Влијанието на Законот за заштита на личните податоци во работата на организациите од граѓанскиот сектор

Септември, 2020 година

Наслов на публикацијата
Влијанието на Законот за заштита на личните податоци во работата на организациите од граѓанскиот сектор

Автори
Мануела Станоевска Стоилковска
Арбен Гудачи
Игор Кузевски

Издавач
Македонско здружение на млади правници
www.myla.org.mk
Септември, 2020

Уредник
Зоран Дранговски

Ликовно и графичко обликување:
Винсент Графика - Скопје

Тираж:
150 примероци
Бесплатен/некомерцијален тираж

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

342.738:340.13]:061.2(497.7)(047.31)

СТАНОЕВСКА Стоилковска, Мануела
Влијанието на Законот за заштита на личните податоци во работата на организациите од граѓанскиот сектор / [Мануела Станоевска Стоилковска, Арбен Гудачи, Игор Кузевски]. - Скопје : Македонско здружение на млади правници, 2020. - 166 стр. ; 21 см

ISBN 978-608-4843-32-0

1. Гудачи, Арбен [автор] 2. Кузевски, Игор [автор]
а) Заштита на лични податоци -- Законска регулатива -- Влијание -- Невладини организации -- Македонија -- Истражувања

COBISS.MK-ID 52053765

СОДРЖИНА

I. ВОВЕД

ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (влијание врз работата на невладините организации)

Едно од основните слободи и права на човекот и граѓанинот уредено со Уставот на Република Северна Македонија е сигурноста и тајноста на личните податоци и гаранцијата за заштита од повреда на личниот интегритет што произлегува од нивното регистрирање и обработка (член 18 од Уставот). Треба да се истакне дека и покрај фактот што овие права се гарантираат со Уставот уште од 1991 година, заштитата на личните податоци реално започнува со донесувањето и примената на Законот за заштита на личните податоци од 2005 година. Овој Закон ја уредуваше и гарантираше заштитата на личните податоци се до февруари 2020 година, кога беше донесен и стапи во сила нов Закон за заштита на личните податоци[1]. Новиот Закон е резултат на потребата од уредување на обработката на личните податоци во новото модерно време која сè повеќе се врши на автоматизиран начин vis-à-vis традиционалниот начин на обработка. Притоа, треба да се истакне дека во рамки на Советот на Европа е завршена постапката за модернизација на постојната Конвенција за заштита на физичките лица која се однесува на автоматската обработка на личните податоци[2], а во рамки на Европската унија е донесена Општата регулатива за заштита на личните податоци (GDPR)[3].

Имајќи ги предвид новите предизвици во однос на заштитата на основните човекови права и слободи, конкретно на правото на приватност и заштитата на личните податоци, како и зголемената употреба на новите информациско/информатички технологии и глобализацијата во однос на обработката на личните податоци, со новиот Закон за заштита на личните податоци покрај постојните, се воведуваат и цела лепеза на нови решенија. Преку нивното почитување и примена се обезбедува заштитата на личните податоци при нивната обработка која ќе биде соодветна на ризиците кои постојат во „новото“ време.
Невладините организации како значаен чинител во општеството, при своето работење обработуваат цел сет на лични податоци за најразлични категории на субјекти на лични податоци. Размената

[1] Законот за заштита на личните податоци е објавен во „Службен весник на Република Македонија“ бр.42/2020
[2] Протокол за изменување и дополнување на Конвенцијата за заштита на физичките лица која се однесува на автоматската обработка на личните податоци (CETS No 223) е потпишан од РС Македонија во декември 2019 година и сега е во постапка за ратификација
[3] Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот за заштита на физичките лица во однос на обработката на личните податоци и слободното движење на овие податоци и за укинување на Директивата 95/46/ЕЗ

на личните податоци со релевантните заинтересирани страни е битен фактор за навремена реакција и во голема мера може да придонесе за остварување на правата на субјектите на лични податоци во конкретен случај. Од друга страна, прекумерната и неовластена обработка на личните податоци претставува повреда на правото на приватност и правото на заштита на лични податоци, а понекогаш откривањето на податоци на неовластени лица може посредно да доведе до загрозување и на други човекови права. Личните податоци и менаџирањето со истите, се важна алатка при остварувањето на функцијата на невладините организации. Неспорна е потребата од обработка на личните податоци заради остварување на дејностите заради кои се основани невладините организациии, но поседувањето на информацијата само по себе може да претставува моќ која наметнува прашања: зошто, каде, кој, во која мера и како истата треба да се искористи?

Целта на оваа анализа е од практичен аспект да ги објасни новините во Законот за заштита на личните податоци, како тие влијаат врз работата на невладините организации, а воедно да се одговори и на прашањето како невладините организации да обезбедат тајност и заштита при обработката на личните податоци, имајќи ги предвид категориите на лица со кои се среќаваат во своето секојдневно работење, а чии податоци се упатени да ги обработуваат.

Кога говориме за новиот Закон за заштита на личните податоци, се поставува прашањето зошто се донесе нов закон. Причините за донесување на Законот се пред се за да го „признае“ фактот дека обработката на лични податоци сè повеќе се врши на автоматизиран начин (иако Законот не го „заборава“ и традиционалниот начин на обработка), за да крајната цел на Законот биде, уредување на начинот, методите и постапките на обработка на личните податоци на начин кој согласно новото време ќе обезбеди почитување и заштита на личните податоци, а во тој контекст пошироко гледано и на приватноста на оние чии податоци се обработуваат – субјектите на личните податоци.
Преку анализата ќе се објасни што сè треба да применуваат невладините организации кога обработуваат лични податоци, како би обезбедиле законитост, транспарентност и отчетност во своето работење при нивна обработка.

I.1 Методологија

Анализата на Законот за заштита на личните податоци и неговото влијание во работата на невладиниот сектор има за цел да го утврди влијанието на Законот во секојдневното работење на невладиниот сектор, имајќи ги предвид спецификите кои ги има овој сектор. Анализата детално ги обработува членовите на Законот, како и подзаконските акти, правните мислења издадени од Агенцијата за заштита на личните податоци, како и најдобрите практики во работењето на Агенцијата за заштита на личните податоци и невладините организации. Исто така, анализата ги опфаќа и меѓународните документи, особено европската легислатива за заштита на личните податоци. Авторите на анализата се правни експерти со долгогодишно искуство во областа на заштитата на личните податоци.
Од страна на авторите на анализата беа користени примарни и секундарни извори, при што примарните податоци беа собирани преку:

- Барања за слободен пристап до информации од јавен карактер поднесени до Агенцијата за заштита на личните податоци. Од Агенцијата како единствен надлежен орган за заштита на обработката на личните податоци се побарани информации за актуелната состојба на регистрирани контролори и офицери за заштита на личните податоци во нашата земја;
- Анонимен прашалник, кој електронски е поднесен до 139 невладини организации во нашата земја. Прашалникот електронски е пополнет од 21 организација и резултатите од истото се презентирани подолу во анализата.

Секундарните извори користени од страна на авторите се:

- Законот за заштита на личните податоци,
- Правилник за известување за обработка на лични податоци со висок ризик,
- Општата Регулатива за заштита на личните податци (GDPR)

Во однос на користење на претходни анализи и истражувања на оваа тема не беше возможна бидејќи оваа е прва анализа од ваков вид, кој на ваков детален начин го анализира законот и подзаконските акти.

Анализата исто така дава препораки за полесно имплементирање на Законот како и соодветна листа за проверка на усогласеноста на работењето на оганизациите со законските прописи. Истата има за цел да послужи на секоја организација да изврши проверка на тоа дали нејзиното работење е усогласено со Законот и доколку не е, кои чекори треба да ги преземе.

II. ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Што е ново во Законот за заштита на личните податоци vis-à-vis претходниот закон?

Законот за заштита на личните податоци од 2005 година[4], ја „одигра“ својата улога во времето во кое беше донесен и се применуваше, и со него, практично се поставија темелите на заштитата на личните податоци во Република Северна Македонија.

Напредокот на техничко-технолошките решенија и сè помасовната обработка на личните податоци на автоматизиран начин, доведоа до тоа Законот за заштита на личните податоци од 2005 година, сè повеќе да „заостанува“ во однос на начинот на уредувањето на техничките и организациските мерки за обезбедување тајност и заштита на личните податоци при нивната обработка, но и во однос на принципите со кои би се обезбедила безбедност на личните податоци соодветна на ризикот при нивната обработка кој ќе биде адекватен на „новото дигитално доба“. Токму од овие причини, Европскиот парламент и Советот на Европската унија на 27 април 2016 година ја донесоа Регулативата (ЕУ) 2016/679 за заштита на физичките лица во однос на обработката на личните податоци и движењето на таквите податоци со што се укина Директивата 95/46/ЕК (Директивата 95/46/ЕК е актот кој беше преточен во Законот за заштита на личните податоци од 2005 година). Со ова практично започнаа реформските процеси во областа на заштитата на личните податоци, при што Регулативата имаше транзиционен период од две години, па истата во Европската Унија започна да се применува од 25 мај 2018 година. Оваа Регулатива, позната кај нас како GDPR, е веќе соодветно транспонирана и во Република Северна Македонија со донесувањето на новиот Закон за заштита на личните податоци кој започна да се применува од 24 февруари, 2020 година.

Имајќи го предвид ова, во продолжение на анализата ќе дадеме појаснување на најзначајните новини во Законот за заштита на личните податоци vis-à-vis претходниот закон и како тие влијаат врз работењето на невладините организации.

[4] Законот за заштита на личните податоци кој беше донесен во 2005 година, со сите свои измени и дополнување е објавен во „Службен весник на Република Македнонија“ бр. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14, 153/15, 99/16 и 64/18).

Со новиот Закон за заштита на личните податоци се воведуваат повеќе нови (покрај досегашните) поими, од кои како позначајни во врска со работењето на невладините организации ќе ги издвоиме следните:

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

„Профилирање“ е секоја форма на автоматска обработка на лични податоци, која се состои од користење на лични податоци за оценување на одредени лични аспекти поврзани со физичкото лице, а особено за анализа или предвидување на аспекти кои се однесуваат на извршување на професионалните обврски на тоа физичко лице, неговата економска состојба, здравје, лични преференции, интереси, доверливост, однесување, локација или движење.

„Псевдонимизација“ е обработка на личните податоци на таков начин што личните податоци не можат повеќе да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува.

„Согласност“ на субјектот на лични податоци е секоја слободно дадена, конкретна, информирана и недвосмислена изјавена волја на субјектот на личните податоци, преку изјава или јасно потврдено дејствие, а со кои се изразува согласност за обработка на неговите лични податоци.

„Посебни категории на лични податоци“ се лични податоци кои откриваат 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.

„Генетски податоци“ се лични податоци поврзани со генетските карактеристики на физичкото лице кои се наследени или стекнати, а кои откриваат единствена информација за неговата физиологија или здравје, која особено се добива со анализа на биолошки примерок од тоа физичко лице.

„Биометриски податоци“ се лични податоци кои се добиваат преку специфична техничка обработка на физичките и физиолошките карактеристики на физичкото лице или карактеристики на неговото однесување, а преку кои се овозможува или потврдува единствената идентификација на физичкото лице.

“Податоци што се однесуваат на здравјето на луѓето“ се лични податоци поврзани со физичкото или менталното здравје на физичкото лице, вклучувајќи и податоци за добиената здравствена заштита кои откриваат информации за неговото здравје.

Покрај новите дефинции, со Законот за заштита на личните податоци се воведуваат и нови принципи (покрај постојните) и генерално се воведува нов концепт при обработката на личните податоци. Имено, она што претставува квантен скок во врска со „правилата на игра“ кај оние кои обработуваат лични податоци, па и во однос на невладините организации е принципот на отчетност. Согласно овој принцип, покрај тоа што контролорот е одговорен за усогласеноста со принципите и генерално со прописите за заштита на личните податоци при нивната обработка (тоа постоеше и со претходниот закон), сега е должен таквата усогласеност и да ја демонстрира. Со новиот Закон постои таканаречената правило дека „работите ги правам не само затоа што морам (номотехничка усогласеност), туку и затоа што сакам (јасна, видлива и разбирлива усогласеност)“. Притоа, во Законот се дадени јасни решенија кога и како тоа треба да се направи. Имено, Законот како постапки и процедури преку кои контролорот може да ја докаже, односно демонстрира

усогласеноста на своето работење со прописите за заштита на личните податоци, а што претставува новина која (ќе) влијае врз работата и на невладините организации, ги предвидува следните елементи:

- Демонстрирање на примената на технички и организациски мерки со кои се обезбедува ниво на безбедност соодветно на ризикот вклучувајќи ги тука и техничката и интегрирана заштита на личните податоци;
- Соодветни политики за заштита на личните податоци;
- Развој и почитување на одобрените кодекси на однесување;
- Почитување на одобрените механизми за сертификација;
- Документирање на сите нарушувања на безбедноста на личните податоци;
- Проценка на влијанието на заштитата на личните податоци; и
- Определувањето и положбата на офицерот за заштита на личните податоци.

Во однос на примената на техничките и организациските мерки, новина е тоа што сега тие се дизајнираат и имплементираат според повеќе критериуми имајќи ги притоа предвид особено природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица. Дополнително, тие се дизајнираат и имплементираат согласно најновите технолошки достигнувања (*a state-of-the-art technology*), што како обврска бара техничките и организациските мерки секогаш да се преиспитуваат и ажурираат, на начин кој ќе биде соодветен на времето во кое се дизајнираат и имплементираат. Такви мерки во овој момент, а кои Законот дури и експлицитно ги наведува се псевдонимизацијата и криптирањето на личните податоци, способноста за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка на личните податоци, или пак на пример способноста за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент.

Во овој контекст, а согласно „state-of-the-art-technology“ пристапот, новина претставува и техничката и интегрирана заштита на личните податоци (*data protection by design and by*

default). Согласно оваа мерка, контролорот ги има следните обврски:

- во моментот на дефинирање на средствата за обработка, како и во моментот на самата обработка, да примени, односно применува соодветни технички и организациски мерки со кои ќе се обезбеди ефикасно спроведување на начелата за заштита на личните податоци, како што се на пример псевдонимизацијата и сведувањето на минимален обем на податоците (data minimization); и
- да ги примени сите потребни заштитни мерки во процесот на обработката, со цел да се исполнат условите за законита обработка на личните податоци, а воедно да се обезбеди заштита на правата на субјектите на личните податоци.

Согласно оваа мерка, контролорот треба да ги примени сите технички и организациски мерки со кои се обезбедува интегрирано (by default), односно на ниво на целиот информациски систем на контролорот, дека се обработуваат само оние лични податоци кои се неопходни за секоја посебна цел на обработката. Оваа обврска се однесува на количеството на собрани лични податоци, опсегот на нивната обработка, рокот на чување и нивната достапност. Воедно, оваа мерка треба да обезбеди дека интегрираните лични податоци без индивидуална интервенција нема да можат да бидат автоматски достапни за неограничен број на физички лица.

Во однос на проценката на влијанието на заштитата на личните податоци (*Data Protection Impact Assessment*), која исто така претставува значајна новина vis-à-vis претходниот закон, ќе напоменеме дека согласно оваа мерка, Законот бара секогаш кога при користење на нови технологии за некој вид на обработка на личните податоци, земајќи ги предвид природата, обемот, контекстот и целите на обработката, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица. Затоа, пред да биде извршена обработката, контролорот треба да изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци. Притоа, Законот утврдува дека проценката треба да се врши во случај на:

- систематска и сеопфатна оценка на личните аспекти кои се поврзани со физички лица, која се заснова на автоматска обработка, вклучувајќи и профилирање, а врз основа на која

се донесуваат одлуки кои произведуваат правно дејство во врска со физичкото лице или значително влијаат на физичкото лице,

- во случај на обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела; или
- во случај на систематско набљудување на јавно достапни простори во големи размери.

Дополнително, Агенцијата за заштита на личните податоци има обврска да воспостави и јавно да објави листа на видовите на операции на обработка[5], за кои се бара проценка на влијанието на заштитата на личните податоци.

Оваа контролна мерка има за цел секогаш кога се воведуваат и користат нови технологии и технолошки решенија при обработката на личните податоци, задолжително претходно да се изврши проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци.

Значајна улога во правилната примена на проценката на влијанието на заштитата на личните податоци, Законот предвидел и за Агенцијата за заштита на личните податоци. Имено, контролорот секогаш ќе треба да се консултира со Агенцијата пред обработката, ако резултатите од проценката на влијанието на заштитата на личните податоци покажат дека, доколку контролорот не преземе мерки за ублажување на ризикот, тогаш обработката ќе предизвика висок ризик. Притоа, кога Агенцијата смета дека планираната обработка го прекршува Законот за заштита на личните податоци, особено кога контролорот не го идентификувал или намалил ризикот во доволна мера, му дава мислење на контролорот или обработувачот, при што може да користи и кое било од своите со закон утврдени овластувања.

Обврската за определување на офицер за заштита на личните податоци[6] не е новина во нашата држава, од причина што за разлика од голем број европски држави оваа обврска во нашето законодавство беше воведена во 2010 година со измена

[5] Листата на видовите операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци е објавена во „Службен весник на Република Северна Македонија“ бр.122/20

[6] Законот за заштита на личните податоци утврдува дека офицер за заштита на личните податоци е овластено лице за заштита на личните податоци определено од контролорот и обработувачот во случаи утврдени со член 41 од Законот

на претходниот Закон за заштита на личните податоци. Но, со донесувањето на новиот Закон за заштита на личните податоци во однос на досегашните решенија утврдени со претходниот закон, дополнително ја зајакнува улогата на офицерот. Имено, контролорот и обработувачот треба секогаш да определат офицер за заштита на личните податоци кога:

- обработката се врши од страна на органите на државната власт;
- основните активности на контролорот или обработувачот се состојат од операции за обработка, кои поради својата природа, опсег и/или цели, бараат во голема мера редовно и систематско следење на субјектите на лични податоци; или
- основните активности на контролорот или обработувачот се состојат од обемна обработка на посебни категории на лични податоци или лични податоци поврзани со казнени осуди и казнени дела.

Имајќи ги предви овие специфики, како и несомнениот факт дека лицето кое е определено да ја врши должноста на офицер за заштита на личните податоци ќе треба да има соодветни теоретски и практични познавања од областа на заштитата на личните податоци, новина која што се воведува со Законот е можноста група на правни лица да можат да определат еден офицер за заштита на личните податоци, под услов офицерот да биде лесно достапен за секое правно лице.
Дополнителна новина е должноста контролорот или обработувачот или здруженија и други тела што ги претставуваат категориите на контролори или обработувачи, исто така да определат офицер за заштита на личните податоци, кој може да ги извршува задачите за тоа здружение или друго тело кое ги претставува контролорите и обработувачите.
Законот понатаму бара офицерот за заштита на личните податоци да се определи врз основа на неговите стручни квалификации, а особено врз основа на неговите стручни знаења за легислативата и практиките во областа на заштитата на личните податоци. Притоа лицето кое е определено за офицер за заштита на личните податоци, треба да биде способно да ги извршува најмалку следните работи:

- да ги информира и советува контролорот или обработувачот и вработените кои вршат обработка соодветно на нивните

обврски според одредбите од Законот за заштита на личните податоци;

- да ја следи усогласеноста со овој закон, со други засегнати закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките на контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распределување на одговорности, подигнување на свеста и обучување на вработените кои што учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци;
- да дава совети во однос на проценката на влијанието на заштитата на личните податоци и следење на извршувањето на проценката;
- редовно да соработува со Агенцијата за заштита на личните податоци;
- да дејствува како контакт точка за Агенцијата за заштита на личните податоци во однос на прашањата поврзани со обработката, вклучувајќи ја и претходната консултација во врска со проценката на влијанието на приватноста заради преземање на мерки за ублажување на ризикот од страна на контролорот, како и советување според потребите за сите други прашања.

Офицерот за заштита на личните податоци и согласно новиот Закон може да биде вработен кај контролорот или обработувачот. Она што е новина, е можноста офицерот за заштита на личните податоци да ги извршува работите врз основа на договор за услуги, односно да биде лице кое не е вработено кај контролорот или обработувачот.

Со цел да се обезбеди дека офицерот, било внатрешен или надворешен, е достапен, важно е да се обезбеди дека неговите податоци за контакт се достапни во согласност со барањата на законот. Офицерот самостојно или со помош на тим, мора да биде во можност секогаш кога е потребно ефикасно да комуницира со субјектите на лични податоци и да соработува со Агенцијата за заштита на личните податоци. Обезбедување на достапноста на офицерот (без оглед дали физички се наоѓа во истите простории како вработените, преку телефон, електронска пошта или други средства за комуникација) е од суштинско значење за вработените, субјектите на лични податоци, па и самиот контролор односно

обработувач. Всушност, достапноста на офицерот претставува важен услов кој треба да биде исполнет за да може група на правни лица да определат еден офицер за заштита на личните податоци.

Контролорите односно обработувачите треба да направат детална анализа за потребата од назначување на офицер за заштита на податоци од која ќе произлезе одговор на прашањето дали ќе биде назначен офицер од редот на своите вработени или ќе биде ангажирано надворешно лице кое ќе ја има улогата на офицер и дали истиот ќе ги претставува и интересите на други контролори (заеднички офицер). Направената анализа и донесената одлуката треба да се дел од задолжителната документација на контролорот односно обработувачот која е потребна за демонстрирање на принципот на одговорност и отчетност.

