секој предизвик со кој се соочуваат судовите и обвинителствата кога обработуваат лични податоци. За ова е потребно знаење, умеење и вештини не само кај офицерот за заштита на личните податоци туку и кај секој судија, јавен обвинител и вработен. Затоа што кога станува збор за безбедноста на личните податоци во рамките на еден систем за заштита на личните податоци, каде што повеќе лица имаат пристап и вршат обработка на личните податоци, не постои разлика во степенот на веројатност и „ранливост“ на системот во зависност од позицијата што одреден вработен ја има во рамките на внатрешното функционирање на еден контролор.

На овој начин ќе се обезбеди дека судовите и обвинителствата објективно вршат оцена и ажурирање на техничките и организациските мерки, при што секогаш ги применуваат оние мерки што се соодветни на времето во кое се дизајнираат и се имплементираат, а согласно најновите технолошки достигнувања (*a state of the art technology*). Со ова практично ќе се обезбеди постојан и реален „одговор“ на заштита на сите информации со кои располагаат судовите и јавните обвинителства, а со тоа и минимизирање на можноста од нарушување на безбедноста на личните податоци што би довело до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци што се пренесуваат, се чуваат или на друг начин се обработуваат од страна на судовите и јавните обвинителства.

3. СУДОВИТЕ И ОБВИНИТЕЛСТВАТА ВО РАМКИТЕ НА НИВНИТЕ ИЗВОРНИ ПРАВОСУДНИ ФУНКЦИИ

Откако ги елабориравме предизвиците за судовите и обвинителствата во однос на нивните обврски како контролори согласно Законот за заштита на личните податоци и на што сè тие треба да внимаваат и да применат, неминовно се наметнува потребата да се одговори и на веројатно поголемиот предизвик во однос на почитувањето и заштитата на правото на приватност и заштитата на личните податоци, тогаш кога тие ја практикуваат својата изворна надлежност, односно кога тие ја спроведуваат својата основна функција во спроведувањето на правото и правдата.

Се поставува прашањето колку и како судовите и јавните обвинителства го практикуваат правото и со својата работа даваат соодветен одговор и конкретен придонес во заштитата на правата на граѓаните во однос на приватноста и заштитата на нивните лични податоци? Согласно Законот за заштита на личните податоци, ако Агенцијата за заштита на личните податоци е надзорното тело што има статус на самостоен и независен државен орган надлежен да врши надзор над законитоста на преземените активности при обработката на личните податоци на територијата на Република Северна Македонија, како и заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци, тогаш тоа секако се и судовите и јавните обвинителства во однос на заштитата на основните права и слободи на физичките лица.

Законот за заштита на личните податоци утврдува дека Агенцијата е целосно политички, финансиски и функционално независна при извршувањето на своите надлежности, задачи и овластувања во согласност со овој закон, но исто така го утврдува и правото на ефективна судска заштита за секој субјект на лични податоци, и тоа како против одлуките на Агенцијата за заштита на личните податоци, така и против конкретен контролор или обработувач непосредно. Притоа, не доведувајќи ги во прашање кои било други достапни управни или вонсудски средства за правна заштита, вклучувајќи го и правото на поднесување на барање до Агенцијата за заштита на личните податоци, тогаш кога одредено физичко лице смета дека се повредени неговите права утврдени со Законот за заштита на личните податоци како резултат на обработката на неговите лични податоци спротивно на овој закон.

Оттука, иако примарната улога во заштитата на личните податоци и приватноста ја има Агенцијата за заштита на личните податоци, треба да се нагласи дека и Агенцијата подлежи на контрола од страна на судовите, односно се обезбедува ефективна судска заштита во однос на нејзините одлуки. Следствено, еднакво значајна и важна е улогата на судовите и на јавните обвинителства кога станува збор за заштитата на личните податоци и приватноста кога тие ги вршат своите изворни, независни надлежности, но и кога самостојно постапуваат во оваа област, целосно независно и без вклучување на Агенцијата во овој процес, како што е, на пример, кога постапуваат по одредено кривично дело или прекршок од областа на заштитата на личните податоци и приватноста.