Што значи поимот „Обработка на лични податоци во голема мера“?

При утврдување на значењето на поимот „голема мера“, односно дали процесите за обработка на личните податоци се од голема мера, треба да се земат предвид особено следните критериуми:

- Бројот на субјекти на лични податоци на кои се однесува обработката;
- Обемот на податоци и/или опсегот на различни категории на лични податоци кои се обработуваат;
- Временскиот период на активностите за обработка (дали е временски ограничен или е траен);
- Географската распространетост на обработката (дали е на едно или повеќе места, една или повеќе држави...).

Што значи поимот „Редовно и систематско следење на субјектите на лични податоци“?

Исто како и обработката на личните податоци од голема мера, поимот на редовно и систематско следење на субјектите на личните податоци не е дефиниран во Законот, но јасно ги вклучува сите форми на следење и профилирање на интернет, вклучувајќи ги и целите на рекламирањето базирано на однесувањето на

корисникот (профилирање). Треба да се има предвид дека поимот следење не е ограничен само на онлајн-околината.
Согласно мислењето на Работната група 29[7] поимот „редовно“ ги има едно или повеќе од следните значења:

- Тековни активности или активности кои се случуваат во одредени интервали за одреден период;
- Повторувачки или активности кои се повторуваат во фиксни времиња; и
- Активности кои се случуваат постојано или периодично.

Исто така, согласно мислењето на Работната група 29 поимот „систематско“ ги има едно или повеќе од следните значења:

- Активности кои се појавуваат според системот (систематски);
- Активности кои се претходно договорени, организирани или методички;
- Активности кои се случуваат како дел од генералниот план за собирање на податоци; и
- Активности кои се спроведуваат како дел од одредена стратегија.

На пример:

- Управување со телекомуникациската мрежа;
- Обезбедување на телекомуникациски услуги;
- е-пошта за повторно враќање;
- Профилирање и оценување за целите на проценка на ризик (на пр. за цели на анализа на кредитен ризик, утврдување на премии за осигурување, спречување на измами, откривање на перење пари);
- Следење на локација (на пример од мобилни апликации);
- Програми за лојалност;
- Рекламирање базирано на начинот на однесување на корисникот;

[7] Работна група 29 беше советодавно тело составено од претставник од органите за заштита на личните податоци на секоја земја-членка на ЕУ, Европскиот супервизор за заштита на податоците и Европската комисија. Со донесување на GDPR е основан Европскиот одбор за заштита на личните податоци

- Следење на велнес, фитнес и здравствени податоци преку уреди што може да се носат;
- Видео надзор;
- Поврзани уреди (на пример паметни мерачи на енергија, паметни автомобили, домашна автоматизација итн).

Што значи поимот „Основни активности на контролорот или обработувачот“?

Основните активности на контролорот, односно обработувачот треба да се разберат како клучни операции за постигнување на целите на контролорот или обработувачот. Под овој поим се подразбираат сите активности каде обработката на податоците претставува неразделен дел од активноста на контролорот или обработувачот.
На пример: Обработката на здравствените податоци, како што е здравствената евиденција на пациентот, треба да се смета како една од основните активности на здравствените установи и затоа во овој случај здравствените установи мора да назначат офицер за заштита на личните податоци.
Од друга страна, сите организации спроведуваат и одредени активности за поддршка.
На пример: Пресметката и исплатата на платата на своите вработени или одржување на стандардни ИТ активности за поддршка на контролорот или обработувачот претставуваат неопходни функции за поддршка на основната дејност на контролорот во однос на главната работа, но иако овие активности се неопходни, тие се сметаат за помошни функции, а не за основни функции (core functions).
Уште една новина во Законот за заштита на личните податоци претставува обврската на контролорите за известување на субјектот на личните податоци за нарушување на безбедноста на личните податоци. Имено во случај на нарушување на безбедноста на личните податоци, за кое постои веројатност да предизвика висок ризик за правата и слободите на физичките лица, контролорот, веднаш го известува субјектот на личните податоци за ова нарушување. Во известувањето до субјектот на личните податоци на јасен и едноставен јазик се опишува природата на нарушувањето на безбедноста на личните податоци и се наведуваат најмалку информациите за името, презимето и

контакт податоците на офицерот за заштита на личните податоци или на друго лице за контакт, од кое може да се добијат повеќе информации; опис на можните последици од нарушувањето на безбедноста на личните податоци; опис на преземените или предложените мерки од страна на контролорот за справување со нарушувањето на безбедноста на личните податоци, вклучувајќи соодветни мерки за намалување на можните негативни ефекти.
Притоа Законот индиректно ја форсира примената на технологии кои ако се правилно применети го намалуваат ризикот од можни злоупотреби на личните податоци. Имено, Законот утврдува дека известувањето до субјектот на личните податоци, не е задолжително, доколку контролорот применил соодветни технички и организациски мерки за заштита и тие мерки биле применети во однос на личните податоци засегнати од нарушувањето на безбедноста на личните податоци, особено мерки кои што личните податоци ги прават неразбирливи за секое лице кое нема овластување за пристап до нив, како што е на пример криптирањето.

II.1 Положбата на офицерот за заштита на личните податоци согласно Законот

Законот за заштита на личните податоци, улогата и положбата на офицерот за заштита на личните податоци уште повеќе ја зајакнува. Контролорот и обработувачот се должни да обезбедат офицерот за заштита на личните податоци на соодветен начин и навремено да биде вклучен во сите прашања поврзани со заштитата на личните податоци. Притоа, треба да му обезбедат поддршка и да му помагаат на офицерот при извршувањето на работите и должностите кои тој треба да ги врши, обезбедувајќи му ресурси неопходни за извршување на тие работи, како и пристап до личните податоци и операциите на обработка, и одржување на неговото стручно знаење. Понатаму, новина во однос на офицерот е и обврската за контролорот и обработувачот да гарантираат дека нема да добива никакви упатства во однос на извршувањето на неговите работи. Притоа, офицерот не смее да биде сменет или казнет од страна на контролорот или обработувачот заради извршувањето на своите работи и должности. Како би се зајакнала целосно положбата на офицерот, контролорот, односно обработувачот имаат обврска во однос на неговата статусна положба да обезбедат

дека тој директно и единствено е одговорен пред највисокото раководно ниво. Законот предвидува обврска за контролорот да обезбеди дека сите физички лица кои во однос на контролорот се јавуваат како субјекти на личните податоци, да можат да го контактираат офицерот за заштита на личните податоци за сите прашања поврзани со обработката на нивните лични податоци и за остварувањето на нивните права според овој закон.

III. НАЧЕЛА ПОВРЗАНИ СО ОБРАБОТКАТА НА ЛИЧНИ ПОДАТОЦИ

Во Законот за заштита на лични податоци се уредени седум начела за обработка на личните податоци:

- Законитост, правичност и транспарентност
- Ограничување на целите
- Минимален обем на податоци
- Точност
- Ограничување на рокот на чување
- Интегритет и доверливост
- Отчетност.

Невладините организации како и сите останати контролори, мора да ги применуваат кумулативно сите начела поврзани со обработката на лични податоци во сите случаи на обработка и во текот на целокупниот процес на обработка на личните податоци. Треба да се истакне дека неприменувањето на било кое начело претставува повреда на одредбите од Законот заштита на личните податоци.

1. ЗАКОНИТОСТ, ПРАВИЧНОСТ И ТРАНСПАРЕНТНОСТ

Согласно првото начело, личните податоци се обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци.

За да биде законска, обработката треба да биде поврзана со активност која е во согласност со Законот во поширока смисла. Обработката на личните податоци од страна на контролорот, односно обработувачот на лични податоци е законска доколку се врши врз основа на закон и доколку релевантната законска рамка е формулирана на јасен и прецизен начин за да може лицата да го приспособат своето однесување на неа. Ова начело утврдува дека секоја операција на обработка треба да биде во согласност со законот кој го применува односниот контролор.

На пример, собирањето на копија од лична карта може да се врши само доколку е уредено во конкретниот закон согласно кој се врши собирањето на податоци. Па така, доколку се легализира

бесправно изграден објект, согласно Законот за постапување со бесправно изградени објекти, подносителот има обврска заедно со барањето да приложи и копија од неговата лична карта за која што обработка во овој случај постои законски основ. Но, доколку субјектот на лични податоци склучува договор со телекомуникациски оператор за користење на телефонски број во тој случај операторот нема законски основ да бара да се приложи или направи копија од личната карта на претплатникот.

Пример за постоење на законски основ за обработка на поголем обем на лични податоци кои се однесуваат на приходи (пример по основ на социјална помош, додатоци за глувост, слепило...) и финансиска состојба на субјектот на личните податоци вклучително и на членовите на неговото семејство, се случаите кога заинтересираното лице за користење на бесплатна правна помош се обраќа до здружение или правна клиника и истото пополнува барање кон кое се приложуваат соодветни докази. Во овој случај здружението има законски основ за обработка на лични податоци за финансиската состојба на барателот и членовите на неговото семејство (а со доставувањето на документите за приход и основ за обработка на здравствени податоци: глувост, слепило, мобилност и сл.), од причина што во Законот за бесплатна правна помош конкретно е уредено дека овие податоци се неопходни за да се одлучи дали барателот има право на бесплатна правна помош.

При одлучувањето дали обработката е правична, треба да се земе предвид начинот односно методот на кој се собрани личните податоци, како и информираноста на субјектот на личните податоци од кој што се добиени односно на кој што се однесуваат податоците.

Правична и транспарентна обработка значи дека сите информации и комуникацијата со субјектот на лични податоци е лесно достапна и се објаснува на јасен и разбирлив јазик, односно сите информации во врска со обработката на тие лични податоци кои се однесуваат на субјектот на личните податоци да бидат лесно достапни и лесно разбирливи (пример: визуелизација или преку употреба на вебстраница). Понатаму, обработката на личните податоци треба да биде транспарентна за субјектите на лични податоци, што значи дека тие треба да бидат свесни за фактот дека личните податоци кои се однесуваат на нив, се обработуваат (во која било форма на обработка) и треба да бидат информирани за целите на таа обработка. Субјектите на

личните податоци треба да бидат свесни за ризиците, правилата, заштитните мерки и правата во врска со обработката на личните податоци и начинот на остварување на нивните права во врска со таквата обработка. При исполнување на неговите обврски да обезбеди транспарентни информации, контролорот, односно обработувачот треба да ги земе предвид специфичните околности и контекстот во кој се обработуваат личните податоци.

Кога личните податоци се собираат од субјектот на личните податоци, субјектот исто така треба да биде информиран дали е должен да ги достави личните податоци и за последиците доколку не ги достави таквите податоци. Аспектот на транспарентност од ова начело бара од контролорот да гарантира дека субјектите на лични податоци чиишто податоци се обработуваат се свесни за обработката и степенот до кој истите се обработуваат.
Ова начело има за цел стекнување на доверба во процесите на обработката на податоците што влијаат врз субјектот на личните податоци овозможувајќи му да ја разбере причината и целта на обработката на податоците и доколку е потребно и можно да одлучи за идна обработка на неговите податоци за цел, различна за целта за која првично се обработени. Аспектот на транспарентност од ова начело, на субјектите на лични податоци им дава практични придобивки овозможувајќи им значајна можност да ги разгледаат и потенцијално да ги остварат своите права во однос на понатамошната обработка на нивните лични податоци.

1.1. УСЛОВИ ЗА ЗАКОНИТОСТ НА ОБРАБОТКАТА

Во Законот за заштита на личните податоци е утврдено 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 на договор каде 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 (наведениот правен основ за обработка на личните податоци се утврдува со закон),
- обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице,
- обработката е потребна за извршување на работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон (наведениот правен основ за обработка на личните податоци се утврдува 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 коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете. (оваа одредба нема да се применуваат за обработка на личните податоци од страна на органите на државната власт при спроведување на нивните надлежности.)

Онаму каде обработката на личните податоци за цел различна од онаа за која што се собрани личните податоци не се заснова на согласност на субјектот на личните податоци или врз основа на конкретен закон, во случаи кога ваквата обработка претставува неопходна и пропорционална мерка во едно демократско општество за да се заштитат целите на обезбедување на:

- националната безбедност; одбраната; јавната безбедност; превенција, истрага, откривање или гонење на сторителите на кривични дела или извршување на изречените казнени санкции, вклучувајќи превенција и спречување на закани за јавната безбедност;
- други важни цели од општ јавен интерес за РС Македонија, а особено важен економски или финансиски интерес, вклучувајќи монетарни, буџетски и даночни прашања, јавно здравје и социјална заштита;
- заштита на независноста на судовите и судските постапки;
- превенција, истрага, откривање и гонење на прекршувањето на етичките правила за регулираните професии;
- следење, инспекциски надзор или регулаторни функции кои се барем повремено поврзани со исполнување на

надлежностите на органите на државната власт во претходно наведените случаите наведени;

- заштита на субјектот на личните податоци или на правата и слободите на други физички лица; спроведување на барањата во граѓански постапки, тогаш контролорот за да утврди дали понатамошната обработка за други цели е во согласност со првичната цел за која биле собрани личните податоци, е должен меѓу другото да ги земе предвид:
- секоја поврзаност помеѓу целите заради кои се собираат личните податоци и целите за предвидената понатамошна обработка,
- контекстот во кој биле собрани личните податоци, особено во поглед на односите помеѓу субјектите на лични податоци и контролорот,
- природата на личните податоци, а особено дали се обработуваат посебни категории на лични податоци или се обработуваат лични податоци кои се однесуваат на казнени осуди и казнени дела согласно Законот за заштита на личните податоци,
- можните последици од предвидената понатамошна обработка за субјектите на лични податоци,
- постоењето на соодветни заштитни мерки кои може да вклучуваат криптирање или псевдонимизација.

Законот ги утврдува критериумите за оценка на компатибилноста помеѓу првичните цели на обработката и натамошната обработка (обработка за потреби различни од првичните). Оценка на компатибилност треба да се спроведе во сите случаи на натамошна обработка доколку нема согласност од субјектот на личните податоци или доколку нема законска одредба која ја оправдува натамошната обработка за потребите на националната безбедност; одбраната; јавната безбедност; превенцијата, истрага... (наведени во Законот), согласно претходно наведените критериуми.

2. ОГРАНИЧУВАЊЕ НА ЦЕЛИТЕ

Согласно ова начело, личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели.

Натамошната обработка за цели на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели при кои што контролорот задолжиелно применил соодветни заштитни мерки за правата и слободите на субјектот на личните податоци во согласност со Законот за заштита на личните податоци нема да се смета дека не е во согласност со првичните цели за кои се собрани личните податоци. Овие мерки може да вклучуваат псевдонимизација под услов, наведените цели да може да се постигнат на овој начин. Кога наведените цели може да се постигнат преку понатамошна обработка, која што не дозволува или повеќе не дозволува идентификација на субјектите на лични податоци, тие цели се постигнати на овој начин. Натамошната обработка во овој случај е законита бидејќи целите се легитимни и личните податоци кои се предмет на обработка се ограничени и веќе не можат да му се препишат на конкретниот субјект на личните податоци.

Главната карактеристика на ова начело е дека податоците не треба да се користат без контрола туку за конкретни цели, кои не може да се постигнат без планираната обработка на податоците. Контролорот, односно обработувачот на самиот почеток треба да утврди која е целта на обработката на личните податоци. Целта треба да биде конкретна, законита и експлицитна (да не остава простор за толкување). Целите треба да бидат изречно утврдени (не општи) и согласни со закон во поширока смисла. Во некои случаи целите на обработката на податоци може да бидат резултат на конкретна законска обврска на контролорот, а во други во зависност од неговиот опфат на активности и потреби за остварување на работниот процес.

Ограничувањето на обработката во рамките на почетната цел значи да се дефинира зошто е потребна обработка на лични податоци. Секоја обработка надвор од обемот на првичната цел за која се собираат податоците претставува понатамошна

обработка. Понатамошната обработка за друга цел не мора да значи дека е некомпатибилна, но компатибилноста треба да се процени од случај до случај, а доколку се утврди дека не е соодветна на првичната цел, контролорот односно обработувачот може да побара дополнителна изречна и информирана согласност од субјектот на кој се однесуваат личните податоци, па во случај ако не добие согласност, собраните лични податоци за првичната цел, не смее да се обработуваат за други цели.

На пример, дококу субјектот на личните податоци (клиентот) ги дал своите податоци на банка за цели на отворање сметка и земање кредит, доколку клиентот не даде дополнителна согласност, банката нема основ неговите податоци да ги обработува за цели на нудење промотивни услуги односно директен маркетинг, бидејќи целта е различна од првичната цел на обработка на личните податоци. Но, доколку клиентот не ги плаќа ратите од кредитот, па од таа причина, а за цели на наплата на побрувањето банката (по склучување договор согласно законските барања) ги даде податоците за контакт на клиентот, износ на ратата и периодот на плаќање на обработувач: правно лице чија што дејност е наплата на долг, а за цели на плаќање на кредитот, во тој случај целта на обработка на податоците на субјектот на личните податоци е компатибилна со првичната цел на обработка.

3. МИНИМАЛЕН ОБЕМ НА ПОДАТОЦИ

Личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат. Согласно ова начело, контролорот односно обработувачот треба да го обработува само минималниот обем на податоци кој е апсолутно неопходен за постигнување на релевантната цел на обработката. Обработката на повеќе лични податоци од она што е неопходно се смета за несразмерна и како таква е повреда на начелото за минимален обем на податоците. Интенцијата на ова начело е да се обработуваат само неопходните податоци сообразно на целта за која се собираат. Сите други податоци надвор од таа граница се сметаат за прекумерни и непропорционални.

На пример, при влез во определен објект каде што овластено лице од контролрот води евиденција на посетители, запишувањето на матичниот број на посетителот, покрај името и презимето на посетителот, претставува преобемна обработка на лични податоци за цели на водење евиденција на посетители и во тој случај обработката на единствен матичен број на граѓанинот е во спротивност со начелото на минимален обем на податоци.
Во нашата држава постои традиција на собирање на лични податоци повеќе од што е потребно и тоа за неодредена цел, односно цели според прифатеното ,,ќе се најдат во иднина ако затребаат", што апсолутно се коси со начелото на минимален обем на податоци. Кога субјектот на лични податоци има можност да одлучи дали и кои лични податоци да ги даде на контролорот во случаи кога личните податоци се обработуваат врз основ на согласност, субјектот секогаш треба да одмери дали категориите на лични податоци кои се бараат од него имаат разумна поврзаност со целта за која се собираат податоците. Практично обемот на лични податоци кој се собира треба да има логична поврзаност со целта за која се собираат податоците.
Како илустрација, доколку се нарачуваат кондури од продавница која продава преку интернет, нелогично е покрај бројот на кондури да се бара и датум на раѓање, возраст или брачен статус.

4. ТОЧНОСТ

Личните податоци се точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени.

Начелото на точност на податоците го обврзува контролорот односно обработувачот да ги обработува само личните податоци кои се точни и ажурирани. Понекогаш точноста на податоците е суштинска за давањето на услугата и/или за извршување на обврските на контролорот, односно обработувачот. На пример, обработката на одредена медицинска дијагноза на еден пациент е од витално значење за неговиот точен и благовремен третман. Недостигот на прецизни информации во овој случај може да има

штетно влијание врз здравствениот статус на пациентот, па дури и полоши импликации. Оттаму, контролорите на податоци треба да преземат мерки преку кои ќе се осигураат дека личните податоци кои се неточни, од гледна точка на целите за кои се обработуваат, благовремено да бидат коригирани или избришани.

Начелото на точност на личните податоци е тесно поврзано со квалитетот на податоците, но и со квалитетот на услугата која ја испорачува контролорот, односно обработувачот. Имено, почитувањето на ова начело во поголем број на случаи е во корист истовремено и за двете страни: субјектот на лични податоци и контролорот. На пример, доколку вработениот ја променил трансакциската сметка преку која зема плата, односно ја затворил старата трансакциска сметка и отворил нова, од интерес на вработениот е да го информира работодавецот за направената промена за да може да добие прилив од работодавецот, а од друга страна информирањето е од интерес на работодавецот за да ги ажурира податоците во направената преметка за плата при што ќе ја отстрани можноста фолиото за плата да биде стопирано или вратено од надлежните институции поради неточни податоци.

Во определени случаи давањето на неточни податоци може да доведе и до недобивање на бараната услуга: на пример во Законот за бесплатна правна помош е уредено дека заинтересираното лице за бесплатна правна помош е должно да даде точни податоци за правното прашање за кое бара секундарна правна помош, за својата финансиска состојба и за финансиската состојба на членовите на семејството со кои живее, како и да достави копии од документите што ги потврдуваат податоците наведени во барањето за секундарна правна помош, како и копии од документи кои Министерството за правда не може да ги прибави по службена должност, а кои се однесуваат на правното прашање согласно со закон.

Тука треба да се напомене и фактот дека точноста не претставува само едно од начелата за заштита на личните податоци, туку и право на субјектот на лични податоци неговите податоци да бидат точни, целосни и ажурирани и право на бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени.

5. ОГРАНИЧУВАЊЕ НА РОКОТ НА ЧУВАЊЕ

Согласно ова начело, личните податоци треба да се чуваат во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци.

Личните податоци може да се чуваат подолго од нивниот рок на чување ако се обработуваат само за целите на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели, а со применување на соодветни технички и организациски мерки за безбедност на личните податоци, заради заштита на правата и слободите на субјектот на личните податоци.