Законот за заштита на личните податоци утврдува дека за сторен прекршок согласно овој закон, прекршочна постапка води и прекршочна санкција изрекува Агенцијата како прекршочен орган, но во овој дел важно е да се нагласи дека сите одлуки на Агенцијата се предмет на судска контрола и заштита.

Од друга страна, материјално-правно и Кривичниот законик инкриминира неколку кривични дела што директно или индиректно се однесуваат на заштитата на личните податоци и приватноста во поширока смисла на зборот. Конкретно, во член 149 од Кривичниот законик е пропишано кривичното дело „Злоупотреба на личните податоци“, а во тој член е утврдено дека:

1. Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.
2. Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета.
3. Ако делото од став 1 и 2 го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години.
4. Обидот е казнив.
5. Ако делото од овој член го стори правно лице, ќе се казни со парична казна“.

Ако се направи анализа на битието на ова кривично дело, ќе се дојде до заклучок дека член 149 од Кривичниот законик директно бара да се почитуваат начелата поврзани со обработката на личните податоци што се утврдени во Законот за заштита на личните податоци, а особено законитоста на обработката на личните податоци. Имено, кога ги образложивме начелата за заштита на личните податоци (погоре во текстот), појаснивме дека првото начело се однесува на барањето личните податоци да се обработуваат согласно со законот, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци („законитост, правичност и транспарентност“).

Притоа, во однос на законитоста на обработката на личните податоци, Законот за заштита на личните податоци во член 10 утврдува дека обработката на личните податоци е законита, само ако и до оној степен доколку е исполнет најмалку еден од следните услови:

- субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или повеќе конкретни цели,
- обработката е потребна за исполнување договор, каде што субјектот на лични податоци е договорна страна или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот,
- обработката е потребна за исполнување на законска обврска на контролорот,
- обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице,
- обработката е потребна за извршување работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон,
- обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси не преовладуваат над 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.

Оттука, имајќи ги предвид посочените норми од Законот за заштита на личните податоци во однос на начелата поврзани со обработката на личните податоци и законитоста на обработката на личните податоци, во корелација со одредбите од Кривичниот законик поврзани со кривичното дело злоупотреба на личните податоци (но, и со други кривични дела од оваа област), несомнено произлегува дека за да може еден јавен обвинител, односно судија да постапува во однос на ова кривично дело (секој во својот дел на надлежности, согласно законот), неминовно мора да го познава и практично да го применува и Законот за заштита на личните податоци. Ова значи дека и при препознавањето и квалификацијата на одредено дејство во рамките на едно кривично дело што е поврзано со заштитата на личните податоци и приватноста и во одмерувањето на видот на казната секогаш треба да се има предвид и практично разбирање во однос на тоа што го утврдува Законот за заштита на личните податоци.

Во овој контекст, ако се направи анализа на прекршочните одредби на Законот за заштита на личните податоци, ќе се утврди дека тој е „построг“ и глобите ги пропишува во паричен износ до 2% (I категорија), односно 4% (II категорија) од вкупниот годишен приход на контролорот или обработувачот-правно лице, (изразена во апсолутен износ) остварен во деловната година што ѝ претходи на годината кога е сторен прекршокот или од вкупниот приход остварен за пократок период од годината што му претходи на прекршокот, доколку во таа година правното лице почнало да работи, а за физичко лице-контролор или обработувач глобата е утврдена во паричен износ од 100 до 250 евра во денарска противвредност.

Притоа, кога станува збор за прекршоците утврдени во Законот за заштита на личните податоци во однос на казните во Кривичниот законик секогаш треба да се има предвид дека станува збор за прекршоци и прекршочна одговорност, која следствено според природата, тежината и времетраењето на повредата, земајќи ги предвид природата, обемот или целта на соодветната обработка, како и бројот на засегнати субјекти на лични податоци и степенот на нивната претрпена штета визави Кривичниот законик е сепак (би требала да биде) поблага. Но, ако се земат предвид добиените информации од досега направените анализи во делот на казните, на пример, тие покажуваат дека казните што се изрекувани досега од страна на судовите се примарно парични и многу поблаги од оние што се предвидуваат со Законот за заштита на личните податоци во однос на прекршочната одговорност. На овој начин, постои реална дискрепанција помеѓу она што за одреден прекршок како висина на глоба го изрекува (или има можност да го изрече) Агенцијата за заштита на личните податоци и она што го имаат како можност и го изрекуваат судовите. Дополнително, овде легитимно се наметнува прашањето дали судовите и јавните обвинителства имаат доволни практични познавања и искуство во препознавањето и важноста на заштитата на личните податоци и приватноста на ниво како што имаат за други видови недозволени дејства што се утврдени како такви согласно законот. Се чини дека ниту надлежните ниту физичките лица како субјекти на личните податоци целосно ги разбираат правата за заштита на личните податоци и приватноста.

Друг важен фактор е улогата на судовите кога постапуваат по тужби против одлуките на Агенцијата за заштита на личните податоци. Имено, овде станува збор за случаи кога судот би требало да има силни, сеопфатни познавања и експертиза во областа на заштитата на личните податоци, но и поширок хоризонт (во однос на Агенцијата) на обезбедување уедначена примена на правото, а со тоа и обезбедување на правна сигурност, како и генерална и специјална превенција во казнената политика. Притоа, тука треба да се имаат предвид две најчесто можни ситуации:

- Едната, кога физичко(и) лице(а) – субјект на личните податоци има право на ефективна судска заштита против правнообврзувачката одлука на Агенцијата што се однесува на него;
- Другата, кога контролор или обработувач ќе бара ефективна судска заштита против правнообврзувачката одлука на Агенцијата што се однесува на тој контролор, односно обработувач.

Во првиот случај станува збор најчесто за ситуација каде што Агенцијата постапува по повод поднесено барање од страна на субјект на лични податоци против одреден контролор или обработувач за кој сметал дека со обработката на неговите лични податоци ги прекршува одредбите од Законот за заштита на личните податоци и каде што Агенцијата спроведува супервизија и донесува решение со кое субјектот на личните податоци не е задоволен (најчесто кога неговото барање е одбиено).

За разлика од првиот, вториот случај, најчесто е ситуација каде што Агенцијата, во рамките на спроведувањето на супервизијата, над заштитата на личните податоци во однос на законитоста на преземените активности при обработката на личните податоци и нивната заштита донела решение со кое утврдила повреда и корективни мерки за отстранување на утврдените повреди или, пак, во рамките на прекршочната надлежност е утврдена и изречена глоба (независно дали е по повод барање субјект на лични податоци или *ex officio*).

За првиот случај, Агенцијата на одреден начин претставува еден вид суд *sui generis*. Имено, во постапката во овој случај има две страни, и тоа субјектот на личните податоци како барател и контролорот/обработувачот против кого е поднесено барањето. Во ваков случај, Агенцијата по спроведената супервизија и утврдената фактичка состојба го применува материјалниот закон и донесува решение со кое мериторно одлучува, а со кое субјектот на личните податоци не е задоволен – најчесто кога неговото барање е одбиено и не е утврдена повреда на заштитата на неговите лични податоци. Против таквата одлука на Агенцијата, законот обезбедува судска заштита и доколку субјектот одлучи, тогаш поднесува тужба до надлежниот суд. Ако се направи анализа на годишните извештаи на Агенцијата за заштита на личните податоци за изминатите години, ќе се заклучи дека во најголем број од случаите (повеќе од 90%) одлуките на Агенцијата се потврдени од страна на надлежните судови. Ова е показател и на одреден начин признание дека Агенцијата за заштита на личните податоци ја остварува својата надлежност во согласност со Законот за заштита на личните податоци. Но, ова може да биде индикатор и показател дека судовите во практикувањето на својата надлежност се разликуваат со она на Агенцијата, особено ако ова како податок се стави во корелација со предвидените и изречените глоби од страна на Агенцијата визави предвидените и изречените казни од страна на судовите (и како број и како вид и висина).

И во втората ситуација каде што Агенцијата во рамките на спроведувањето на супервизијата донесува решение со кое утврдува повреди и корективни мерки за отстранување на утврдените повреди или, пак, во рамките на прекршочната постапка е утврдена и изречена глоба за контролор или обработувач, кој поради ова бара ефективна судска заштита. Во најголем број случаи, одлуките на Агенцијата се потврдени, но иако ретко, има и случаи каде што судовите ги уважуваат аргументите на контролорите, со многу „штуро“ образложение.