Законот за заштита на личните податоци утрвдува дека при обработката за цели на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели, контролорот е должен да примени соодветни заштитни мерки за правата и слободите на субјектот на личните податоци во согласност со овој закон. Овие заштитни мерки обезбедуваат применување на технички и организациски мерки, особено во однос на почитувањето на начелото на обработка на минимален обем на податоци. Овие мерки може да вклучуваат псевдонимизација под услов, наведените цели да може да се постигнат на овој начин. Кога наведените цели може да се постигнат преку понатамошна обработка, која што не дозволува или повеќе не дозволува идентификација на субјектите на лични податоци, тие цели се постигнати на овој начин.

Законот за заштита на лични податоци му овозможува на контролорот, односно обработувачот да ги чува податоците само за ограничен временски период. Треба да се истакне дека чувањето на податоци за неограничен временски период е забрането. По правило податоците може да се обработуваат (чуваат) сè додека е потребно контролорот односно обработувачот да ги постигне релевантните цели на обработката.

Личните податоци треба да се чуваат во форма која овозможува идентификација на субјектите на податоци во период кој не е подолг отколку што е потребно да се постигнат целите за коишто

се обработуваат податоците. Личните податоци може да се чуваат и подолг период, но само за цели на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели со преземање на соодветните технички и организациски мерки со цел да се заштитат правата и слободите на субјектот на личните податоци.

Роковите на чување на лични податоци може да бидат определени со закон или доколку не постои законска определеност на рокот на чување на личните податоци, во тој случај контролорот, односно обработувачот го утврдува рокот на чување на личните податоци по претходно направена анализа за неопходноста на податоците. Имено, во овие случаи личните податоци можат да се чуваат до исполнување на целта за која што истите биле собрани. Практично анализата која што контролорот, односно обработувачот треба да ја направи за да го определи рокот на чување треба да даде одговор на прашањето: кога целта за која се собрани податоците се смета за исполнета?! Контролорот, односно обработувачот треба да прави периодичен преглед на личните податоци кои се чуваат, како и ревидирање на роковите доколку е потребно, а соодветно на целите.

Во оваа констелација може повторно да се напомене дека традицијата на собирање на лични податоци за да се најдат во иднина ако затребаат, што се негува во нашата држава, апсолутно се коси покрај со начелото на минимален обем на податоци, и со начелото на ограничување на рокот на чување на личните податоци.

Принципот на ограничување на рокот на чување гарантира дека периодот за кој се чуваат личните податоци е сведен на потребниот максимален рок, со други зборови дека секогаш постои рок за чување на личните податоци.

По истекот на роковите за чување на лични податоци истите мора да се избришат, односно уништат на начин кој што е уреден согласно правилата за заштита на лични податоци применувајќи соодветни технички и организациски мерки.

Зошто ограничувањето на рокот на чување на личните податоци е важно?

Обезбедувањето дека се бришат или анонимизираат личните податоци кога веќе не се потребни, ќе го намали ризикот податоците да станат небитни, прекумерни, неточни или застарени. Покрај тоа ќе помогне да се почитуваат начелата на

минимизирање и точност на податоците, како и да се намали ризикот на користење на ваквите податоци по грешка на штета на сите засегнати страни. Личните податоци што се чуваат предолго, по дефиниција, ќе бидат непотребни, а многу е веројатно дека нема да постои ниту законски основ за чување. Воедно, од практичен аспект, неефикасно е да се чуваат повеќе лични податоци отколку се потребни, а може да имплицира и непотребни трошоци поврзани со складирање и безбедност на податоците. Добра практика околу ограничувањето на рокот на чување е постоењето на јасни политики/процедури за период на чување и бришење, што исто така ќе го намали товарот за справување со прашања за роковите на чување на личните податоци и индивидуални барања за бришење или остварување на новото право „да се биде заборавен“. Политиките за чување и период на бришење или анонимизирање на податоците, треба да ги содржат видовите записи или податоци што се чуваат, за што се користат и колку ќе се чуваат, како и период на вршење на проверка и ревидирање на роковите на чување. Ваквата политика/процедура помага да се воспостават и документираат стандардни периоди на чување за различни категории на лични податоци што доведува до доследно почитување на начелото на ограничување на рокот на чување на личните податоци.

6. ИНТЕГРИТЕТ И ДОВЕРЛИВОСТ

Согласно ова начело личните податоци треба се обработуваат на начин кој обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки.

За разлика од претходно елаборираните начела ова начело заедно со начелото на отчетност претставуваат новина во легислативата за заштита на лични податоци.

Контролорите имаат обврска да обезбедат соодветна безбедност на личните податоци со примена на адекватни технички или организациски мерки. Целта на начелото интегритет и доверливост е да се гарантира заштита на личните податоци од

неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, или пак откривање или пристап до податоците. Ваквите незаконски дејствија може да резултираат со физичка, материјална или нематеријална штета за субјектите на лични податоци, додека соодветната имплементација на начелото на интегритет и доверливост треба да спречи или барем да го минимизира евентуалното појавување на која било од овие закани.

Интегритетот и доверливоста на личните податоци подразбира одржување на конзистентност, комплетност, точност и доверливост на личните податоци во текот на целиот циклус на нивна обработка.Тоа подразбира дека личните податоци не смеат да се менуваат при обработување, пренос на истите и мора да се преземат мерки и активности за да се обезбеди дека податоците не можат да бидат изменети од неовластени лица.

Интегритетот и доверливоста како начела за заштита на личните податоци, покрај обезбедување на интегритет и доверливост на самите лични податоци вклучува и интегритет и доверливост на целокупниот систем за заштита на личните податоци, односно на информациските и човечките ресурси, што се обезбедува со имплементирање на соодветни технички и организациски мерки на безбедност, вклучително и соодветна опрема за обработка на лични податоци прилагодена и дизајнирана согласно барањата на новиот Закон за заштита на личните податоци (*privacy by deffault and privacy by design*).

7. ОТЧЕТНОСТ

Последното, седмо начело кое се однесува на обработката на личните податоци е начелото на отчетност. Согласно ова начело, контролорот е одговорен за усогласеноста со сите претходно наведени начела, при што е должен истата и да ја демонстрира (отчетност).

Ова начело во законот е утврдено во одделен став за да се потенцира неговата важност, како и неговото влијание на сите други начела споменати претходно. Начелото на отчетност има два важни аспекти:

- Обврската на контролорот во пракса да ги спроведе сите други шест начела за обработка на личните податоци односно одговорност на контролорот да преземе соодветни и ефективни мерки за спроведување на начелата за заштита на личните податоци во пракса и
- Обврската на контролорот на личните податоци да обезбеди докази за усогласеност со сите други шест начела на обработка на податоците, односно способност да демонстрира, по барање, на надворешните засегнати страни, вклучувајќи го и надзорниот орган (Агенцијата за заштита на личните податоци), дека се преземени соодветни и ефективни мерки за спроведување на принципите во пракса.

Принципот на отчетност има за цел да гарантира дека контролорите на личните податоци се во позиција да обезбедат и демонстрираат усогласеност со начелата за заштита на личните податоци во пракса, при што контролорот е должен да обезбеди и приложи соодветен доказ. Целта на ова начело е да ја потврди и да ја зајакне одговорноста на контролорите за обработката и квалитетот на личните податоци.

Обврската, контролорот да го почитува начелото на отчетност, подразбира дека контролорот е одговорен при обработката на личните податоци и демонстрира дека организацијата има капацитет да ги почитува законските барања. Генерално, целта на пристапот за одговорност е воведување на контролорот во правила и механизми за обработка на лични податоци кои, од една страна, лесно се спроведуваат, а од друга страна, обезбедуваат следливост на релевантните операции и го имаат целокупниот ефект на убедливо покажување дека обработката на лични податоци е во целосна усогласеност со барањата.

Отчетноста се карактеризира со фактот дека се фокусира на утврдување на целите за заштита на личните податоци врз основа на критериумите што се предвидени со постојното законодавство. Дозволена е апсолутна слобода во однос на технолошката поддршка за отчетноста. Крајната цел на ова начело е да ги покрие сите операции за обработка на лични податоци во контролорот.

Почитувањето на начелото на отчетност, се очекува да го олесни прекуграничното движење на податоци под унифицирани правила и стандарди предвидени за заштита на поединците. Во однос на

субјектите на личните податоци, механизмите за демонстрирање на отчетноста треба да ја зголемат нивната доверба дека нивните податоци се заштитени.

Отчетноста како начело, е од суштинско значење за идентификување на специфични закани и ризици за правата на субјектите на личните податоци, а соодветно, помага при воведувањето на нови модели на обработка или барем нивно ажурирање. Од друга страна, начелото на отчетност бара од контролорите да ја преземат одговорноста за податоците што ги обработуваат. Преземањето одговорност за она што прави контролорот со личните податоци и демонстрирањето на чекорите кои контролорот ги презема за заштита на правата на субјектите на личните податоци не само што резултира во подобра правна усогласеност, туку нуди и конкурентска предност. Отчетноста претставува и можност контролорот да покаже и докаже дека ја почитува приватноста на субјектите на лични податоци (вработени, клиенти, потрошувачи) чии лични податоци ги обработува. Демонстрирањето на отчетност и одговорност несомнено може да му помогне на контролорот да ја развива и одржува довербата на субјектите чии што лични податоци ги обработува.

Начелото на отчетност се однесува на сите контролори на лични податоци и на сите процеси на обработка на лични податоци. Меѓутоа, препорачливо е конкретните мерки преземени од страна на контролорите да одговараат на ризиците кои произлегуваат од обработката и природата на личните податоци. Препорачливо е контролорите да применуваат и механизми за проценка на ефикасноста (или неефикасноста) на мерките кои ги применуваат за демонстрирање на отчетноста. Ова начело вклучува не само усогласување со Законот за заштита на личните податоци, туку и активно обезбедување и способност да се демонстрира таква усогласеност. Начелото на отчетност оди подалеку од самото усогласување со правилата: тоа подразбира промена во културата на обработка на лични податоци и допринесува за создавање на култура на посветеност на заштитата на личните податоци, со вградување на систематска и докажана усогласеност во контролорот.

Начините на демострирање на отчетност се прикажани во точката II.2 од оваа анализа, како една од круцијалните новини од новиот Закон за заштита на личните податоци.

IV. КЛУЧНИ ТЕМИ И ПРАШАЊА

Откако, во главите I, II и III ги елабориравме новините во Законот за заштита на личните податоци, како и клучните принципи и начела кои се најважни во работењето на секој контролор, па и во работењето на невладините организации, во продолжение на анализата се дава одговор на клучните теми и прашања кои директно го засегаат и влијаат на начинот на работењето на невладините организации, тогаш кога тие обработуваат лични податоци. Во таа насока, во продолжение се дадени објаснувања на Законот за заштита на личните податоци во однос на следните прашања:

- Согласност
- Конторолор и обработувач
- Безбедност на обработката
- Офицер за заштита на личнитите податоци
- Права на субјектот на личните податоци
- Специфичности во заштитата на лица со пречки во телесниот или менталниот развој или комбинирани пречки (начин на добивање на согласност, ризици, правила, заштитни мерки и права во однос на обработката на личните податоци во однос на активностите кои се насочени кон овие лица).

IV.1 СОГЛАСНОСТ

Законот за заштита на личните податоци утврдува дека, кога обработката на личните податоци се врши врз основа на согласност, контролорот е должен да демонстрира дека субјектот на личните податоци дал согласност за обработка на неговите лични податоци. Притоа, за согласноста да се смета за законита, таа треба да биде слободно дадена, конкретна, информирана и недвосмислена изјавена волја на субјектот на личните податоци, преку изјава или јасно потврдено дејствие, а со кои се изразува согласноста за обработка на неговите лични податоци.

Ако согласноста на субјектот на лични податоци е дадена во форма на писмена изјава која се однесува и на други прашања, барањето за согласност мора да се презентира на начин кој јасно може да се разликува од другите прашања, во разбирлива и лесно достапна форма, користејќи јасни и едноставни средства.

Ако согласноста на субјектот на лични податоци се однесува на обработка на личните податоци за повеќе цели, тогаш согласноста, односно барањето за согласност мора да биде грануларно и да дава можност за изјаснување на субјектот на личните податоци за секоја цел на обработката на личните податоци одделно (без оглед дали станува збор за согласност во писмена изјава или пак по електронски пат).

При тоа, субјектот на лични податоци кој дал согласност за обработка на неговите лични податоци, има право да ја повлече согласноста во секое време, а повлекувањето на согласноста не влијае на законитоста на обработката, заснована на дадена согласност пред нејзиното повлекување.

Треба да се нагласи дека во случај на обработка на личните податоци врз основа на претходно добиена согласност од субјектот на личните податоци, треба да се запазат и почитуваат начелата за заштита на личните податоци од аспект на јасното утврдување на целта заради која се обработуваат, како и од аспект на соодветноста, релевантноста и обемноста на податоците кои се обработуваат, а во корелација со целите заради кои се собираат и обработуваат, како и во однос на нивната точност, целосност, ажурираност и рок на чување и обработка (data economy, data necessity, data accuracy, purpose limitation).

Ставајќи ја согласноста во контекст на основите за обработка на личните податоци, притоа директно поврзувајќи ја со начелата за обработка на личните податоци, а особено со законитоста на обработката на личните податоци, треба да се истакне дека обработката на личните податоци од аспект на законитоста во основа се сведува на две прашања, кои ако се правилно поставени и особено ако се точно одговорени, директно ќе им помогнат на невладините организации да знаат дали вршат законита или можеби незаконита обработка на личните податоци. Имено, со цел секогаш невладините организации да знаат кога може да вршат обработка на личните податоци, треба да си ги постават следните прашања:

1. Дали имаме законски основ за обработката на личните податоци кои (ќе) ги обработуваме?

2. Доколку одговорот на првото прашање е негативен, во тој случај дали од субјектот на личните податоци, имаме претходно добиена согласност за обработка на неговите лични податоци за однапред утврдена цел, односно цели, која во секое време ќе можеме да ја докажаме?

Доколку одговорот на првото прашање е позитивен, во тој случај не постои потребата од поставување на второто прашање. Но, доколку одговорот на првото прашање е негативен, во тој случај се поставува второто прашање и доколку одговорот и на ова прашање е негативен, во тој случај веројатноста дека обработката на личните податоци е незаконита, е реална.

Кога говориме за начелата за заштита на личните податоци и нивната обработка, треба да се истакне дека постои разлика од аспект на условите кога може да се врши обработка на личните податоци кога станува збор за обработка врз основа на согласност на посебните категории на лични податоци и единствениот матичен број на граѓанинот. Имено, во Законот за заштита на личните податоци е утврдено дека обработката на посебните категории на лични податоци е забранета, а дека само по исклучок, обработката на посебните категории на лични податоци може да се врши ако субјектот на лични податоци дал изречна согласност за нивна обработка за една или повеќе конкретни цели. Притоа, во Законот е утврдено и дека согласноста не може да биде основ за обработка на оваа категорија на лични податоци кога со закон е предвидено дека забраната за обработка на такви податоци не може да се отповика од субјектот на личните податоци. Притоа, треба да се нагласи дека за согласноста да биде основ за законита обработка на посебните категории лични податоци, а во услови кога невладинте организации немаат законски основ за нивна обработка (но да речеме реелна потреба), покрај согласноста и почитувањето на начелата, ќе биде потребно и претходно одобрение од страна на Агенцијата за заштита на личните податоци за кое невладините организации треба да поднесат соодветно барање.

Кога говориме за согласноста, треба да се нагласи дека новина претставува согласноста на дете во однос на услугите на информатичкото општество. Имено, за сè друго како цел каде се врши обработка на личните податоци на деца, обработката е законска само ако и доколку таквата согласност е дадена или дозволена од законскиот застапник на детето. Но, во случај на услуги на информатичко општество, обработката на личните податоци на дете е законска, ако детето има најмалку 14 години. Сето ова може да има влијание на начинот на работењето на невладните организации во случај кога обработката на личните податоци е заснована на согласност на субјектот на личните податоци.

IV.2 КОНТОРОЛОР И ОБРАБОТУВАЧ (Невладини организации)

Кога говориме за Законот за заштита на личните податоци во однос на работењето на невладините организации тогаш кога тие обработуваат лични податоци, треба да се истакне дека и GDPR, а следствено и Законот, се применуваат не само за „профитните бизниси“, туку и за невладините организации, како што се на пример добротворни организации, здруженија, па дури и за политичките партии. Правилата се исти за сите, колку и да изгледаат сложени, иако ако правилно се разберат, тие се еден вид алатка која го помага работењето на сите, па и на невладините организации.

Законот за заштита на личните податоци не пристапува од аспект на тоа дали нешто е добро, или лошо од аспект на дејноста, или дали е добротворно и благородно, или не. Законот, согласно својот предмет на уредување се „занимава“ со заштитата на личните податоци на физичките лица и нивните права, и утврдува „барања“ за контролорот, односно обработувачот без оглед дали тие обработуваат лични податоци за деловни активности или пак за добротворни цели. Невладините организации кои обработуваат лични податоци (контролори, или обработувачи), треба да создадат цврсти темели за обработка на личните податоци, а потоа редовно да ги надградуваат. Оттука, сите начела, принципи, институти што важат за сите кои обработуваат лични податоци, а за кои се говори погоре во анализата, еднакво се однесуваат и на невладините организации. Затоа, на пример невладините организации како контролори треба секогаш да ги ажурираат личните податоци со кои располагаат, но и да ги избришат тогаш кога веќе не служат на целта за која биле собрани и се обработуваат. Исто така, невладините организации како контролори мора да донесат и применат соодветни заштитни мерки, како технички, така и организациски, особено при ракување со чувствителните лични податоци (посебни категории на лични податоци). Оттука, не ретко ќе се појави и потребата од ангажирање на стручни лица за приватност кои ќе можат да одговорат на задачата, а во случај кога невладните организации обработуваат посебни категории на лични податоци, ќе треба да определат и офицер за заштита на личните податоци.

Имајќи го сето ова предвид во однос на невладините организации како контролори, односно обработувачи, во продолжение ќе ги

наведеме главните задачи и одговорности кои тие треба да ги применат согласно Законот за заштита на личните податоци.

Најпрво, треба да наведеме дека согласно Законот за заштита на личните податоци под поимот:

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

Со други зборови, кога станува збор за невладините организации тие секогаш кога ќе обработуваат лични податоци самостојно или со други за свое име и сметка ќе бидат контролори, а кога ќе обработуваат лични податоци во име на контролорот, ќе бидат обработувачи.

Најважната обврска која ја имаат контролорот и обработувачот е да применат соодветни технички и организациски мерки за да обезбедат и да можат да докажат дека обработката се врши во согласност со Законот за заштита на личните податоци.

Примената на соодветни технички и организациски мерки, особено кога невладините организации обработуваат и чувствителни податоци треба да ги опфати и најновите технолошки достигнувања како што е на пример псевдонимизацијата, а кои се развиени со цел ефикасно спроведување на начелата за заштита на личните податоци. Тука, особено при обработката на личните податоци невладините организации ќе треба да настојуваат преку примената на техничките и организациските мерки да го сведат обработувањето на минимален обем на податоци со цел да се обезбеди заштита на правата на субјектите на личните податоци. Притоа, примената на технички и организациски мерки треба да обезбеди дека интегрирано се обработуваат само оние лични податоци кои се неопходни за секоја посебна цел на обработката.

Во однос на ова, невладните организации треба да внимаваат оваа обврска дека се однесува како на количеството на собрани лични податоци, така и на опсегот на нивната обработка, рокот на чување и нивната достапност. На овој начин, невладините организации како крајна цел на техничките и организациките мерки треба да обезбедат дека личните податоци без согласност на субјектот на личните податоци нема да може да бидат автоматски достапни за неограничен број на физички лица.

Кога говориме за невладините организации како контролори, треба да се наведе дека новина претставува и тоа што Законот за заштита на личните податоци дозволува тие да се јават и како заеднички контролори. Имено, Законот уредува дека ако два или повеќе контролори заедно ги утврдат целите и начините на обработка, тогаш тие претставуваат заеднички контролори. Притоа, заедничките контролори се должни на транспарентен начин да ја определат нивната соодветна одговорност за исполнување на обврските од Законот за заштита на личните податоци, особено во однос на остварувањето на правата на субјектите на личните податоци и нивните обврски за обезбедување на информациите кога податоците се собираат од субјектот на личните податоци и кога личните податоци не се добиени од субјектот на личните податоци. Воедно, тие се должни како заеднички контролори одговорноста да ја уредат со нивен меѓусебен договор, освен во случај кога одговорностите им се утврдени со закон.

Треба да се истакне дека во случај кога невладината организација не е основана во Македонија, но врши активности за обработка на личните податоци поврзани со понуда на стоки или услуги, без разлика дали од субјектот на лични податоци кој е македонски државјанин се бара да изврши плаќање или пак се врши набљудување на однесувањето на субјектите на лични податоци, доколку тоа однесување се одвива во Македонија, тогаш таа невладина организација треба да определи овластен претставник во Република Северна Македонија и тоа во писмена форма.