Но, помалку значајна е и дадената можност со Законот за заштита на личните податоци секој субјект на лични податоци да има право на непосредна ефективна судска заштита, независно од Агенцијата за заштита на личните податоци, кога смета дека се повредени неговите права утврдени со овој закон, како резултат на обработката на неговите лични податоци спротивно од овој закон. Со ова законско решение, Законот за заштита на личните податоци практично дава можност за избор за субјектот на личните податоци да може да се определи дали ќе поднесе барање за заштита на личните податоци до Агенцијата за заштита на личните податоци или, пак, тоа ќе го стори со иницирање на судска постапка непосредно до надлежен суд, без вклучување на Агенцијата. Во ваков случај, судот, за разлика од Агенцијата, води судска постапка согласно законот, наместо постапка за супервизија и врз основа на утврдената фактичка состојба треба да донесе одлука согласно законот.

Сето ова покажува дека улогата на судовите и јавните обвинителства во заштитата на личните податоци и приватноста е исклучително важна, но и дека во реализацијата на заштитата на овие права, особено во денешниот, модерен, современ начин на живеење, сето ова за судовите и јавните обвинителства (впрочем, како и за сите) претставува сериозен предизвик.

Имено, од нив се бара да применат соодветни технички и организациски мерки, за да обезбедат ниво на безбедност на личните податоци со кои располагаат. А соодветно на ризикот и според најновите технолошки достигнувања, природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозност за правата и слободите на физичките лица, што бара познавање не само на правото туку сè повеќе и на технологијата, за да може да се одговори на новото време, и кога се јавуваат како контролори, а и кога ги практикуваат своите изворни надлежности и функции согласно Уставот и законите.

ЗАКЛУЧНИ СОГЛЕДУВАЊА И ПРЕПОРАКИ

Сигурноста и тајноста на личните податоци, како и почитувањето и заштитата на приватноста на граѓаните на Република Северна Македонија се слободи и права што се гарантираат со Уставот на Република Северна Македонија.

Агенцијата за заштита на личните податоци е главниот промотор и заштитник на овие права, но имајќи предвид дека станува збор, пред сè, за уставно-гарантирани човекови права и слободи, нивната заштита, покрај Агенцијата, во значителна мера и најмалку еднакво, зависи и од судовите и јавните обвинителства во Република Северна Македонија. Оттука, решенијата што ги овозможува новото модерно време во контекст на обработката и заштитата на личните податоци и приватноста, со примената на современи технолошки достигнувања се предизвик и за судовите и за јавните обвинителства. Сето ова бара познавање не само на правото туку и сè повеќе разбирање на новите технолошки решенија, како и свест за ризиците што постојат при обработката на личните податоци. Оттука, нужно се јавува потребата судиите и јавните обвинители (правниците) сè повеќе да бидат и „информатичари“. Впрочем, неслучајно денес во Европа и светот во оваа област сè повеќе се зборува за нова професија, модерно, иако сè уште неформално, наречена „*IT Lawyer*“, односно „правник-информатичар“.

Но, со ваквиот брз технолошки развој насочен кон забрзување на општествениот и економскиот развој, никогаш не треба да се дозволи со постигнувањето на оваа цел да се предизвика повреда или ограничување на човековите права и слободи.

Република Северна Македонија, како земја што сака да биде дел од европското семејство, во духот на европските вредности треба да обезбеди примена на информатичко-комуникациските технологии на начин што ќе обезбеди дека нема да бидеме „принудени“ да избираме помеѓу ефикасниот и ефективен развој од една страна и заштитата на личните податоци и правото на приватност како основни човекови права и слободи од другата страна, бидејќи објективно можат да се постигнат и двете.

Во таа насока, предизвикот за судовите и обвинителствата во Македонија секако е да го постигнат токму ова, односно кога постапуваат во рамките на нивните судски и обвинителски функции и надлежности да обезбедат баланс меѓу почитувањето и заштитата на личните податоци и правото на приватност од една страна, визави современиот технолошки, информатичко-комуникациски развој, од друга страна. Во таа насока, улогата на судовите и јавните обвинителства во системот на заштита на лични податоци и приватноста е исклучително многу значајна и претставува предизвик на кој тие мораат да одговорат соодветно.

Анализата покажува дека за надминување на сите овие предизвици треба да се преземат соодветно чекори веднаш, а амбицијата на овој документ е да даде преглед и приоритет во однос на овие предизвици. Во овој контекст се и следните препораки за надминување на предизвиците, а кои веќе се идентификувани погоре во текстот на документот.

» ВКЛУЧУВАЊЕ НА АЗЛП ВО ЦЕЛИОТ ПРОЦЕС

Обезбедување проактивна и редовна комуникација на судовите и јавните обвинителства со Агенцијата за заштита на личните податоци. Притоа, иницијативата секогаш треба да биде од страна на судовите и обвинителствата со споделување на предизвиците и непосредна комуникација со Агенцијата. На овој начин ќе се обезбеди континуирано зголемување на свеста кај сите вработени во правосудните органи. Тоа секако ќе биде преку споделување на сопствени и меѓународни искуства од страна на Агенцијата со сите релевантни информации од областа на заштитата на личните податоци.

» ОБУКИ

Значаен чекор треба да биде и спроведувањето обуки од страна на Агенцијата за заштита на личните податоци приспособени на потребите на судовите и јавните обвинителства. Ако се има предвид дека една од надлежностите на Агенцијата согласно Законот за заштита на личните податоци е подготвување и спроведување обуки за вработените во контролорите, односно обработувачите, како и за офицерите за заштита на личните податоци, тогаш зошто ова да не биде искористено од страна на судовите и обвинителствата и да стане редовна практика. Впрочем, ваков пристап веќе имаат дел од органите на државната управа. Притоа, предноста ќе биде што овие обуки треба да се дизајнираат и да се организираат со цел офицерите за заштита на личните податоци, но и другите вработени, вклучувајќи ги и судиите и обвинителите, да се стекнат со знаења од областа на заштитата на личните податоци. Офицерите, пак, за заштита на личните податоци да се стекнат со знаења и вештини во однос на практиките и прописите за заштита на личните податоци и со способност да ги извршуваат работите што за нив произлегуваат согласно Законот за заштита на личните податоци.

Обуки може и треба да се спроведуваат континуирано, и од страна на Агенцијата и во рамките на програмите на Академијата на судии и јавни обвинители. Ако се има предвид дека согласно Законот за заштита на личните податоци офицерот за заштита на личните податоци има законска обврска да ги информира и да ги советува контролорот или обработувачот и вработените кои вршат обработка соодветно на нивните обврски според одредбите од овој закон и директно треба да врши работи на подигнување на свеста и обучување на вработените кои учествуваат во операциите на обработка, тогаш секако како неопходна се јавува и потребата од обука за обучувачи на офицерите, за да можат да се оспособат со знаења и вештини за пренесување на знаењето и информациите од областа на заштитата на личните податоци. На овој начин ќе се постигне самоодржливост и предвидливост во рамките на судовите и обвинителствата, а со тоа и ниво на свест кај сите вработени кои се вклучени во операциите на обработка на личните податоци и минимизирање на ризиците од можни, несакани „протекувања“ на чувствителни информации што во себе содржат и лични податоци.

Обуките треба да се дизајнираат и во однос на судиите и обвинителите кога тие постапуваат во рамките на нивните изворни надлежности. Имено, обезбедувањето на заштитата на овие уставно-гарантирани права и слободи од страна на судовите и јавните обвинителства ќе може целосно да се постигне само ако тие имаат докрај познавања и целосно разбирање на овие права и, следствено, како нивното загрозување може да влијае и врз загрозување на другите исто така уставно-гарантирани права и слободи. Оттука, обуки во овој сегмент, освен преку Агенцијата за заштита на личните податоци, треба особено преку курикулумите на Академијата на судии и јавни обвинители

да се воспостават на редовна основа со цел судиите и обвинителите да се стекнуваат со знаења, умеења и вештини соодветни на модерното современо време на обработка на личните податоци. Тука секако можат да се користат и експертските капацитети обезбедени преку домашна и/или меѓународна поддршка.