Кога станува збор за невладина организација која како контролор обработката ја врши и преку обработувач, односно обработката се врши во име на невладината организација како контролор, тогаш таа (невладината организација) може да користи само обработувачи кои обезбедуваат доволна гаранција за примена на соодветни технички и организациски мерки на таков начин на кој

обработката ќе се одвива во согласност со барањата од Законот за заштита на личните податоци и ќе обезбедува заштита на правата на субјектите на личните податоци. Во овој случај обработката од страна на обработувачот се регулира со договор или со друг правен акт во согласност со Закон, кој што е обврзувачки за обработувачот во однос на невладинита организација како контролор, и со кој се регулира предметот и времетраењето на обработката, природата и целта на обработката, видот на личните податоци и категориите на субјекти на личните податоци, како и обврските и правата на невладината организација како контролор.

Следна важна обврска за невладините организации како контролори е водењето евиденција во писмена и електронска форма во однос на операциите за обработка на личните податоци за кои се одговорни. Оваа евиденција е утврдена со Законот за заштита на личните податоци и таа особено треба да ги содржи следните информации:

- називот, односно името и презимето и контакт податоците на контролорот и на сите заеднички контролори, на овластениот претставник на контролорот и на офицерот за заштита на личните податоци;
- целите на обработката;
- опис на категориите на субјекти на лични податоци и на категориите на личните податоци;
- - категориите на корисници на кои се откриени или ќе бидат откриени личните податоци, вклучувајќи корисници во трети земји или меѓународни организации;
- преносот на лични податоци во трета земја или меѓународна организација, вклучувајќи идентификација на таа трета земја или меѓународна организација,
- предвидените рокови за бришење на различните категории на лични податоци;
- општ опис на техничките и организациските мерки за безбедност на личните податоци.

IV.3 БЕЗБЕДНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ (Безбедност на обработката)

Најважната работа за секој контролор е кога врши обработка на личните податоци да внимава на начелата и принципите за заштита на личните податоци, а со тоа да обезбеди и законитост при обработката на личните податоци. Во современиот начин на живеење, во услови кога личните податоци се повеќе се обработуваат во автоматизирана, електронска форма, единствениот исправен, па и возможен начин сето ова да се обезбеди е со доследно дизајнирање и примена на соодветни технички и организациски мерки. Сето ова еднакво се однесува и на невладините организации без оглед дали тие се јавуваат во својство на контролори или обработувачи. Законот за заштита на личните податоци утврдува дека земајќи ги предвид најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозноста за правата и слободите на физичките лица, контролорот и обработувачот се должни да применат соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот. Притоа, според потребата, Законот предвидува дека примената на технички и организациски мерки треба да опфати и:

- псевдонимизација и криптирање на личните податоци;
- способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка;
- способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент;
- процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.

Невладините организации кога обработуваат лични податоци треба при процена на соодветно ниво на безбедност да ги земат предвид ризиците кои се поврзани со обработката, особено од случајно или незаконско уништување, губење, менување,

неовластено откривање, или неовластен пристап до пренесените, зачуваните или на друг начин обработени лични податоци.

Притоа, невладините организации треба да вршат редовна оценка и ажурирање на техничките и организациските мерки кои ги применуваат и да настојуваат секогаш да ги применуваат оние мерки кои се соодветни на времето во кое се дизајнираат и имплементираат, а согласно најновите технолошки достигнувања (*a state of the art technology implementation*).

За техничките и организациските мерки да бидат правилно дизајнирани и имплементирани, невладините организации ќе треба да направат утврдување и процена на ризикот земајќи ги предвид притоа сите ризици кои се поврзани со обработката на личните податоци.

Притоа, правилното управување со ризикот треба да ги опфати следните четири фази:

- Преглед на сите процеси со кои се врши обработка на лични податоци;
- Процена на ризиците за секој процес на обработка на лични податоци;
- Спроведување и проверка на планираните мерки; и
- Спроведување на периодични безбедносни проверки.

Прегледот на процеси со кои се врши обработка на личните податоци треба да ги опфати сите можни процеси, а особено хардверските и софтверските решенија, комуникациските канали преку кои се врши пренос на личните податоци, а воедно да ги опфати и документите во хартиена форма на кои исто така се содржани, односно се врши обработка на личните податоци.

Проценатa на ризиците пак, треба да го опфати утврдувањето на:

- Веројатните ризици врз правата и слободите на засегнатите физички лица и тоа за следните потенцијални настани кои се однесуваат на неовластен пристап до личните податоци, непосакувани промени на личните податоци и привремена или целосна недостапност до личните податоци;
- Идентификување на изворите на ризик кој што може да биде причина за секој непосакуван настан, а имајќи ги предвид внатрешните и надворешните човечки ресурси како и другите внатрешни и надворешни извори;

- Идентификување на можните закани кои би можеле да се случат преку медиуми од кои зависат личните податоци, а кои може да бидат употребени на несоодветен начин, изменети, изгубени, набљудувани, оштетени и преоптоварени;
- Утврдување на постојни или планирани мерки што ќе овозможат решавање на секој ризик; и
- Оценување на сериозноста и веројатноста на ризиците.

Дополнително, контролорот задолжително треба да врши спроведување и проверка на планираните мерки, а со цел да се обезбеди дека тие се применуваат и тековно се тестираат, како и да спроведува периодични безбедносни проверки за што ќе треба да подготви акционен план, чија имплементација се следи од страна на раководството на контролорот.

Со правилна анализа и управување на ризикот се создаваат и главните претпоставки за соодветно дизајнирање и примена на техничките и организациските мерки за обезбедување безбедност на личните податоци. Притоа, согласно новиот закон, како и актите кои (ќе) произлегуваат од него, невладините организации земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различна веројатност и сериозноста за правата и слободите на физичките лица, ќе треба да применат технички и организациски мерки кои ќе бидат пропорционални на активностите за обработка на личните податоци. Притоа, невладините организации ќе треба да ги документираат сите процеси кои се однесуваат на обработката на личните податоци, а истите ќе треба да ги содржат податоците за:

- Идентификацијата, оценката и класификацијата на ризикот на процесите со кои се врши обработка на личните податоци (анализа на ризик);
- 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 свест на раководството и вработените за приватноста и безбедносните ризици во невладните организации;
- Дизајнирање, развивање и одржување на софтверските програми за обработка на личните податоци, особено од

аспект на техничката и интегрирана заштита на личните податоци (Data protection by design and by default);

- Начинот на обезбедување на автентикација на овластените лица во информацискиот систем;
- Начинот на обезбедување на контрола на пристап до информацискиот систем;
- Начинот на обезбедување евиденција за секој пристап до информацискиот систем;
- Начинот на управување со инциденти;
- Начинот на обезбедување на опремата на невладините организации на која се врши обработка на личните податоци;
- Начинот на обезбедување на преносливите медиуми;
- Начинот на заштита на внатрешната мрежа на невладините организации;
- Начинот на обезбедување на серверите и веб страницата на невладините организации;
- Начинот на евидентирање и чување на документацијата за софтверските програми за обработка на личните податоци;
- Начинот на обработка на личните податоци кои се псевдонимизирани или кои 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 на 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;
- Физичката безбедност;
- Начинот на ангажирање на надворешни субјекти (обработувачи);

- Динамика и начин на вршење на периодични контроли, како и процесите за вршење на внатрешна контрола и
- Други мерки и контроли кои невладините организации ги применуваат врз основа на анализата на ризикот.
- Согласно, начелото на отчетност, а имајќи ги предвид и другите принципи во Законот, исто така невладините организации ќе треба да ја менуваат и дополнуваат својата документација (откако ќе ја донесат), секогаш кога ќе се направат промени во информацискиот систем и информатичката инфраструктура, како и да вршат нејзино оценување, евалуација и ажурирање.

IV.4 ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИВОНЕВЛАДИНИТЕОРГАНЗИАЦИИ

За новините во однос на офицерот за заштита на личните податоци, неговата полжба, обврските на офицерот и случаите кога задолжително се определува офицер елабориравме во точките II.2 и II.3 од оваа анализа. Во овој дел ќе се задржиме подетално на улогата на офицерот во невладините организации.

Имено, како што претходно веќе е образложено во кои случаи е задолжително определувањето на офицер за заштита на личните податоци, овде ќе се задржиме првично на третиот случај кога е задолжително определувањето на офицер, односно кога основните активности на контролорот или обработувачот се состојат од обемна обработка на посебни категории на лични податоци или лични податоци поврзани со казнени осуди и казнени дела. Ова од причина што голем дел од невладините организации се наоѓаат во оваа ситуација. Дел од невладините организации во функција на остварување на своите основни цели за кои што се основани, обработуваат токму вакви категории на лични податоци. Тоа значи дека доколку невладината организација во рамки на своето работење се занимава на пример: со помош при остварувањето на човековите права и застапување пред институциите, помага на социјално загрозени категории на лица, се грижи за заштита на децата, вклучена е во давање на бесплатна правна помош, помага на жртви од семејно насилство,обезбедува психо-социјална поддршка, застапува при

добивање азил или пак невладината организација е формирана заради остварување на правата на лицата со попреченост, лица заболени од ХИВ, лица со ретки болести, промовирање на родова еднаквост.... итн., во најголем дел од овие случаи невладината организација многу веројатно ќе обработува посебни категории на лични податоци, па следствено на тоа има обврска да определи и офицер за заштита на личните податоци.

Понатаму, во случаите кога невладината организација е вклучена на пример: во одбраната и застапувањето во кривичната постапка согласно со одредбите на Законот за кривична постапка (на пример, бесплатна помош на преведувач, односно толкувач, ако не го разбираат или не го зборуваат јазикот на кој се води постапката) во тие случаи е вклучена и во обработка на податоци за казнени дела и казнени осуди.

Во сите овие случаи невладините организации обработуваат посебни категории на лични податоци и имаат обврска да определат офицер за заштита на личните податоци. Исто така како што и претходно е наведено, доколку во исклучителен случај основните активности на невладината организација која би се јавила во улога на контролор или обработувач се состојат од операции за обработка, кои поради својата природа, опсег и/или цели, бараат во голема мера редовно и систематско следење на субјектите на лични податоци и во таков случај би било задолжително определувањето на офицер за заштита на личните податоци.

Доколку определувањето на офицер за невладината организација која не обработува категории на лични податоци како во наведените примери, во такви околности сè уште останува можноста на доброволна основа да се определи офицер како една од алатките за демонстрирање на одговорност и отчетност на невладината организација.

Во Законот за заштита на личните податоци се набројани условите кои треба да ги исполнува едно лице за да може истото да биде определено за офицер за заштита на личните податоци. Офицерот за заштита на личните податоци се определува врз основа на неговите стручни квалификации, а особено врз основа на стручни знаења за легислативата и практиките во областа на заштитата на личните податоци, како и неговата способност да ги извршува работите кои се определени во Законот за заштита на личните податоци. За офицер се определува лице, кое: ги исполнува условите за вработување определени со закон, активно

го користи македонскиот јазик, во моментот на определувањето со правосилна судска пресуда не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност, има завршено високо образование и има стекнати знаења и вештини по однос на практиките и прописите за заштита на личните податоци.

Експертското познавање и вештините на офицерот за заштита на личните податоци треба да се утврдат во согласност со извршените операции за обработка на личните податоци и заштитата потребна за обработката на личните податоци. Потребното ниво на експертско познавање не е строго дефинирано, но мора да биде пропорционално со чувствителноста, сложеноста и количината на лични податоци што ги обработува невладината организација. На пример, кога активноста за обработка на личните податоци е особено сложена, или кога е вклучена голема количина на чувствителни податоци, на офицерот ќе му биде потребно повисоко ниво на стручност и поддршка. Исто така, постои разлика во зависност од тоа дали организацијата систематски пренесува лични податоци надвор од Европската Унија или дали таквите преноси се повремени. Затоа офицеорот треба внимателно да се избере, со должно почитување кон прашањата за заштита на личните податоци што се јавуваат во рамките на невладината организација. Во однос на професионалните квалитети на офицерот, релевантен фактор е дека истиот мора да има стручност во однос на националните и европските закони и практики за заштита на личните податоци и темелно познавање на Законот за заштита на личните податоци. Исто така, познавањето на областа на работа, дејствување и функционирање на невладината организација е корисно за поефикасно вршење на задачите од страна на офицерот. Воедно, офицерот за заштита на личните податоци треба да има добро разбирање за извршените операции за обработка, како и за информациските системи и безбедноста на личните податоци, како и потребите за заштита на личните податоци на невладината организација. При остварувањето на своите задачи офицерот треба да има способност кон задачите да пристапува од аспект на анализа на ризик, што значи дека офицерот во остварување на својата улога ги зема предвид ризиците поврзани со операциите на обработка, како и природата, опсегот, контекстот и целите на обработката. Ова значи дека од офицерот се бара да направи приоритена листа на своите активности и да ги фокусира своите напори кон прашања кои

претставуваат поголем ризик за заштитата на личните податоци. Ова не значи дека офицерот треба да го занемари следењето на усогласеноста на операциите за обработка на личните податоци кои имаат релативно пониско ниво на ризик, но укажува на тоа дека офицерот треба да се фокусира првенствено на областите со повисок ризик. Овој пристап секако треба да му помогне на офицерот во исполнувањето на неговите задачи: во советување на контролорот за тоа каква методологија да се користи при спроведувањето на проценката на влијанието на заштитата на личните податоци, кои области треба да бидат предмет на внатрешна или надворешна ревизија за заштита на податоци, кои внатрешни активности за обука треба да им се обезбедат на вработените или раководството одговорни за активностите за обработка на личните податоци и на кои операции за обработка да им го посветат поголемиот дел од своето време и ресурси.

Способноста на офицерот за заштита на личните податоци за исполнување на задолжителните задачи треба да се толкува како повикување кон неговите лични квалитети и знаења, но исто така и кон неговата позиција во рамките на невладината организација. Личните квалитети треба да вклучуваат интегритет и висока професионална етика, од причина што офицерот има клучна улога во поттикнувањето и развивањето на културата за заштита на личните податоци во рамките на невладината организација. Офицерот за заштита на личните податоци помага да се имплементираат начелата за заштита на личните податоци, принципите на обработка на личните податоци, во остварувањето на правата на субјектите на личните податоци, имплементрањето на техничка и интегрирана заштита на личните податоци, евидентирањето на активностите за обработка, безбедноста на обработката и известување и соопштување за нарушувања на безбедноста на личните податоците.

Офицерот за заштита на личните податоци може да врши и други задачи и должности. Невладината организација во улога на контролор или обработувач е должна да обезбеди дека таквите задачи и должности не доведуваат до судир на интереси.

При определувањето на офицер за заштита на личните податоци, Работната група 29 советува дека во зависност од активностите, големината и структурата на организацијата, може да биде добра практика за контролорите или обработувачите:

- да се идентификуваат позициите кои би биле некомпатибилни со функцијата на офицер за заштита на личните податоци

- да се изготват внатрешни правила за да се избегне ефектот на конфликт на интереси
- да се вклучи поопшто објаснување за конфликтите на интереси
- да се изјави дека нивниот офицер за заштита на личните податоци нема конфликт на интереси во однос на неговата функција како офицер, како начин за подигнување на свеста на ова барање
- да се вклучат заштитни мерки во внатрешните правила на организацијата и да се осигури дека објавениот оглас за позиција на офицер или договорот за услуги е доволно прецизен и детален за да се избегне конфликт на интереси. Во овој контекст, исто така треба да се има предвид дека конфликтите на интереси може да имаат различни форми во зависност од тоа дали офицерот е регрутиран внатрешно или надворешно.

Понатаму, невладината организација како контролор односно обработувач има обврска јавно да ги објави контакт податоците за офицерот за заштита на личните податоци и да ја извести Агенцијата за заштита на личните податоци. Објавувањето на податоците за офицерот е од значење исто така и заради суштинско остварување на неговта улога, односно можноста на вработените, а пред се субјектите чии лични податоци се обработуваат, да се обратат до офицерот заради остварување на своите права или добивање насоки за постапување со личните податоци за чија обработка се овластени.

Офицер определен врз основа на договор за услуги

Како што и претходно е истакнато новиот Закон за заштита на личните податоци дава можност под определени услови за офицер за заштита на лични податоци да биде назначено лице кое не е вработено кај контролорот и можност за определување на заеднички офицер под услов истиот да биде достапен за сите контролори.

При изборот помеѓу можноста да биде определен офицер од редот на вработените кај контролорот или надворешен офицер за заштита на личните податоци, контролорот треба да ги земе предвид спецификите на контекстот на обработка на податоците, операциите на обработка, обемот на податоци, категориите

на субјекти на лични податоци, количината на лични податоци кои се обработуваат и бројот на субјекти чии лични податоци се обработуваат што влијае на очекуваната ангажираност и трошоците за назначување на офицер. Начинот на назначување не прави разлика во однос на барањата, статусот и задачите на офицерот за заштита на личните податоци.

Законските услови и професионалните квалификации кои претходно се наведени секако треба да ги исполнува односно поседува и ,,надворешниот“ односно заедничкиот офицер. Во случаите кога невладините организации ќе определат ,,надворешен офицер“ истиот се определува врз основа на склучен договор за услуги во кој точно треба да бидат наведени условите односно обврските на офицерот особено обврската за достапност и доверливост. Како надворешен офицер може да се ангажира и тим на лица чии индивидуални вештини и професионални квалитети може да се комбинираат така што тимот ќе може поефикасно да му служат на клиентот – невладината организација, исполнувајќи ги задачите на офицер за заштита на личните податоци, при што во таков случај заради елиминирање на правни недореченост и добра организација, како и за спречување на конфликт на интереси за членовите на тимот, се препорачува да се има јасна распределба на задачите во рамките на тимот и да се назначи единствено лице како водечки контакт и „одговорно лице“ за секој клиент. Овие услови е препорачливо да бидат наведени во договорот за услуги.

Тука дополнително уште еднаш е потребно да се потенцира дека офицерот кој што се определува треба да има интегритет без оглед дали е внатрешен или надворешен, а особено од аспект на доверливоста како основен постулат за доследно остварување на неговата функција. Воедно, офицерот за заштита на личните податоци е обврзан со тајност и доверливост во врска со извршувањето на неговите задачи согласно закон.

Понатаму, без оглед дали офицерот е вработен кај контролорот или е ангажиран со договор за услуги, истиот треба да биде во позиција да ги извршува своите должности и задачи на независен начин при што контролорот има обврска да обезбеди дека офицерот нема да добива инструкции или да биде под влијание при остварувањето на своите задачи, како и дека нема да биде отповикан или казнет од контролорот или обработувачот за извршување на своите задачи.

Ова значи дека, при исполнување на задачите утврдени со закон, офицерот не смее да биде поучуван од страна на менаџментот на организацијата за тоа како да се справи со некое прашање, каков резултат треба да се постигне, како да се испита одредено барање на субјект на лични податоци или дали да се консултира со Агенцијата за заштита на личните податоци. Воедно на офицерот, не смее му се наложи од страна на менаџментот на организацијата да заземе одреден став за прашање поврзано со Законот за заштита на личните податоци или да му се наложи на кој начин треба да толкува определено законско решение.

Од друга страна, треба да се истакне дека автономијата на офицерот за заштита на личните податоци не значи дека истиот има овластувања за донесување одлуки што ги надминуваат неговите задачи и надлежности определени во Законот за заштита на личните податоци.

Офицерот за заштита на личните податоци директно одговара пред највисокото раководно ниво на контролорот или обработувачот. Ваквата директна одговорност обезбедува високото раководство да е свесно за советите и препораките на офицерот за заштита на личните податоци како дел од мисијата на офицерот да го известува и советува контролорот или обработувачот.

Зошто е важна улогата на офицерот?

Офицерот за заштита на личните податоци е битна фигура кај контролорот и има есенцијално значење во воспоставувањето, менаџирањето, контролата и одржувањето на целокупниот систем за заштита на личните податоци и содавањето на култура на заштита на личните податоци во невладината организација како контролор.

Информирање и советување на контролорот односно обработувачот и вработените кои вршат обработка на лични податоци

Една од работите кои офицерот ги врши е информирањето и советувањето на контролорот односно обработувачот и вработените кои вршат обработка на лични податоци. Во контекст на исполнување на оваа задача, невладината организација како контролор има обврска да обезбеди на соодветен начин и навремено офицерот да биде вклучен во сите прашања поврзани со заштитата на личните податоци.

Ова подразбира дека во случај кога се планира на пример формирање на нова збирка на лични податоци или се планира собирање на лични податоци од нови категории на субјекти на лични податоци за определена цел, во тој случај пред самото собирање на овие лични податоци, офицерот треба да биде консултиран по однос на законскиот основ за таква обработка на лични податоци, за мерките за обезбедување на безбедност на обработката кои треба да се применат при обработката на тие податоци, за роковите на чување итн.

Понатаму, доколку на пример невладината организација планира да воведе нов софтвер за обработка на лични податоци, офицерот треба да биде консултиран за техничките и организациските мерки за заштита на личните податоци се со цел да се обезбеди нивна техничка и интегрирана заштита на личните податоци (data protection by design and by default) односно да се набави таков софтвер кој што ќе ги исполни стандардите за нивна заштита.

Треба да се напомене и фактот дека и во случаите кога се склучува договор со обработувач кој што ќе обработува лични податоци во име и за сметка на невладината организација, во најрана фаза треба да биде вклучен офицерот за заштита на личните податоци. На пример, доколку невладината организација склучува договор со сметководствено биро кое ќе пресметува плати и надоместоци во име и за сметка на невладината организација, офицерот треба да се осигура дека сметководственото биро на кое невладината организација планира да му ги довери личните податоци за своите вработени и/или ангажирани лица, е усогласено со прописите за заштита на личните податоци. Во овој случај сметководственото биро како обработувач ќе треба да му демоснстрира на офицерот на невладината организација соодветна документација и мерки кои гарантираат безбедност на податоците и усогласеност со прописите за заштита на личните податоци. Дополнително офицерот треба да биде вклучен при изготвувањето на договорот за услуги кој што ќе го склучат невладината организација и сметководственото биро, за аспектите кои се однесуваат на техничките и организациските мерки за безбедност на податоците, доверливоста и начинот за вршење на контрола/ревизија.

Исто така, во случаите кога вработените во невладината организација, ангажираните лица или волонтерите при своето работење ќе се соочат со дилеми во однос на примената на прописите за заштита на лчичните податоци, истите треба да

имаат можност да му се обратат на офицерот за совет. На пример доколку вработените не се сигурни дали треба да соберат односно обработуваат определена категорија на личен податок или не се сигурни во кој рок собраните лични податоци треба да се избришат или уништат, во тој случај треба за совет да се обратат до офицерот за заштита на личните податоци, кој што пак ќе им даде конкретни насоки или ќе ги упати на соодветната документација поврзана со предметното прашање.

Исто така, офицерот мора да биде консултиран во случаите на нарушување на безбедноста на личните податоци или друг инцидент, за да може ефикасно да помогне во остварувањето на законските обврски на контролорот во ваквите случаи.

Оттука, потребно е повторно да се потенцира дека од клучно значење е офицерот или тимот на офицери за заштита на личните податоци да бидат вклучени уште во најраната можна фаза за сите прашања што се однесуваат на заштитата на личните податоци. Тоа може да се реализира, на пример, со присуство на офицерот на состаноците кога се донесуваат одлуки со импликации за заштита на личните податоци, при што сите релевантни информации мора навремено да му се пренесат, со цел да му се овозможи да даде соодветен совет. Мислењето на офицерот за заштита на личните податоци секогаш мора да се земе предвид. Во случај на несогласување на менаџментот со мислењето, советите и препораките на офицерот се препорачува, да се документираат причините зошто истите не се испочитувани. Покрај ова, важно е офицерот за заштита на личните податоци да се смета за партнер за дискусија во рамките на организацијата и тој да биде дел од релевантните работни групи кои се занимаваат со активности за обработка на лични податоци во рамките на организацијата. Менаџментот никогаш не треба да заборави дека со офицерот за заштита на личните податоци е на иста, партнерска а не спротивна, ривалска страна и дека советите секогаш се во функција на почитување на прописите за заштита на личните податоци. Во секој случај најдобро е да се најде решение кое ќе ги испочитува советите на офицерот, ќе ги земе предвид неговите препораки, а се во правец на демонстрирање на одговорност и отчетност на организацијата, но и функционирање и остварување на нејзините надлежностите во согласност со начелата за заштита на личните податоци.

Онаму каде што е соодветно, контролорот или обработувачот може да развие насоки или процедури за заштита на личните

податоци кои утврдуваат во кои ситуации треба да се консултира офицерот за заштита на личните податоци.

Улогата на офицерот за заштита на личните податоци во проценката на влијанието на заштитата на личните податоци

Кога при користење на нови технологии за некој вид на обработка на лични податоци, која согласно природата, обемот, контекстот и целите на обработката, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица, пред да биде извршена обработката, невладината организација како контролор е должна да изврши проценка на влијанието на предвидените операции во однос на заштитата на личните податоци. Една проценка може да се однесува на серија слични операции на обработка, кои претставуваат слични високи ризици. При вршењето на проценка на влијанието врз заштитата на личните податоци, контролорот е должен да побара совет од офицерот, ако тој е определен.
Вршењето на проценка на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци во случаите определени со закон, од една страна претставува обврска на контролорот, додека од друга страна е една од законски определените задачи на офицерот за заштита на личните податоци кој дава совети во однос на проценката на влијанието на заштитата на личните податоци и го следи извршувањето на проценката онаму каде што е потребно. Во овој случај контролорот треба да побара совет од офицерот за заштита на личните податоци, особено за следните прашања:

- дали да се спроведе проценка на влијанието на заштитата на личните податоци?
- каква методологија да се следи при спроведување на проценката на влијанието на заштитата на личните податоци?
- дали да се изврши проценката на влијанието на заштитата на личните податоци од страна на вработени или преку надворешни соработници?
- кои заштитни мерки (вклучувајќи технички и организациски мерки) да се применуваат за да се ублажат сите ризици за правата и интересите на субјектите на личните податоци?

- дали е правилно извршена проценката на влијанието на заштитата на личните податоци и дали нејзините заклучоци се во согласност со Законот за заштита на личните податоци, односно дали да се продолжи со обработката и кои заштитни мерки да се применуваат?

Доколку контролорот не се согласува со советот што го дава офицерот за заштита на личните податоци, како составен дел од документацијата за проценката на влијанието на заштитата на личните податоци треба да биде и писменото образложение, зошто советот не е земен предвид.

Офицерот може исто така, да предложи контролорот да изврши проценка на влијанието на заштитата на личните податоци за конкретна операција на обработка. Истовремено, треба да им помогне на засегнатите страни за методологијата, да помогне да се оцени квалитетот на проценката на ризикот, да се утврди дали преостанатиот ризик е прифатлив и да развива знаење специфично за контекстот на контролорот на личните податоци.

На пример, офицерот за заштита на личните податоци треба на невладината организација да и предложи проценка на влијанието на заштитата на личните податоци во случаите кога е планирана обработка на лични податоци за ранливи категории на субјекти на лични податоци и обработка на чувствителни податоци или податоци од мошне лична природа. Во овој случај, офицерот треба да предложи проценка на влијанието на заштитата на личните податоци бидејќи се исполнети два од предвидените критериуми кога се смета дека обработката е од висок ризик. Обработката на лични податоци за ранливи категории на субјекти на лични податоци се смета како критериум поради зголемената нерамнотежа на моќта помеѓу субјектите на личните податоци и контролорот на личните податоците, што значи дека поединците не можат лесно да се согласат или да се спротивстават на обработката на нивните податоци или да ги остварат своите права. Ранливите субјекти на лични податоци можат да вклучуваат деца (може да се смета дека не се способни свесно и смислено да се спротивстават или да се согласат за обработката на нивните лични податоци), вработените, поранливи сегменти од населението за кои е потребна посебна заштита (лица со интелектуална попреченост, лица кои бараат азил) и во секој случај кога може да се идентификува нерамнотежа во односот помеѓу положбата на субјектот на личните податоци и контролорот. А вториот критериум: обработка на чувствителни

податоци или податоци од мошне лична природа, исто така може да претставува висок ризик за приватноста бидејќи овде може да бидат вклучени посебни категории на лични податоци или чувствителни податоци на пример, информации за политичките мислења на поединците, сексуална определба на субјекти на лични податоци, како и лични податоци кои се однесуваат на кривични пресуди или казнени осуди.

Следење на усогласеноста, подигање на свеста за заштита на лични податоци и ревизии

Офицерот за заштита на личните податоци има задача да ја следи усогласеноста на Законот за заштита на личните податоци, други засегнати закони кои се однесуваат на заштитата на личните податоци во државата, со политиките на контролорот или обработувачот во однос на заштитата на личните податоци, вклучувајќи распределување на одговорности, подигнување на свеста и обучување на вработените кои што учествуваат во операциите на обработка, како и вршење на ревизии за заштита на личните податоци.

Како дел од должноста за следење на усогласеноста, офицерот особено може да: собира информации за да ги идентификува активностите за обработка, ја анализира и проверува усогласеноста на активностите за обработка и да информира, советува и издава препораки до контролорот или обработувачот. Офицерот треба да биде во тек со промената на секторската легислатива и да се грижи за тековно ажурирање на донесените процедури.

Следењето на усогласеноста не значи дека офицерот е лично одговорен кога има случај на неусогласеност. Законот за заштита на личните податоци јасно уредува дека контролорот е одговорен да спроведува соодветни технички и организациски мерки за да се обезбеди заштита на личните податоци и да биде способен да докаже дека обработката се врши во согласност со законот, а офицерот како важна алка во системот за заштита на личните податоци значително придонесува контролорот да демонстрира отчетност.

Контролорот треба да му овозможи на офицерот неопходен пристап до други услуги, како што се човечки ресурси во организацијата, лицата кои работат на правни работи, ИТ,

безбедност итн., така што офицерот ќе добие суштинска поддршка, придонес и информации од другите сектори.

Исто така, за доследно следење на усогласеноста на офицерот треба да му се обезбеди континуирана обука од областа на заштита на личните податоци, што ќе придонесе за постојано зголемување на нивото на експертиза. Контролорот треба да го поттикне офицерот да учествува на курсеви за обука за заштита на личните податоци и други форми на професионален развој, како што се учество во форуми за приватност, работилници, семинари итн.

Законот за заштита на личните податоци определува листа на минимум работи кои треба да ги врши офицерот. Контролорот може да му додели и други задолженија доколку не постои конфликт на интереси со остварувањето на задачите.

Невладината организација како контролор може на офицерот да му додели задача за одржување на регистар/евиденција на операции за обработка под одговорност на контролорот или обработувачот. Таквата евиденција/регистар на операции на обработка може да се вброи како една од алатките што му овозможуваат на офицерот да ги извршува своите задачи за следење на усогласеноста, информирање и советување на контролорот или обработувачот. Оваа евиденција претставува алатка која му овозможува на контролрот во секое време на барање на Агенцијата за заштита на личните податоци како надзорен орган, да даде преглед за сите активности на обработка на лични податоци кои ги спроведува организацијата. Од тие причини овој регистар/евиденција претставува предуслов за усогласувањето и како таков претставува и делотворна мерка за отчетност.

Понатаму, офицерот има значајна улога во информирањето на вработените за нивните права, обврски кои произлегуваат од прописите за заштита на личните податоци, како и во однос на полесно разбирање на мерките кои треба да ги применуваат за да се обезбеди заштита на личните податоци. Офицерот за заштита на личните податоци има слобода во однос на начините како ќе ги информира и едуцира вработените.

Офицерот понатаму има обврска да врши ревизии/контроли во однос на примената на прописите за заштита на личните податоци. Кои ревизии и на која фреквенција истите ќе се вршат офицерот

определува врз основа на претходно направена анализа, за што прави годишен план за ревизии/контроли.

Во текот на овие ревизии меѓудругото офицерот ќе добие сознанија по однос на тоа кои обуки од областа за заштита на лични податоци се потребни и за кои вработени. Офицерот треба да изготви план за обуки на вработените во кој ќе бидат вклучени темите на обуките кои тој ќе ги испорача на вработените, во кој период како и други предложени обуки на кои треба да се упатат вработените.

Офицерот за заштита на личните податоци како контакт точка

Погоре веќе беше истакната улогата на офицерот како контакт точка помеѓу контролорот и вработените (советување, едукација, ревизија...).

Офицерот за заштита на личните податоци има задача да соработува со Агенцијата за заштита на личните податоци. Офицерот дејствува како контакт точка за Агенцијата во однос на прашањата поврзани со обработката, вклучувајќи ја претходната консултација, како и советување според потребите за сите други прашања. Улогата како контакт точка со Агенцијата исто така се рефлектира и при известувањето за нарушување на безбедноста на податоците.

- Овие задачи се однесуваат на улогата на олеснувач на офицерот за заштита на личните податоци, кој што дејствува како точка за контакт за да го олесни пристапот на надзорниот орган - Агенцијата за заштита на личните податоци, до документите на невладината организација и потребните информации за извршување на задачите на Агенцијата, како и за вршење на истражни, корективни, овластувачки и советодавни функции кои што се нејзини законски утврдени надлежности. Офицерот за заштита на личните податоци е мостот кој што ги поврзува надзорниот орган и невладината организација и офицерот во секое време може ја контактира Агенцијата и да бара совет, консултација, мислење или препорака. Законот за заштита на личните податоци дури предвидува и случаи каде е задолжително офицерот да ја консултира Агенцијата.

Офицерот за заштита на личните податоци исто така претставува контакт точка помеѓу контролорот и субјектите на личните податоци. Имено, субјектите на личните податоци заради остварување на своите права загрантирани со законот за заштита на личните податоци, се обраќаат до контролорот преку офицерот за заштита на личните податоци.

IV.5 ПРАВА НА СУБЈЕКТОТ НА ЛИЧНИТЕ ПОДАТОЦИ

Правата на субјектите на личните податоци беа загарантирани и со претходниот Закон за заштита на личните податоци, но со новиот Закон се прошири лепезата на права кои контролорот односно обработувачот имаат обврска да ги остварат. Новиот закон особено го зајакнува аспектот на транспарентност при обработката на личните податоци кој што треба да се рефлектира не само при собирањето на личните податоци, туку низ целокупниот процес на обработката. Исто така, со новиот закон дел од посточките права на субјектите во однос на обработката на нивните податоци се реформираат и прошируваат, а дел од правата кои се предвидени во новиот закон претставуваат апсолутна новина.

Невладините организации како контролори на лични податоци ќе треба да донесат процедури во кои подетално ќе го разработат начинот на кој што ќе овозможуваат остварување на законски предвидените права на субјектите на личните податоци (на пример изјава за приватност, политика за приватност...) кои ќе треба да бидат јавно објавени односно достапни за субјектите на личните податоци.

Остварувањето на овие права всушност преставува дел од отчетноста на контролорите, односно алатка преку која контролорите ќе демонстрираат усогласеност со прописите за заштита на личните податоци и ќе ја стекнат довербата на субјектите на личните податоци, демонстрирајќи им дека се грижат за нивните податоци и за остварувањето на нивните права, како и дека ќе им помогнат на да го разберат ризикот и предизвиците кои може да произлезат при обработката на нивните податоци.

Со Законот за заштита на личните податоци се гарантираат следните права на субјектите на личните податоци:

1. Транспарентност, што подразбира: транспарентни информации, комуникација и начини на остварување на правата на субјектот на личните податоци

2. Информации и пристап до лични податоци, што се однесува на:

- информациите кои се доставуваат при собирање на лични податоци од субјектот на личните податоци,
- информациите кои се доставуваат кога личните податоци не се добиени од субјектот на личните податоци, и
- правото на пристап на субјектот на личните податоци

3. Исправка и бришење, што вклучува:

- право на исправка,
- право на бришење („право да се биде заборавен“),
- право на ограничување на обработката,
- обврска за известување при исправка или бришење на личните податоци или ограничување на обработката и
- право на преносливост на податоците.

4. Право на приговор и автоматизирано донесување на поединечни одлуки:

- право на приговор,
- автоматско донесување на поединечни одлуки, вклучувајќи и профилирање.

IV.5.1 ТРАНСПАРЕНТНОСТ

Транспарентноста како обврска на контролорот во себе ги апсорбира сите други права на субјектот на личните податоци и претставува појдовна точка за остварување на останатите права.

Транспарентноста го обврзува контролорот да преземе соодветни мерки за обезбедување на сите информации:

- коишто се доставуваат при собирање на личните податоци од субјектот и информации кои што се доставуваат кога личните податоци не се добиени од субјектот на личните

податоци,

- како и на секоја комуникација и сите активности преземени со остварување на правата за пристап, исправка, бришење, преносливост, приговор, автоматско донесување на поединечна одлука вклучувајќи и профилирање и известување на нарушување на безбедноста на личните податоци, поврзани со обработката која се однесува на неговите лични податоци на концизен, транспарентен, разбирлив начин и во лесно достапна форма, со користење на јасен едноставен јазик, особено за информации кои посебно се наменети за дете.

Информациите треба да бидат дадени во писмена форма или со други средства, вклучувајќи каде што е применливо, и по електронски пат.

По барање на субјектот на личните податоци, информациите може да се дадат усно, под услов идентитетот на субјектот да е докажан со други средства.

Транспарентноста како обврска, се рефлектира на три аспекти односно прашања:

- Како се исполнува обврската за обезбедување на информациите до субјектите на личните податоци, поврзани со фер обработка?
- Како контролорите комуницираат со субјектите на личните податоци во врска со остварувањето на нивните права според Законот за заштита на личните податоци? и
- Како контролорите го олеснуваат процесот на остварувањето на правата на субјектите на лични податоци?

Барањата на транспарентност според Законот за заштита на личните податоци се применуваат без оглед на правниот основ според кој се врши обработката, низ целиот животен циклус на обработка, но и во следните фази на циклусот на обработка на податоците:

- пред или на почетокот на циклусот на обработка на податоците, т.е. кога се собираат личните податоци од самиот субјект или се добиваат на друг начин,
- во текот на целиот период на обработка, т.е. при комуникација со субјектите на лични податоци за нивните права и

- во специфични ситуации додека обработката е во тек, на пример кога ќе се случи нарушување на безбедноста на податоците или во случај на настанати промени во обработката.

Контролорот е должен да го олесни остварувањето на правата на субјектот на личните податоци. Во случаи кога целите за кои контролорот обработува лични податоци, не бараат или престанала потребата за натамошна идентификација на субјектот на личните податоци од страна на контролорот, тој не е обврзан да одржува, стекнува или да обработува дополнителни информации за идентификација на субјектот на личните податоци само заради усогласување со закон. Во ваквите случаи, кога контролорот не е во состојба да го идентификува субјектот на личните податоци, соодветно го информира, ако тоа е можно. Во тие случаи, остварувањето на правата за пристап, исправка, бришење, преносливост, приговор, автоматско донесување на поединечна одлука вклучувајќи и профилирање нема да се остваруваат, освен ако субјектот на лични податоци, со цел да го оствари своето право, обезбедува дополнителни информации, овозможувајќи ја неговата идентификација. При ваков случај контролорот нема да одбие да дејствува на барање на субјектот на личните податоци за остварување на неговите права, освен ако контролорот докаже дека не е во состојба да го идентификува субјектот на личните податоци.

Контролорот на барање на субјектот на личните податоци е должен да достави информација за преземените активности, за остварување на правата за пристап, исправка, бришење, преносливост, приговор, автоматско донесување на поединечна одлука вклучувајќи и профилирање и известување за нарушување на безбедноста на личните податоци, до субјектот на личните податоци без непотребно одложување и во секој случај во период од еден месец од денот на приемот на барањето. Доколку е потребно овој рок може да биде продолжен за уште два месеци земајќи ги предвид сложеноста и бројот на барањата. Контролорот го информира субјектот на личните податоци за секое продолжување во рок од еден месец од денот на приемот на барањето, заедно со причината за одложувањето. Кога субјектот поднесува барање во електронска форма, информациите се даваат со користење на електронски средства каде што е можно, освен ако субјектот на личните податоци побара поинаку.

Ако контролорот не презема активности по барањето на субјектот на личните податоци, контролорот го информира субјектот на личните податоци без одложување и најдоцна во рок од еден месец од денот на приемот на барањето, за причините за непреземените активности и за можноста за поднесување на барање до Агенцијата за заштита на личните податоци, како и за можноста за користење на судска заштита согласно закон.

Обезбедената информација кога личните податоци се собираат од субјектот на личните податоци и кога личните податоци не се добиени од субјектот на личните податоци, и секоја комуникација и сите активности преземени за остварување на правата за пристап, исправка, бришење, преносливост, приговор, автоматско донесување на поединечна одлука вклучувајќи и профилирање и известување за нарушување на безбедноста на личните податоци, се овозможуваат без надоместок. Во случај кога барањата од субјектот на личните податоци се очигледно неосновани или прекумерни, особено во однос на нивниот повторувачки карактер, контролорот може да наплати надоместок имајќи ги предвид обемот, сложеноста и времето потребно за обезбедување на информацијата, комуникацијата или постапувањето по барањето, или да одбие да постапи по барањето. Докажувањето на неоснованоста или прекумерниот карактер на барањето паѓа на товар на контролорот.

По исклучок, во случите кога целите за кои контролорот обработува лични податоци, не бараат или престанала потребата за натамошна идентификација на субјектот на личните податоци од страна на контролорот, каде што контролорот има основано сомневање во врска со идентитетот на физичкото лице што го поднесува барањето за остварување на правата за пристап, исправка, бришење, преносливост, приговор, автоматско донесување на поединечна одлука вклучувајќи и профилирање и известување за нарушување на безбедноста на личните податоци, контролорот може да побара доставување на дополнителни информации потребни за утврдување на идентитетот на субјектот на личните податоци.

Во случаите кога субјектот на личните податоци се обидува да го потврди својот идентитет при остварување на неговите права на пристап и контролорот треба да ги направи сите можни напори за да го идентификува. Во овој случај контролорот односно обработувачот може да провери две работи пред да ја исполни обврската да одговори на барањето. Најпрвин, може да се

побара доволно информации да се оцени дали бараните лични податоци се однесуваат на лицето кое го доставува барањето. Целта е да се избегне испраќање на лични податоци за одреден поединец на друго лице, што би се случило како резултат на несреќен случај, небрежност или измама. Клучната работа е дека субјектот на личните податоци мора да биде разумен во своето барање. Контролорот односно обработувачот не треба да бара многу повеќе информации доколку е очигледен идентитетот на лицето кое го поднесува барањето. Ова особено во случај, на пример, доколку тој веќе има релација со физичкото лице. Сепак, контролорот односно обработувачот не треба во секоја пригода да претпоставува дека лицето кое го поднесува барањето е она кое тврди дека е. Во некои случаи, разумно е да се побара од лицето кое го поднесува барањето да го потврди идентитетот пред да му се достави информацијата.