» МАПИРАЊЕ И УТВРДУВАЊЕ НА ПРОЦЕСИТЕ НА ОБРАБОТКА

Со цел да се обезбеди соодветна заштита при обработката на личните податоци, неопходно е да се изврши мапирање, односно утврдување на сите процеси на кои се врши обработка на личните податоци во рамките на судовите и обвинителствата. Овој чекор ќе обезбеди информации за законската основа за чување и обработка на личните податоци, за рокот и причините за чување на личните податоци, категориите на лични податоци што се предмет на обработката и категориите на субјекти на личните податоци, како и податок за тоа каде примарно во рамките на конкретен суд или обвинителство се чуваат и се обработуваат податоците. Тука треба да се искористат и знаењата на Агенцијата што може да помогне со споделување на своите искуства, но уште еднаш ќе нагласиме дека целиот процес мора да биди воден и завршен од судовите, односно обвинителствата. Овој чекор е значаен затоа што ќе обезбеди почитување на начелата поврзани со обработката на личните податоци, особено на начелото на минимален обем на податоци согласно кое личните податоци треба да бидат соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат.

» УПРАВУВАЊЕ СО РИЗИКОТ

Значаен чекор за судовите и обвинителствата е да спроведат анализа на ризик, за која зборевме погоре во текстот, а која треба да опфати:

- список (преглед) на сите процеси со кои се врши обработка на лични податоци (за кој говоревме претходно);
- процена на ризиците за секој процес на обработка на лични податоци;
- спроведување и проверка на планираните мерки; и
- спроведување на периодични безбедносни проверки.

» ДОКУМЕНТИРАЊЕ НА СИТЕ ПРОЦЕСИ И МЕРКИ

Откако ќе се изврши мапирање на процесите и анализа на ризикот, треба да се документираат сите политики и процедури за заштита на личните податоци со опишани технички и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичката инфраструктура во рамките на судовите и обвинителствата. Ова подразбира дека треба да се документира Политиката за систем за заштита на личните податоци како прв стратешки документ на судовите и обвинителствата, потоа секако мапираните процеси со преглед на процесите на кои се врши обработка на лични податоци, за да се документираат сите технички и организациски мерки што се применуваат од страна на судовите и обвинителствата.

» ОЦЕНУВАЊЕ, ЕВАЛУАЦИЈА И АЖУРИРАЊЕ НА ДОНЕСЕНАТА ДОКУМЕНТАЦИЈА И ПРОЦЕСИТЕ

Со документирањето на процесите и донесувањето на неопходната документација за технички и организациски мерки не завршува работата во делот на заштитата на личните податоци и приватноста. Како што судовите и обвинителствата во остварувањето на своите надлежности континуирано вршат обработка на личните податоци, така останува континуирана и потребата од постојана работа во оваа област. Ова е главниот предизвик за сите контролори, па тука е исклучително важна улогата на офицерот за заштита на личните податоци. Ова подразбира дека офицерот може да има еден вид координативна и контролна улога, но никако да не се разбере дека треба сам да врши оценување, евалуација и ажурирање на документацијата. Уште повеќе, секогаш кога судовите и обвинителствата прават промени во информацискиот систем и информатичката инфраструктура треба да се водат од примената на техничка и интегрирана заштита на личните податоци (англ. *Data protection by design and by default*), со што уште на почетокот „*by design*“ и „*by default*“ ќе обезбедат спроведување на начелата за заштита на личните податоци. За ова е потребно знаење, умеење и вештини не само кај офицерот за заштита на личните податоци туку и кај секој судија, јавен обвинител и вработен. Затоа што, кога станува збор за безбедноста на личните податоци во рамките на еден систем за заштита на личните податоци, каде што повеќе лица имаат пристап и вршат обработка на личните податоци, не постои разлика во степенот на веројатност и „ранливоста“ на системот во зависност од позицијата што одреден вработен ја има во рамките на еден контролор.

На овој начин ќе се обезбеди дека судовите и обвинителствата објективно вршат оцена и ажурирање на техничките и организациските мерки, при што секогаш ги применуваат оние мерки што се соодветни на времето во кое се дизајнираат и се имплементираат, а согласно најновите технолошки достигнувања (*a state of the art technology*). Со ова практично ќе се обезбеди постојан и реален „одговор“ на заштита на сите информации со кои располагаат судовите и јавните обвинителства, а со тоа и минимизирање на можноста од нарушување на безбедноста на личните податоци што би довело до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци што се пренесуваат, чуваат или на друг начин се обработуваат од страна на судовите и јавните обвинителства.