Нивото на проверки на контролорот односно обработувачот треба да зависи и од можните ризици и непријатности кои би можеле да му се предизвикаат на поединецот како резултат на несоодветно откривање на информацијата. Втор механизам кој контролорот, односно обработувачот има право да го користи, е пред да одговори на барањето информации, да побара информации кои разумно би биле потребни за да се пронајдат личните податоци на кои се однесува барањето. Сè додека не ја добие таа информација, контролорот односно обработувачот нема обврска да одговори на барањето. Во некои случаи е тешко да се вратат и организираат личните податоци, но сепак, не би било прифатливо контролорот односно обработувачот да го оддолжи пристапот на субјектот поради ова, освен доколку е разумна неопходноста да се побараат повеќе информации пред да се пронајде односниот податок.

Правото да се биде информиран ја опфаќа обврската да се обезбеди „правична информација за обработката“ посебно преку изјавата/политиката за приватност. Тоа ја потенцира потребата за транспарентност во врска со прашањето како да се користат личните податоци. Ова го обврзува контролорот да пропише процедура и механизми за остварување на правата на субјектите на лични податоци, вклучувајќи и начин за поднесување на електронски барања.

Сите лични податоци кои се собрани, користени, консултирани или обработувани на друг начин и до кој степен личните податоци се или ќе бидат обработени, треба да бидат

објаснети во Политиката на приватност, односно изјавата за приватност на контролорот. Еден од модулите за остварување на транспарентност е потребните информации и комуникацијата во врска со обработката на тие лични податоци да бидат лесно достапни, лесно разбирливи, концизни, јасни, со јазик и фрази кои вообичаено се користат.

Условот, информациите да се разбирливи значи дека истите треба да ги разбере просечен поединец од субјектите на лични податоци за кои се наменети информациите. Разбирливоста е тесно поврзана со барањето да се користи јасен и обичен јазик, односно информациите треба да бидат изложени на начин што може лесно да се разберат. Тоа значи дека информациите наменети за субјектот на лични податоци не треба да содржат претерано легалистички, технички или специјалистички јазик или терминологија.

Во случаите кога информациите се преведени на еден или повеќе други јазици, контролорот треба да обезбеди преводите да се точни, а фразеологијата и синтаксата имаат смисла на јазикот на кој се преведени, така што преведот да не мора да се дешифрира или преиспитува.

Лесната достапност, како елемент на транспарентноста значи дека пристапот до политиката на приватност, односно изјавата на приватност е едноставен, а субјектот на податоци не треба да ги бара/пребарува информациите, односно треба веднаш да му биде јасно каде и како може на овие информации да им пристапи. Објавената политика на приватност, односно изјавата на приватност треба да му овозможи на субјектот на личните податоци лесно да се движи низ конкретниот дел од овие документи до кој сака да пристапи, и да не мора да пребарува големи текстови, во потрага по одредени теми.

Информациите кои се доставуваат до субјектите при собирање на нивните лични податоци и информациите кои што се доставуваат кога личните податоци не се добиени од субјектот на личните податоци, може да се обезбедат во комбинација со стандардизирани икони, со цел да им даде лесно видлив, разбирлив и јасно читлив начин за да се обезбеди јасен преглед на целта на обработката. Ако стандардизираните икони се претставени во електронска форма тие треба да бидат машинско читливи (читливи преку софтверски апликации).

Машински читливи означува формат на датотека структурирана така што софтверските апликации можат лесно да ги идентификуваат, препознаат и извлечат специфичните податоци, вклучително и индивидуални изјави на фактите и нивната внатрешна структура.

Во дигиталниот контекст, со оглед на обемот на информации што се потребни за да се обезбедат од субјектот на личните податоците, контролорите може да користат комбинирани методи за да обезбедат транспарентност.

На пример во случаите кога личните податоци ги внесува самиот субјект на лични податоци преку веб форма, информациите може да бидат дадени со помош на контекстуални пораки (pop up) или да се појавува директен линк кој води до потребните информации.

Во случите кога транспарентноста се обезбедува со објавување на изјава/политика за приватност на веб страницата на контролорот, се препорачува слоевита изјава, односно политика. Како добра пракса е дизајнот односно изгледот на првиот слој на изјавата/политиката да биде таков што субјектот на личните податоци ќе добие јасен преглед на информациите кои му се достапни, а се однесуваат на обработката на неговите лични податоци, како и приказ каде може да се најдат подетални информации во рамки на слоевите на изјавата/политиката. ,,Првиот слој“ генерално треба да ги пренесе најважните информации (имено податоците за целите на обработката, идентитетот на контролорот и постоењето на правата на субјектот на податоците, заедно со информации за најголемите ризици за конкретната обработка), но и да го задржи вниманието на субјектот на личните податоци. Практично преку ,,првиот слој“ од изјавата/политиката субјектот на личните податоци остварува примарен контакт со контролорот, и од таа причина истиот игра важна улога во стекнувањето на првиот впечаток на субјектот на личните податоци по однос на прашањето колку и како контролорот се грижи за неговите лични податоци.

Исто така, контролорот има обврска да го обезбеди правото на транспарентност и во случаи кога обработката не е автоматизирана (во недигитална околина), на пример преку давање објаснувања при остварување на телефонски повик со субјектот на личните податоци во случаи кога се врши продажба преку телефон.

На пример, кога се склучуваат договори по пошта, во функција на остварување на транспарентноста може да се достават писмени објаснувања, летоци, информации во договорна документација кои се однесуваат на правата на субјектите на личните податоци. Понатаму, кога се користи паметна технологија без екран/ IoT околина, на пример аналитика за следење на Wi-Fi, може да се користат QR кодови, гласовни сигнали, видеа вклучени во дигитални упатства за поставување, писмени информации на паметниот уред, пораки испратени преку СМС или е-пошта.

Исто така, во случај кога се врши видео надзор на јавни површини согласно закон, транспарентноста се остварува преку поставување на информативни табли во кои се содржани потребните информации.

Контролорот треба редовно да ја ажурира политиката/изјавата за приватност во случаите кога има значајни промени во однос на податоците на контролорот (пр.промена на седиште, контакт адреса, телефон...), промена во однос на тоа како субјектите на личните податоци можат да ги остварат своите права, промена во природата на обработката (на пр. зголемување на категориите на корисници или планиран пренос во трета земја). На пример доколку постои промена која може да не биде фундаментална во однос на операција за обработка, но која може да биде релевантна и да влијае врз субјектот на податоците, во тој случај таа информација треба да се достави до субјектот на личните податоци пред да биде направена промената.

Известувањето кога постојат крупни промени треба секогаш да се соопштува по пат на соодветен модалитет (на пример, е-пошта, писмо на хартија, pop up прозорци на веб-страница или друго), односно модалитет кој ефективно ќе го привлече вниманието на субјектот на податоците кон самото известување за промената (на пример: специјално известување за направените промени, а не да биде пратено заедно со содржина за директен маркетинг).

Редовното ажурирање на изјавата/политиката на приватност, а особено соодветниот начин на правење достапна на истата, како елемент на транспарентноста овозможува точни, вистинити и навремени информации за субјектите на личните податоци и придонесува за стекнување или задржување на нивната доверба. Редовното ажурирање е важен елемент и при демонстрирањето отчетност.

IV.5.2 ИНФОРМАЦИИ И ПРИСТАП ДО ЛИЧНИ ПОДАТОЦИ

Правото на информираност и пристап, согласно прописите за заштита на личните податоци, субјектите на лични податоци можат да го остварат во три случаи: информирање при самото собирање на личните податоци, информирање во разумен рок по добивањето на личните податоци (најцоцна во рок од еден месец) кога личните податоци не се добиени од субјектот на личните податоци, и информирање по поднесено барање за пристап од страна на субјектот.

Кога личните податоци се собираат од субјектот на личните податоци, контролорот во моментот на собирањето на личните податоци, на субјектот му ги обезбедува следните информации:

- идентитетот и контакт податоците на контролорот и податоци за неговиот овластен претставник;
- контакт податоци за офицерот за заштита на личните податоци;
- целите на обработката за коишто личните податоци се наменети, како и правната основа за обработката;
- легитимните интереси што ги спроведува контролорот или трето лице кога 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 коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете;
- корисниците или категориите на корисници на личните податоци, доколку ги има;
- намерата дека контролорот ќе пренесува лични податоци во трета земја или меѓународна организација, како и во други случаи на пренос, повикување на соодветните или прифатените заштитни мерки и начинот за добивање на копија од нив или информации каде истите се достапни.

Покрај наведените информации, контролорот во моментот на собирањето на личните податоци, на субјектот му ги дава следните дополнителни информации кои се неопходни за обезбедување на правична и транспарентна обработка:

- временскиот период за кој ќе се чуваат личните податоци, а ако тоа е невозможно, критериумите што се користат за одредување на тој период;
- постоењето на право да се бара од страна на контролорот пристап, исправка или бришење на личните податоци или ограничување на обработката на личните податоци кои се однесуваат на субјектот на личните податоци, или право на приговор за обработката, како и право на преносливост на податоците;
- постоењето на правото за повлекување на согласноста во секое време, без да се влијае на законитоста на обработката која била заснована на согласноста пред истата да биде повлечена, кога обработката се врши врз основа на дадена согласност за една или повеќе конкретни цели, или врз основа на дадена согласност за обработка на посебни категории на лични податоци за една или повеќе конкретни цели;
- правото на поднесување барање до Агенцијата за заштита на личните податоци согласно со закон;
- информација дали давањето на личните податоци е законска или договорна обврска или услов кој е потребен за склучување на договор, како и дали субјектот има обврска да ги даде личните податоци и можните последици ако овие податоци не бидат дадени;
- за постоењето на автоматизиран процес на одлучување, вклучувајќи го и профилирањето што предизвикува правни последици за субјектот или на сличен начин влијае на него, за автоматското донесување на одлуки вклучувајќи и профилирање врз основа на посебни категории на лични податоци за определени цели утврдени во законот за заштита на личните податоци и најмалку во оние случаи, кога е вклучена значајна информација за логички поврзаните процеси на обработка, како и значењето и предвидените последици од таквата обработка за субјектот на личните податоци.

Кога контролорот има намера и понатаму да обработува лични податоци за цел различна од онаа за која се собрани личните податоци, контролорот пред понатамошната обработка, на субјектот му ги обезбедува информации за другата цел и сите други потребни информации.

Контролорот во моментот кога се собираат податоците од субјектот не ги обезбедува претходно наведените информации, само ако веќе располага со информациите. Притоа, секоја понатамошна обработка на податоците за цели поинакви од оние за кои веќе биле собрани, е возможна само по споделување на информацијата до субјектот на личните податоци пред да дојде до натамошната обработка. Ова практично значи дека субјектот треба секогаш да биде информиран за обработката на своите лични податоци.

Кога пак личните податоци не се добиени од субјектот на личните податоци, контролорот му ги обезбедува следните информации:

- идентитетот и контакт податоците на контролорот и податоци за неговиот овластен претставник;
- контакт податоци за офицерот за заштита на личните податоци;
- целите на обработката за коишто личните податоци се наменети, како и правната основа за обработката;
- категориите на лични податоци кои се обработуваат;
- корисниците или категориите на корисници на личните податоци, доколку ги има;
- намерата на контролорот да пренесе лични податоци во трета земја или меѓународна организација, како и во случај на пренос на лични податоци кој подлежи на соодветни заштитни мерки, пренос врз основа за задолжителни корпоративни правила, пренос потребен заради извршување на договор помеѓу субјектот и контролорот или преддоговрни мерки преземени на барање на субјектот, повикување на соодветните или прифатените заштитни мерки и начинот за добивање на копија од нив или информации каде истите се достапни.

Покрај овие информации, контролорот на субјектот на личните податоци му ги дава и следните дополнителни информации кои се неопходни за обезбедување на правична и транспарентна обработка на неговите лични податоци:

- податок за временскиот период за кој ќе се чуваат личните податоци, а ако тоа не е возможно, критериумите што се користат за одредување на тој период;

- податок за легитимните интереси што ги спроведува контролорот или трето лице кога обработката се врши 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 субјектите коишто бараат заштита на личните податоци, особено кога субјектот е дете;
- информација за постоењето на право да се бара од страна на контролорот пристап, исправка или бришење на личните податоци или ограничување на обработката на личните податоци кои се однесуваат на субјектот на личните податоци, или право на приговор за обработката, како и право на преносливост на податоците;
- информација за постоењето на правото за повлекување на согласноста во секое време, без да се влијае на законитоста на обработката која била заснована на согласноста пред истата да биде повлечена, кога обработката се врши врз основа на дадена согласност за една или повеќе конкретни цели, или врз основа на дадена согласност за обработка на посебни категории на лични податоци за една или повеќе конкретни цели;
- информација за правото на поднесување барање до Агенцијата за заштита на личните податоци;
- изворот на личните податоци и доколку е применливо, дали податоците се од јавно достапни извори; информација за постоењето на автоматизиран процес на одлучување, вклучувајќи го и профилирањето што предизвикува правни последици за субјектот или на сличен начин влијае на него, за автоматско донесување на одлуки вклучувајќи и профилирање врз основа на посебни категории на лични податоци за определени цели утврдени во Законот за заштита на личните податоци, и најмалку во оние случаи, кога е вклучена значајна информација за логиката на обработката, како и за значењето и предвидените последици од таквата обработка за субјектот на личните податоци.

Сите овие информации контролорот треба да ги обезбеди во разумен рок по добивањето на личните податоци, а најдоцна во рок од еден месец, имајќи ги предвид посебните околности под кои личните податоци се обработуваат. Ако личните податоци се користат за комуникација со субјектот на личните податоци,

најдоцна при остварување на првиот контакт со истиот или, ако е предвидено откривање на друг примач, најдоцна до моментот кога личните податоци се откриени за прв пат.

Кога контролорот има намера и понатаму да обработува лични податоци за цел различна од онаа за која се собрани личните податоци, пред понатамошната обработка, на субјектот на личните податоци треба да му обезбеди информации за другата цел и сите други потребни информации.

Обврската за давање на претходно наведените информации не се применува ако:

- субјектот на личните податоци веќе располага со информациите,
- ако обезбедувањето на таквите информации е невозможно или бара несразмерно големи напори, особено за обработка на податоци за цели на архивирање од јавен интерес, или за научни или историски истражувања или за статистички цели, кои се предмет на услови и заштитни мерки кои обезбедуваат примена на технички и организациски мерки, особено во однос на почитувањето на начелото на обработка на минимален обем на податоци,
- или доколку постои веројатност дека обврската за обезбедување на информациите на субјектот кога личните податоци не се добиени од него, ќе го направи невозможно или сериозно ќе го отежне постигнувањето на целите на таа обработка. Во овие случаи контролорот презема соодветни мерки за заштита на правата, слободите и легитимните интереси на субјектот на личните податоци, вклучувајќи и обезбедување на јавен пристап до информациите.
- добивањето или откривањето е јасно дозволено со закон во кој се предвидуваат соодветни мерки за заштита на легитимните интереси на субјектот на личните податоци или
- личните податоци мора да останат доверливи во согласност со обврската за деловна тајна, што се регулира со закон, вклучувајќи и законска обврска за доверливост.

Во случај кога обврската за давање на потребните информации не се применува од причина што обезбедувањето на таквите информации е невозможно или бара несразмерно голем напор, битно е да се напомене дека во овој случај невозможноста или непропорционалниот напор мора да бидат директно поврзани со

фактот дека личните податоци се добиени од страна на субјектот на личните податоци.
И во овие ситуации целосно се применува начелото дека сета натамошна обработка на податоците за цели различни од онаа за која истите се веќе собрани, е возможна само откога информацијата ќе се достави на субјектот пред да дојде до натамошна обработка.
Информациите за обработката на личните податоци кои ги обезбедува контролорот односно обработувачот мора да бидат: концизни, транспарентни, разбирливи и лесно достапни; напишани на јасен и разбирлив начин, особено ако се однесуваат на дете, и бесплатни.

ПРАВОТО НА ПРИСТАП му овозможува на субјектот на личните податоци да добие информација за видот на обработуваните податоци за него и да провери дали таа информација е точна и ажурирана.

Согласно правото на пристап на субјектот на личните податоци, истиот има право да добие потврда од контролорот дали се обработуваат негови лични податоци и доколку се обработуваат, да добие пристап до личните податоци и до следните информации:

- целите на обработката;
- категориите на лични податоци кои се обработуваат;
- корисниците или категориите на 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, а ако тоа не е возможно, критериумите што се користат за одредување на тој период;
- постоењето на 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;
- правото на поднесување на барање до Агенцијата за заштита на личните податоци доколку смета дека обработката на неговите лични податоци, ги прекршува одредбите од Законот за заштита на личните податоци;

- кога личните податоци не се собираат од субјектот на личните податоци, сите достапни информации за нивниот извор;
- постоењето на автоматизиран процес на одлучување, вклучувајќи го и профилирањето што предизвикува правни последици за субјектот или на сличен начин влијае на него, за автоматско донесување на одлуки вклучувајќи и профилирање врз основа на посебни категории на лични податоци за определени цели утврдени во Законот за заштита на личните податоци, и најмалку во оние случаи, кога е вклучена значајна информација за логиката на обработката, како и значењето и предвидените последици од таквата обработка за субјектот на личните податоци.

Кога личните податоци се пренесуваат во трета земја или меѓународна организација, субјектот на личните податоци има право да биде информиран за соодветните заштитни мерки кои се однесуваат на преносот на лични податоци кој подлежи на соодветни заштитни мерки.

Контролорот е должен да обезбеди копија од личните податоци што се обработуваат. За сите дополнителни копии побарани од субјектот, контролорот донесува одлука дали ќе наплати надоместок. Доколку контролорот наплати надоместок, висината на истиот зависи од обемот, сложеноста и времето потребно за обезбедување на копиите. Ако субјектот на личните податоци поднесе барање по електронски пат, информациите ќе му бидат обезбедени на вообичаен начин кој се користи во случај на електронска форма. Треба да се истакне дека правото да се добие копија не смее никако да влијае негативно врз правата и слободите на другите физички лица.

Согласно правото на пристап на субјектот на личните податоци, субјектот има право да бара пристап само до своите лични податоци, но не и за други лица (освен доколку не постапува во името на тоа лице согласно закон). Постапката за остварување на правото на пристап треба да биде интегрирана во политиката/изјавата за приватност. Со оваа постапка важно е да се обезбеди дека личните податоци што се откриени како одговор на остварувањето на правото на пристап се однесуваат само на субјектот на личните податоци кој побарал такви податоци. Исто така е важно да се отстранат информации кои не се лични податоци. По приемот на барањето за пристап, најпрвин

контролорот треба да го идентификува субјектот. Контролорот може да бара дополнителни информации за проверка на идентитетот на субјектот со користење на разумни средства, особено во контекст на онлајн услугите. На пример, како средства за проверка на идентитетот може да се користат онлајн идентификатори, електронски потписи или други механизми. Контролорот треба да биде сигурен дека точно ја разбрал природата на барањето, односно која информација се бара од субјектот на личните податоци и дали контролорот ја има таа информација. Исто така, важно е да се утврди дали бараната информација потпаѓа под дефиницијата за лични податоци. Понатаму, потребно е да се преземат мерки за отстранување на информациите кои ќе се даваат како податоци од друго лице кои не може и не треба да бидат предмет на барањето за пристап. Дотолку повеќе, треба да се избере соодветна форма за да се овозможи правото на пристап. На пример, кога субјектот на личните податоци го доставува барањето по електронски пат, информацијата мора да биде дадена во најчесто користена електронска форма.

Добра пракса претставува доколку контролорот е во можност, да обезбеди пристап на далечина преку безбеден систем кој му дава на субјектот на личните податоци директен пристап до неговите лични податоци. Онаму каде се обработува голема количина на информации, се препорачува субјектот во неговото барање да го конкретизира обемот на информации до кои бара пристап или конкретните активности на кои се однесува барањето. По правило, одговорот на барањето за пристап се обезбедува бесплатно, но контролорот го задржува правото да наплати минимален надомест кога барањата се неосновани и прекумерни.

Контролорот мора да се придржува кон барањето на субјектот на личните податоци и да го исполни во целост, освен доколку не постојат рестриктивни законски средства кои го ограничуваат правото на пристап.

IV.5.3 ИСПРАВКА И БРИШЕЊЕ

Правото на исправка подразбира дека субјектот на личните податоци има право да побара и да добие од контролорот, исправка на неговите неточни лични податоци. Притоа, оваа обврска контролорот треба да ја исполни во рок од 15 дена од денот на поднесување на барањето. Земајќи ги предвид целите

на обработката, субјектот има право да ги дополни нецелосните лични податоци, со давање на дополнителна изјава.

Едно од основните начела на обработка е личните податоци да бидат точни и ажурирани. Од една страна, ажурирањето на податоците е обврска на контролорите, а од друга страна, ова право на субјектот на личните податоци е утврдено со закон.

Постапката на исправка, односно ажурирање на личните податоци треба да биде детално пропишана во интерна процедура на контролорот, а изјавата/политиката на приватност треба да содржи информација на кој начин субјектот на личните податоци може да го оствари ова право.

Во зависност од политиките за обработка на лични податоци на контролорот, на определен период, согласно природата и целта за која се користат тие податоци, контролорите треба да ја проверуваат точноста на личните податоци и да преземат мерки за нивно ажурирање.

Треба да се има предвид дека неточните и неажурираните лични податоци на субјектот на кој се однесуваат, може во определени ситуации да му нанесат штета. Субјектот на личните податоци вообичаено станува свесен за неточните информации за него кога ќе го оствари своето право на пристап, но неретко и во случаи кога нема да добие опеделена услуга. Субјектот на личните податоци може да го оствари своето право на исправка со испраќање на писмено барање до контролорот, барајќи исправка на неточните или нецелосните лични податоци или пак, може да му ги достави на контролорот податоците кои треба да се изменат. Контролорот мора да ги исправи овие податоци без непотребно одложување. Во случај контролорот кога нема да изврши ажурирање на личните податоци или субјектот на личните податоци да не е задоволен од одговорот или пак ажурирањето не е целосно, субјектот има право да поднесе барање до Агенцијата за заштита на личните податоци.

Правото на бришење („право да се биде заборавен“) претставува новина во Законот за заштита на личните податоци. Правниот концепт на „правото да се биде заборавен“ е израз на намерата на законодавецот да го зајакне правото на субјектот на личните податоци, овозможувајќи му да ја контролира обработката на личните податоци под јасно дефинирани услови.

Ова право се остварува само кога обработката на личните податоци се врши автоматизирано.

Правото на бришење („право да се биде заборавен“) му дава право на субјектот на личните податоци да побара од контролорот да ги избрише неговите лични податоци при што контролорот има обврска да ги избрише личните податоци во рок од 30 дена од денот на поднесување на барањето за бришење, но само доколку е исполнет еден од следните услови:

1. личните податоци повеќе не се потребни за целите за кои биле собрани или обработени на друг начин;

2. субјектот на личните податоци ја повлекува својата согласност врз која се заснова законитата обработка на податоците за една или повеќе конкретни цели и кога обработката се врши врз основа на дадена изречна согласност на субјектот на лични податоци за обработка на посебни категории на лични податоци за една или повеќе конкретни цели, и ако не постои друга законска основа за обработка;

3. субјектот на личните податоци поднесе приговор на обработката врз основа на конкретна ситуација поврзана со него кога извршената обработка е потребна за извршување на 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 коишто бараат заштита на личните податоци, особено кога субјектот е дете, при што не постојат преовладувачки легитимни цели за обработката, или субјектот поднесе приговор на обработката на неговите лични податоци за цели на директен маркетинг, кој вклучува и профилирање до оној степен до кој истото е поврзано со директниот маркетинг.

4. личните податоци биле незаконски обработени;

5. личните податоци треба да бидат избришани со цел почитување на обврска утврдена со закон која се однесува на контролорот;

6. личните податоци биле собрани во врска со понудата на услуги на информатичко општество, во случај кога субјектот на лични податоци има дадено согласност кога бил на возраст под 14 години (или таквата согласност е дадена или дозволена

од законскиот застапник на детето) за обработка на неговите лични податоци за една или повеќе конкретни цели, во врска со директното нудење на услуги на информатичкото општество на деца.

Според првиот основ субјектот може да поднесе барање за бришење кога личните податоци повеќе не се потребни за целите за кои биле собрани или обработени на друг начин. На пример субјектот може да поднесе барање за бришење на неговите лични податоци според овој основ до компанијата во која што повеќе не работи, а неговите контакт податоци се објавени на веб страницата на компанијата. Исто така, субјектот на личните податоци може да поднесе барање за бришење на содржина кога личните информации се очигледно неточни или застарени, на пример бришење од јавен телефонски именик, на телефонски број кој субјектот веќе не го користи.

Во случај кога субјектот ја повлекол согласноста за употреба на неговите лични податоци кои биле објавени на пример на одредена веб-страница каде се објавуваат различни огласи, субјектот на личните податоци може да побара бришење на неговите податоци од веб операторот.

Според третиот основ, право да побара бришење кога субјектот на податоците го искористил своето право да се спротивстави на обработката на неговите лични податоци, субјектот може на пример од провајдерот/пребарувачот да побара да избрише лични податоци што се однесуваат на него, каде што тој се спротивставува на обработката и каде не постојат преовладувачки легитимни основи за обработка од страна на контролорот на податоци. Товарот на докажување, паѓа на контролорот, кој треба да демонстрира легитимна основа за обработката. Како резултат на ова, кога провајдерот/пребарувачот прима барање да се отстранат личните податоци, ќе мора да ги избрише личните податоци, освен ако не може да демонстрира преовладување на легитимен основ, за понатамошно постоење на специфичниот резултат од пребарувањето, кој ги надминува интересите, правата и слободите на субјектот на личните податоци. Всушност, при остварувањето на правото на бришење, ќе треба да се направи баланс помеѓу причините поврзани со конкретната состојба на субјектот на личните податоци и легитимните основи на провајдерот/пребарувачот, односно рамнотежа помеѓу заштитата на приватноста и интересите на корисниците на интернет во пристапот до информациите. Според Работната група 29 во овој

случај релевантни се следните критериуми за бришење согласно овој основ:

- улогата на субјектот на личните податоци во јавниот живот (дали се работи за јавна личност);
- дали информациите за кои станува збор не се поврзани со неговиот професионален живот и влијаат на неговата приватност;
- дали информациите претставуваат говор на омраза, клевета или слични прекршоци во областа на изразување против него согласно судска наредба;
- информациите јасно го одразуваат личното мислење на поединецот и веројатнно не се потврдени факти;
- податоците се однесуваат на релативно помало кривично дело што се случило многу одамна и предизвикува предрасуди за субјектот на личните податоци.

Во овој поглед, конкретната состојба во која се наоѓа субјектот на личните податоци ќе биде во основа на барањето за бришење (на пример, ако резултатот од пребарувањето создава штета на субјектот на личните податоци кога аплицира за работа или го поткопува неговиот углед во неговиот личен живот) и ќе бидат земени предвид при правењето баланс помеѓу личните права и правото на информации, покрај класичните критериуми за постапување со барања за бришење.

Согласно четвртиот основ субјектот на личните податоци може да поднесе барање за бришење во случаите кога личните податоци биле назаконски обработени. На пример во случај кога објавување на одредени лични информации е експлицитно забрането со судска наредба, а контролорот ги објави на интернет или на својат веб страница.

Петтиот основ му дава право на субјектот на личните податоци да поднесе барање за бришење кога личните податоци треба да бидат избришани заради почитување на законска обврска на контролорот, на пример, субјектот може да побара од провајдерот/пребарувачот да избрише еден или повеќе резултати од пребарувањето доколку личните податоци треба да бидат избришани во согласност со законската обврска на контролорот во случај кога поради измена на закон според кој постапува контролорот истиот повеќе нема основ да обработува определени категории на лични податоци.

Шестиот основ се однесува на правото на поднесување барање да се отстранат личните податоци кога се собрани во врска со понудата на услуги од информатичко општество на дете (лице на возраст до 14 години). Според овој основ, субјектот може да побара од провајдерот/пребарувачот да избрише еден или повеќе резултати ако се собрани лични податоци во врска со понудата на услуги на информатичко општество на дете. На пример може да се побара бришење на лични податоци кои биле дадени од страна на дете за симнување и вклучување во некоја он лајн игра.

Кога контролорот ги објавил јавно личните податоци и е должен да ги избрише личните податоци доколку е исполнет најмалку еден од шесте претходно наведени услови, тогаш контролорот презема дејствија, вклучувајќи технички мерки за да ги извести другите контролори кои ги обработуваат личните податоци дека субјектот побарал бришење на сите линкови или копии или репродукции на личните податоци од страна на тие контролори, земајќи ги предвид достапната технологија и трошоците на спроведувањето.

Наведеното бришење на личните податоци според наведените начин и околности и известувањето на другите контролори се применуваат до оној степен до кој обработката е неопходна:

1. за остварувањето на правото на слобода на изразување и информирање;

2. за усогласување со законска обврска која бара обработка според закон што се применува во однос на контролорот, или за извршување на работи од јавен интерес или при вршење на јавно овластување утврдено со закон доделено на контролорот;

3. од причини од јавен интерес во областа на јавното здравство, при што се обработуваат посебни категории на лични податоци кога обработката е неопходна за целите на превентивна или трудова медицина, за проценка на работоспособноста на вработениот, медицинска дијагноза, обезбедување на здравствена или социјална нега или третман или за целите на управување со услугите и системите за здравствена или социјална заштита, врз основа на закон или во согласност со здравствениот работник во кој предмет се условите и заштитните мерки неопходни за заштита на суштинските интереси на субјектот на личните податоци или на друго физичко лице, кога субјектот на личните податоци физички или правно не е во можност да ја даде

својата согласност; и кога обработката е неопходна за целите од јавен интерес во областа на јавното здравство, како што се заштита против сериозни прекугранични закани за здравјето или обезбедување на високи стандарди за квалитет и безбедност на здравствената заштита и лековите или медицинските помагала, врз основа на закон, во кој се предвидени соодветни и конкретни мерки за заштита на правата и слободите на субјектот на личните податоци, особено заштита на деловна тајна.

4. за целите на архивирање од јавен интерес, за цели на научни или историски истражувања или за статистички цели, во случај кога обработката се врши за овие цели при што контролорот е должен да примени соодветни заштитни мерки за правата и слободите на субјектот на личните податоци во согласност со закон, доколку постои веројатност правото субјектот да побара од контролорот да ги избрише неговите лични податоци при што контролорот има обврска да ги избрише личните податоци во рок од 30 дена од денот на поднесување на барањето за бришење да се направи невозможно или сериозно да го отежне постигнувањето на целите на таа обработка.

Заштитните мерки кои контролорот треба да ги примени вклучуваат применување на технички и организациски мерки, особено во однос на почитувањето на начелото на обработка на минимален обем на податоци. Овие мерки може да вклучуваат псевдонимизација под услов, наведените цели да може да се постигнат на овој начин. Кога наведените цели може да се постигнат преку понатамошна обработка, која што не дозволува или повеќе не дозволува идентификација на субјектите на лични податоци, тие цели се постигнати на овој начин и

5. за воспоставување, остварување или одбрана на барања засновани на закон.

Поради бројните барања и критериуми кои треба да се земат предвид при задоволување на правото на субјектот на личните податоци на бришење „правото да се биде заборавен“ за секој случај треба да се третира поединечно. Добра практика е да се користи претходно подготвена методологија усогласена со активноста на односниот контролор, како одраз на неговото специфично искуство и технолошки способности во заштитата на личните податоци на поединците. Наоѓањето на балансирана заштита зависи од повеќе кумулативни фактори: природата на засегнатата информација; чувствителноста на информацијата во поглед на приватноста на субјектот на личните податоци;

интересот на јавноста да ја добие информацијата и улогата на засегнатото лице во јавниот живот.

Право на ограничување на обработката подразбира дека субјектот на личните податоци има право да побара ограничување на обработката од контролорот, ако е исполнет еден од следните услови:

1. точноста на личните податоци се оспорува од субјектот на личните податоци, за период кој му овозможува на контролорот да ја провери точноста на личните податоци;
2. обработката е незаконска и субјектот на личните податоци се спротивставува на бришењето на личните податоци, при што наместо тоа бара ограничување на нивната употреба;
3. за целите на обработка, контролорот нема повеќе потреба од личните податоци, но субјектот на личните податоци ги бара за воспоставување, остварување или одбрана на неговите правни барања;
4. субјектот на личните податоци се спротивставува на обработката, кога истата е потребна за извршување на работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон, кога 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 коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете, вклучувајќи и профилирање засновано на овие одредби (контролорот не може повеќе да врши обработка на личните податоци, освен ако докаже дека постојат релевантни легитимни интереси за обработка, кои преовладуваат над интересите, правата и слободите на субјектот на личните податоци, или за воспоставување, остварување или одбрана на неговите правни барања), во очекување на верификација дали легитимните интереси на контролорот преовладуваат над интересите на субјектот.

Кога обработката е ограничена според претходно наведните услови, таквите лични податоци може да се обработуваат, само со согласност на субјектот на личните податоци со исклучок на нивното чување, или за воспоставување, остварување или одбрана на неговите правни барања или за заштита на правата на друго физичко или правно лице или поради важни причини од јавен интерес.

Кога субјектот на личните податоци го остварил правото на ограничување на обработката согласно претходно наведените услови, тогаш контролорот го информира пред да престане ограничувањето на обработката.

Секој контролор мора да ги прегледа личните податоци кои ги обработува, за да направи проценка на околностите под кои дошло до остварување на овие права и да го извести субјектот на личните податоци за ова.

Обврската за известување при исправка или бришење на личните податоци или ограничување на обработката подразбира дека контролорот е должен да ги пријавува сите исправки или бришења на личните податоци или ограничувања на обработката извршени заради остварување на правотот на исправка, правото на бришење (право да се биде заборавен) и правото на ограничување на обработката, за секој корисник на кого личните податоци биле откриени, освен ако тоа е невозможно или бара несразмерно големи напори. Ако субјектот на личните податоци побара, тогаш контролорот го информира за тие корисници.

Ова право подразбира да се извести субјектот за личните податоци кога трети лица добиле податоци кои подоцна биле коригирани или избришани или обработката била ограничена по барање на субјектот. Во случај на такво барање на субјектот, им се дава информација за корисниците на таквите податоци. На субјектот исто така мора да му се даде информација кога е донесена одлука за откажување на ограничувањата кои се однесуваат на обработувањето на личните податоци.

Правото на преносливост на податоците е ново право кое е тесно поврзано со правото на пристап, и нормирањето на истото е резултат на интензивниот развој на технологиите. Бидејќи ова право овозможува директен пренос на лични податоци од еден контролор на друг, правото на преносливост на податоци е исто така важна алатка што ќе го поддржи слободниот проток на лични податоци и ќе ја поттикне конкуренцијата помеѓу контролорите. Исто така ќе го олесни префрлувањето помеѓу различни даватели на услуги и затоа ќе го поттикне развојот на нови услуги во контекст на дигиталната стратегија за единствен пазар.

Правото на преносливост на податоците означува дека субјектот на личните податоци има право да ги добие неговите лични податоци, а кои тој ги има дадено на контролорот во структуриран, вообичаено користен, машински читлив формат при што има право да ги пренесе тие податоци на друг контролор без попречување од страна на контролорот на кого личните податоци се дадени, ако:

1.обработката е заснована врз основа на согласност која ја дал субјектот на лични податоци за обработка на неговите лични податоци за една или повеќе конкретни цели или субјектот дал изречна согласност за обработка на посебни категории на лични податоци за една или повеќе конкретни цели, освен кога со закон е предвидено дека забраната за обработка на посебни категории на лични податоци за обработка на такви податоци не може да се отповика од субјектот на личните податоци, или обработката е потребна за исполнување на договор каде 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 и

2. обработката се врши на автоматизиран начин.

При остварувањето на правото на преносливост на податоците кога обработката се врши на автоматизиран начин, субјектот на личните податоци има право да добие директен пренос на личните податоци од еден контролор на друг, ако тоа е технички возможно.

Остварувањето на правото од првиот случај не го исклучува остварувањето на правото на бришење (право да се биде заборавен). Правото на бришење (право да се биде заборавен) не се однесува на обработката потребна за извршување на работи од јавен интерес или при вршење на службеното овластување доделено на контролорот.

Правото на преносливост на податоците наведено во првиот случај, не смее да влијае негативно врз правата и слободите на другите физички лица.

Ова право му овозможува на субјектот на личните податоци да ги добие личните податоци кои се однесуваат на него, што тој ги доставил до контролорот, во структуриран, најчесто користен и машински читлив формат и да ги предаде тие податоци на друг

контролор каде што обработката се врши на автоматизиран начин. Ова право мора да се применува кога субјектот на личните податоци ги обезбедил своите лични податоци врз основа на својата дадена согласност или кога обработката е неопходна поради договорна обврска. Онаму каде што обработката е заснована врз законска основа различна од согласност или договор, правото на преносливост не може да се оствари. Во овој контекст, остварувањето на ова право не е применливо во случаи кога обработката на личните податоци е потребна за да се исполни законска обврска која ја има контролорот, за извршување на работи од јавен интерес или при вршење на службеното овластување доделено на контролорот. Во случај на група на лични податоци каде е засегнат повеќе од еден субјект на личните податоци, правото на нивно добивање не смее да влијае негативно врз правата и слободите на другите субјекти на лични податоци, во согласност со постојната законска регулатива. Исто така, тоа право не смее да биде во спротивност со правото на субјектот на личните податоци да добие бришење на личните податоци и ограничувања на тоа право, онака како што е утврдено во постојниот закон и, особено, не треба да претпоставува бришење на личните податоци во врска со субјектот на личните податоци што му ги обезбедил тој за извршување на договорот до оној степен до кој личните податоци се потребни за извршување на тој договор. Како резултат на ова остварување, субјектот добива овластувања и поголема контрола врз личните податоци кои се однесуваат на него. Оттаму, контролорите на личните податоци треба да бидат охрабрени да развиваат интероперабилни формати кои овозможуваат преносливост на податоците, без тоа да предизвика експлицитна обврска за нив. Сепак, кога е технички изводливо, субјектот на личните податоци треба да има право да ги пренесе личните податоците директно од еден контролор на друг. Контролорите не треба да создаваат пречки за остварување на правото на преносливост. Ова ќе треба да го олеснат и за субјектот на личните податоци, овозможувајќи повторна употреба на податоците, како и контролорите, обезбедувајќи брз, сигурен и безбеден механизам за да обезбедат пренос на податоците од еден контролор до друг под одредени околности и под контрола на субјектот на личните податоци. Значаен елемент во остварувањето на правото на преносливост е изборот на субјектот на личните податоци. Давањето на податоци од контролорот на субјектот на личните податоци

или директно до друг контролор, во зависност од желбите на субјектот ја исклучува одговорноста на контролоротиспраќач за обработка извршена од субјектот или од друг контролор кој ги добил личните податоци. Во исто време, контролорот прима тел на податоци има обврска преносливите податоци кои се дадени да бидат релевантни и да не бидат прекумерни во врска со новата обработка на податоците. Постои и обврска контролорот-прима тел да ги обработува податоците кои се обезбедени во согласност со општите начела: законитост, правичност, транспарентност, ограничување на целите, минимален обем на податоци, точност, ограничување на рокот на чување, интегритет, доверливост и отчетност. Кога т.н. контролориспраќач ќе добие барање од субјектот на личните податоци за преносливост на податоците, контролорот треба да ги преземе сите заштитни мерки за да потврди дека тој ќе дејствува од името на субјектот на личните податоци. За таа цел, се препорачува контролорот да воспостави посебни процедури во кои јасно и прецизно се дефинира опфатот и видот на податоците кои субјектот на личните податоци може да побара да се пренесат, и да обезбеди потврда од субјектот на личните податоци во врска со односниот процес на пренос.

Ова право е ограничено на лични податоци обезбедени од субјектот на податоците, односно правото на преносливост на податоци опфаќа податоци обезбедени свесно и активно од субјектот на личните податоци, како и личните податоци генерирани од неговата активност. Ова ново право не треба да биде ограничено само на личните информации кои директно се соопштуваат од субјектот на податоците, на пример, преку интернет-формулар. Ова право, што се применува под одредени услови, го поддржува изборот на корисникот, контролата на корисниците и зајакнувањето на корисниците.

Примери на обработка кога може да се применува правото на преносливост на податоците: податоци кои се чуваат на сервис за емитување музика во живо и пренос на податоците за омилената музика на друга платформа; наслови на книги од електронска библиотека; податоци од паметен мерач на потрошувачка на енергија; враќање на список со контакти од апликација на страницата за проверка на електронска пошта; дневник на активности; историја на користени вебстраници; активности на пребарување.

Како добра практика, контролорите на податоци треба да започнат со развој на средства што ќе придонесат да одговорат на барањата за пренос на податоци, како што се алатки за преземање и Интерфејси за програмирање апликации. Тие треба да гарантираат дека личните податоци се пренесуваат во структуриран, најчесто користен и машински читлив формат, и тие треба да бидат охрабрени за да обезбедат интероперабилност на форматот на податоците дадени во барањето за преносливост на податоци.

Се препорачува засегнатите страни во соодветната област (индустриска гранка, трговски здруженија, здруженија на граѓани...) да работат заедно на заеднички сет на интероперативни стандарди и формати за да ги испорачаат барањата од правото на преносливост на податоци.

Новото право на преносливост на податоци има за цел да ја зајакне контролата на субјектите на податоци во однос на нивните лични податоци, бидејќи ја олеснува нивната можност за пренесување, копирање или пренесување на лични податоци лесно од една ИТ околина во друга (без разлика дали на нивните сопствени системи, системи на доверливи трети лица или оние на нови контролори на податоци). Потврдувајќи ги личните права на лицата и контролата врз личните податоци што се однесуваат на нив, преносливоста на податоците претставува можност да се „изврши одново урамнотежување“ на односот помеѓу субјектите на личните податоци и контролорите.

Кога се применува правото на преносливост на податоци?

Правото на преносливост на податоци се применува само ако обработката на личните податоци се врши автоматизирано и не ги опфаќа личните податоци кои се обработуваат рачно.

Првиот услов за применување на правото на преносливост е дека субјектот на личните податоци може да го оствари само за лични податоци што се однесуваат на него, вториот услов е тие податоци субјектот на лични податоци самиот да ги доставил на контролорот и третиот услов е правото на преносливост на податоци да нема негативно влијае врз правата и слободите на другите субјекти на лични податоци.

Главни елементи на преносливоста на податоците се следните:

- Право на примање лични податоци
- Право на пренесување на лични податоци од еден контролор на податоци на друг контролор
- Контрола врз податоците
- Преносливост на податоци наспроти другите права на субјектите на податоци.

Првично, преносливоста на податоците е право на субјектот да добие подмножество на лични податоци обработени од контролор вон врска со него и да ги чува тие податоци за понатамошна лична употреба. Таквото складирање може да биде на приватен уред или на приватен облак, без притоа да се пренесуваат податоците на друг контролор. Во овој поглед, преносливоста на податоците го надополнува правото на пристап. Една од специфичностите на преносливоста на податоците е фактот дека нуди лесен начин за субјектите на лични податоци сами да управуваат и да ги користат повторно личните податоци. Овие податоци треба да се добијат во структуриран, најчесто користен и машински читлив формат. На пример, субјект на лични податоци може да биде заинтересиран за преземање на неговата моментална листа за репродукција (или историја на слушани нумери) од услуга за стримирање музика, за да открие колку пати слушал конкретни песни.

Второ, ова право на субјектите им овозможува да пренесуваат лични податоци од еден контролор на податоци на друг контролор на податоци „без пречки“ директно на барање на субјектот на податоците и кога тоа е технички изводливо. Во суштина, овој елемент на преносливост на податоци обезбедува можност субјектите не само да ги прибираат и повторно употребат, туку и да ги пренесат податоците што ги доставиле до друг давател на услуги (или во истиот деловен сектор или во различен).

Ова право му овозможува чувство на контрола на субјектот на лични податоци, односно уверување дека преносот на неговите лични податоци е под негова контрола и според неговите желби. Контролорите на податоци кои одговараат на барања за пренос на податоци, под утврдените услови, не се одговорни за обработката што ја врши субјектот на личните податоците или од друга компанија која прима лични податоци. Тие дејствуваат во

име на субјектот, вклучително и кога личните податоци директно се пренесуваат на друг контролор. Истовремено, контролорот треба да воспостави заштитни мерки за да се обезбеди дека навистина постапува во име на субјектот на личните податоците. На пример, контролорот може да воспостави процедури за да обезбеди дека видот на пренесените лични податоци се навистина оние што субјектот сака да ги пренесува, на пример со добивање на потврда пред пренесување или порано, за тоа кога е дадена првичната согласност за обработка, или пред договорот да биде финализиран. Контролорите на податоци што одговараат на барање за пренос на податоци немаат специфична обврска да го проверат и потврдат квалитетот на податоците пред да ги пренесат. Се разбира, овие податоци веќе треба да бидат точни и ажурирани, според начелата за заштита на личните податоци. Покрај тоа, преносливоста на податоците не наметнува обврска на контролорот на податоците да ги задржи личните податоци подолго отколку што е потребно или надвор од одреден рок на чување.

Исто така, контролорот треба да спроведе специфични процедури во соработка со своите обработувачи за да одговори на барањата за преносливост на податоци. Во случај на заедничка контрола, договорот треба јасно да ги распредели одговорностите помеѓу секој контролор на податоци во однос на обработката на барањата за преносливост на податоци.

Кога субјектот на личните податоци го остварува своето право на преносливост на податоци, тој го прави без да се повреди кое било друго право на други субјекти на лични податоци. Преносливоста на податоците не предизвикува нивно автоматско бришење од системите на контролорот и не влијае на оригиналниот рок на чување што се однесува на податоците што се пренесени. Субјектот на личните податоци може да ги остварува неговите права сè додека контролорот сè уште ги обработува податоците. Подеднакво, ако субјектот на личните податоци сака да го искористи своето право на бришење („право да се биде заборавен“), преносливоста на податоците не може да се користи од контролорот како начин за одложување или одбивање на бришењето.

Со цел да се усогласат со ова право, контролорите мора да ги информираат субјектите на податоци за постоењето на новото право на преносливост. Кога односните лични податоци се

директно собрани од субјектот на личните податоци, тоа мора да се случи во моментот кога истите се добиваат. Ако личните податоци не се добиени од субјектот на лични податоци, контролорот мора да ги обезбеди информациите кои што има обврска да ги достави на субјектите на лични податоци согласно закон.

Во принцип, терминот „обезбедени од субјектот на личните податоци“ треба да се толкува широко, и треба да ги исклучи „заклучоците“ и „изведените податоци“, кои вклучуваат лични податоци што се создадени од давателот на услугата (на пример, алгоритмички резултати).

Така, терминот „обезбедено од“ вклучува лични податоци што се однесуваат на активност на субјектот на личните податоци или резултат на набљудување на однесувањето на поединецот, но не вклучува податоци кои произлегуваат од направената анализа на тоа однесување.

При обезбедување на потребните информации, контролорите мора да обезбедат дека тие го разликуваат правото на преносливост на податоците од други права. Контролорите треба јасно да ја објаснат разликата помеѓу видовите податоци што субјектот на личните податоци може да ги добие преку правото на пристап и преносливоста на податоците. Контролорот пред да одговори на барањето треба да го идентификува субјектот на личните податоци, а во случаите кога контролорот има основани сомнежи за идентитетот на субјектот, може да побара дополнителни информации за да го потврди неговиот идентитетот. Кога информациите и податоците собрани на интернет се поврзани со псевдоними или уникатни идентификатори, контролорите можат да спроведат соодветни процедури, на пример преку постапки за автениткација, кориснички имиња и лозинки...

Контролорот е одговорен за преземање на сите безбедносни мерки потребни за да се обезбеди не само личните податоци да се безбедно пренесени (со употреба на пример криптирање на податоците) до вистинската дестинација (со употреба на силни мерки за автентикација), но исто така, да продолжи да ги заштитува личните податоци што остануваат во нивните системи. Понатаму, контролорот е одговрен и за транспарентните процедури за справување со можните ризици при обработката на личните податоци, при што контролорите треба да ги проценат специфичните ризици поврзани со преносливоста на податоците и да преземат соодветни мерки за ублажување на ризиците.

На пример, доколку обемот на податоци што ги бара субјектот на лични податоци е проблематичен, наместо контролорот потенцијално да овозможи подолг временски период за остварување на правото на преносливост, ќе треба да разгледа алтернативни средства за обезбедување на податоците, како што се користење на стриминг или зачувување на ЦД, ДВД, УСБ или други физички медиуми или дозволување на личните податоци директно да се пренесуваат на друг контролор каде што тоа е технички изводливо, или преку користење на автоматизирана алатка која овозможува вадење/издвојување на релевантни податоци.

IV.5.4 ПРАВО НА ПРИГОВОР И АВТОМАТИЗИРАНО ДОНЕСУВАЊЕ НА ПОЕДИНЕЧНИ ОДЛУКИ

Правото на приговор му овозможува на субјектот на личните податоци врз основа на конкретна ситуација поврзана со него да поднесе приговор до контролорот, во секое време, за начинот на обработката на неговите лични податоци, во случаите која обработката е потребна за извршување на работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон и кога 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 коишто бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете, вклучувајќи и профилирање според овие основи. Контролорот не може повеќе да врши обработка на личните податоци, освен ако докаже дека постојат релевантни легитимни интереси за обработка, кои преовладуваат над интересите, правата и слободите на субјектот на личните податоци, или за воспоставување, остварување или одбрана на неговите правни барања.

Доколку личните податоци се обработуваат за цели на директен маркетинг, субјектот на личните податоци има право во секое време да поднесе приговор на обработката на неговите лични податоци поврзани со овој вид на маркетинг, кој вклучува и профилирање до оној степен до кој истото е поврзано со директниот маркетинг. Кога субјектот на личните податоци

приговара на обработката на неговите лични податоци за цели на директен маркетинг, контролорот има обврска да ја запре натамошната обработка на личните податоци за тие цели.

Најдоцна до моментот на првата комуникација со субјектот на личните податоци, субјектот на личните податоци мора изречно да биде известен за неговото право на приговор, при што известувањето мора да се направи на јасен начин и одвоено од било која друга информација.

Во контекст на користењето на услугите на информатичкото општество и независно од прописите за електронските комуникации, субјектот на личните податоци може да го користи правото на приговор преку автоматски средства со користење на технички спецификации.

Кога личните податоци се обработуваат за цели на научни или историски истражувања или за статистички цели (при што контролорот е должен да примени соодветни заштитни мерки за правата и слободите на субјектот на личните податоци), субјектот на личните податоците има право, врз основа на конкретната ситуација поврзана со него да поднесе приговор против обработката на неговите лични податоци, освен ако обработката е неопходна за реализирање на работи од јавен интерес.

Овие заштитни мерки обезбедуваат применување на технички и организациски мерки, особено во однос на почитувањето на начелото на обработка на минимален обем на податоци. Овие мерки може да вклучуваат псевдонимизација под услов, наведените цели да може да се постигнат на овој начин. Кога наведените цели може да се постигнат преку понатамошна обработка, која што не дозволува или повеќе не дозволува идентификација на субјектите на лични податоци, тие цели се постигнати на овој начин.

Иако не е изречно утврдено со закон, согласно начелата на транспарентност, одговорност и отчетност, контролорот треба да води ажурирана листа на информации за субјектот на личните податоци кои го остварил своето право на приговор, и секако треба да има процедура во која подетално се опишува начинот на кој се постапува при поднесен приговор од страна на субјект на лични податоци. Со оглед што како и другите права кои беа елаборирани погоре, и правото на приговор во смисла на Законот за заштита на личните податоци е лично право, субјектот на личните податоци може да приговара само против обработка

на негови лични податоци, а врз основа на конкретна ситуација поврзана со него.

Автоматско донесување на поединечни одлуки, вклучувајќи и профилирање: Субјектот на личните податоци има право да не биде предмет на одлука заснована единствено на автоматизирана обработка, вклучувајќи го и профилирањето што предизвикува правни последици за него или на сличен начин значително влијае на него.

Исклучок од ова право претставува доколку одлуката:

- е потребна за склучување или извршување на договор меѓу субјектот на личните податоци и контролорот;
- е дозволена со закон што се применува во однос на контролорот, и во кој исто така се предвидени соодветни мерки за заштита на правата и слободите и легитимните интереси на субјектот на личните податоци или
- се заснова на изречна согласност на субјектот на личните податоци.

Во првиот и третиот од наведените случаи, контролорот е должен да примени соодветни мерки за заштита на правата и слободите, како и на легитимните интереси на субјектот на личните податоци, а најмалку право на обезбедување на човечка интервенција од страна на контролорот, право на изразување на личен став и право на оспорување на таквата одлука.

Одлуките од вториот случај не смеат да се засноваат на посебни категории на лични податоци, освен ако субјектот на лични податоци дал изречна согласност за обработка на тие посебни категории на лични податоци за една или повеќе конкретни цели или обработката е неопходна поради причини од јавен интерес врз основа на закон пропорционално на целта и почитување на суштината на правото на заштита на личните податоци, како и обезбедување соодветни и конкретни мерки за заштита на фундаменталните права и интереси на субјектот на личните податоци, при што се воспоставени и соодветни мерки за заштита на неговите права, слободи и легитимни интереси.

Дефиницијата за профилирање е дадена на страна број пет од оваа анализа.

Профилирањето практично е составено од три елементи:

- Обработката мора да биде во автоматизирана форма;
- Обработката треба да се врши врз лични податоци и
- Целта мора да биде проценка на личните аспекти на субјектот на личните податоци.

Профилирањето е постапка што може да вклучува низа статистички отстапувања. Често се користи за да се прават предвидувања за луѓето, користејќи податоци од различни извори за да се заклучи нешто за поединецот, засновано на квалитетите на другите кои изгледаат статистички слични. Профилирањето може да вклучува три различни фази: собирање на податоци; автоматизирана анализа за да се идентификуваат корелациите и примена на корелацијата со поединецот за идентификување на карактеристиките на сегашното или идното однесување. Генерално, профилирање значи да се соберат информации за лице (или група на лица) и да се проценат нивните карактеристики или обрасци на однесување со цел да се стават во одредена категорија или група, особено да се анализираат и/или да се прават предвидувања за нив, на пример за можност за извршување на задача, интереси или веројатно однесување.

По дефиниција профилирање би претставувало и следењето на профил на социјалните мрежи на определено лице кое споделува вести, ставови и информации од определена политичка партија, па за истото може да се смета (предвидување) дека на претстојни избори би гласало за таа политичка партија (веројатно однесување).

Автоматското одлучување има различен обем и може делумно да се преклопува или да резултира од профилирање. Единствено автоматизирано донесување одлуки е можност за донесување одлуки со технолошки средства без вклучување на човечки фактор. Автоматизираните одлуки можат да се засноваат на кој било вид на податоци, на пример: податоци обезбедени директно од засегнатите лица (како што се одговори на прашалник); податоци за набљудување на поединци (како што се податоци за локација собрани преку апликација); изведени податоци, како профил на поединецот (на пр. проценка за кредитоспособност).

Автоматизираните одлуки можат да се донесат со или без профилирање, а профилирањето може да се одвива без

да донесете автоматски решенија. Сепак, профилирањето и автоматското донесување одлуки не се нужно одделни активности. Нешто што започнува како едноставен автоматизиран процес на одлучување може да стане процес што се заснова на профилирање, во зависност од тоа како се користат податоците.

На пример: Изрекување на казни за брзо возење единствено врз основа на докази од камери е автоматски процес на донесување одлуки што не мора да вклучува профилирање.

Ова донесување на одлука, би станало одлука заснована на профилирање, ако навиките за возење на поединецот се следат со текот на времето, и на пример износот на изречената глоба би бил исход на проценка која вклучува други фактори, како на пример дали пречекорувањето на брзината е прекршок кој се повторува или дали возачот имал други неодамнешни нарушувања во безбедноста на сообраќајот.

Одлуките кои не се само автоматизирани може да вклучуваат профилирање. На пример, пред да одобри хипотекарен кредит, банката може да го земе предвид кредитниот резултат на заемопримачот, со дополнителна значајна интервенција извршена од луѓето пред да се примени каква било одлука за заемопримачот.

Постојат потенцијално три начини на кои може да се користи профилирање: општо профилирање; донесување одлуки засновано врз профилирање; и единствено автоматско донесување одлуки, вклучително и профилирање, кое произведува правни ефекти или значително влијае на субјектот на личните податоци.

Контролорите можат да вршат профилирање и автоматско донесување одлуки сè додека можат да ги исполнат сите начела за заштита на личните податоци, да имаат законска основа за обработка и да применуваат дополнителни заштитни мерки и ограничувања во случај на единствено автоматско донесување одлуки, вклучително и профилирање во случаите определни согласно Законот за заштита на личните податоци.

Развивањето на модерни технологии им овозможува на контролорите на лични податоци да собираат и анализираат лични податоци за различни цели, да донесуваат заклучоци за субјектот на личните податоци и да предвидат преземање на можни чекори по однос на овие заклучоци.

Ова значи дека профилирањето не е истоветно со следењето, туку нешто повеќе, вклучувајќи ја намерата да се донесе одлука за субјектот на личните податоци или оди и понатаму за да се предвиди однесувањето и преференциите на субјектот. Навлегувајќи во личната сфера на поединечниот субјект на личните податоци, целта на профилирањето е да се добие одреден резултат или активност која произлегува од обработката на личните податоци. Токму затоа субјектот на личните податоци треба да биде информиран за постоењето на профилирање и за последиците на таквото профилирање. Онаму каде личните податоци се собираат од субјектот на личните податоци, субјектот треба исто така да биде информиран дали има обврска да ги даде личните податоци, но и за последиците од нивно давање, во случај тој да не ги обезбеди таквите податоци. Од практична гледна точка, таа информација може да се обезбеди во комбинација од стандардизираните икони за да има јасно видлив, разбирлив и јасно читлив начин со цел разумен преглед на обработката која се планира. Во случај кога иконите се презентираат електронски, тие треба да бидат машински читливи. Секој субјект на личните податоци треба да има право да разбере и добие информации, конкретно по однос на целите за обработка на личните податоци, онаму каде е можно, за периодот во кој се обработуваат личните податоци, корисниците на личните податоци, логиката на која било автоматизирана обработка на личните податоци и, барем кога станува збор за профилирање, последиците на таквата обработка.

Самото профилирање не претставува директен маркетинг, туку може да се однесува на обработка на личните податоци за потребите на директниот маркетинг. Во вакви случаи, субјектот на личните податоци треба да има право да не биде предмет на одлучување, што може да вклучува мерка, евалуација на личните аспекти кои се однесуваат на него кои се базираат единствено врз автоматизираната обработка. Во случаи кога обработката е наменета за директен маркетинг, вклучувајќи профилирање, субјектот на личните податоци има право да поднесе приговор. Во таков случај, обработката мора да се прекине и контролорот веќе нема овластување ниту основ да ги обработува податоците за субјекот за цели на директен маркетинг.

Обработката на лични податоци за автоматско донесување на поединечни одлуки треба да обезбеди соодветни заштитни механизми за заштита на правата, слободите и легитимните

интереси на субјектот на личните податоци. При автоматизирана обработка вклучувајќи го и профилирањето, за цели на склучување или извршување на договор и кога обработка се врши врз основа на дадена изречна согласност контролорот треба да обезбеди: конкретна информација на субјектот на личните податоци; правото на човечка интервенција; правото на изразување на сопствено мислење; правото да се одбие објаснување за одлуките донесени после таква оценка и правото да се оспори таквата одлука.

Автоматизираното донесување на поединечни одлуки, вклучувајќи и профилирање не треба да се однесува на деца. Исто така, кога се обработуваат лични податоци за потребите на одлучување по однос на одредени физички лица по какви било систематски и опсежни оценки на личните аспекти поврзани со тие лица врз база на профилирање на нивните податоци или по обработката на посебни категории на лични податоци, биометриски податоци, или податоци за кривични осуди и дела или за слични безбедносни мерки, контролорот треба да направи проценка на влијанието на заштитата на личните податоци.

IV.5.5 ОГРАНИЧУВАЊА И ОТСТАПУВАЊА

Ограничувања

Со законот кој што се применува за контролорот или обработувачот може да се ограничат обемот на обврските и правата на транспарентност, информираност и пристап до лични податоци, исправка и бришење („право да се биде заборавен“), ограничување на обработката, обврската за известување при исправка или бришење на личните податоци или ограничување на обработката, правото на преносливост на податоците, правото на приговор и автоматизирано донесување на поединечни одлуки вклучувајќи и профилирање, обврската за известување на субјектот на личните податоци за нарушување на безбедноста на личните податоци, како и начелата поврзани со обработката на лични податоци, доколку тие одредби се во согласност со правата и обврските утврдени во членовите од Законот за заштита на личните податоци кои се однесуваат на правата на субјектите на личните податоци и кога таквото ограничување е во согласност со суштината на основните права и слободи и

претставува неопходна и пропорционална мерка со цел да се обезбеди:

1. националната безбедност;

2. одбраната;

3. јавната безбедност;

4. превенција, истрага, откривање или гонење на сторителите на кривични дела или извршување на изречените казнени санкции, вклучувајќи превенција и спречување на закани за јавната безбедност;

5. други важни цели од општ јавен интерес за Република Северна Македонија, а особено важен економски или финансиски интерес на државата, вклучувајќи монетарни, буџетски и даночни прашања, јавно здравје и социјална заштита;

6. заштита на независноста на судовите и судските постапки;

7. превенција, истрага, откривање и гонење на прекршувањето на етичките правила за регулираните професии;

8. следење, инспекциски надзор или регулаторни функции кои се барем повремено поврзани со исполнување на надлежностите на органите на државната власт во случаите од 1 до 5 и случајот 7;

9. заштита на субјектот на личните податоци или на правата и слободите на други физички лица;

10. спроведување на барањата во граѓански постапки.

Секоја законска мерка наведена погоре, особено содржи посебни одредби, по потреба најмалку за:

1. целите на обработката или категориите на обработка;

2. категориите на личните податоци;

3. обемот на воведените ограничувања;

4. заштитните мерки за спречување на злоупотреба или незаконски пристап или пренос;

5. спецификацијата на контролорот или категориите на контролори;

6. роковите на чување и применливите заштитни мерки, земајќи ги предвид природата, обемот и целите на обработката или категориите на обработка;

7. ризиците за правата и слободите на субјектите на личните податоци и

8. правото на субјектите на личните податоци да бидат информирани за ограничувањето, освен по исклучок ако истото би било во спротивност со целта на ограничувањето.

Секој случај треба одделно да се разгледува, при што треба да се бара рамнотежа помеѓу правата на субјектите на личните податоци и овластувањата на односните контролори. Ограничувањето може да се наметне поради легитимни интереси на други одредби кои преовладуваат. На пример, одредби од друг посебен закон кои пропишуваат ограничување или застој на информација која може да му се обезбеди на субјектот на личните податоци поради ризик од откривање на кривично дело. Легитимните интереси кои преовладуваат се пооправдани од интересите кои се поврзани со заштитата на личните податоци. Евентуални исклучоци или ограничувања мора да се неопходни во едно демократско општество и мора да бидат сразмерни со саканата цел. Во многу исклучителни случаи како што се медицински индикации, заштитата на физичкото лице може да бара ограничувања по однос на транспарентноста; ова е поврзано посебно со ограничувањето на правото на пристап на секое физичко лице.

Внесување на ваков тип на одредби во закон е гаранција за субјектот на личните податоци дека неговите податоци ќе се обработуваат законски и безбедно. Пример за ова се превенција, истрага, откривање или гонење на сторители на кривични дела или извршување на изречени казни вклучително заштитни мерки и спречување на закани по јавната безбедност. Ограничувањата во оваа област се наметнати од конкретни процедурални законски правила и процедури со цел да не се попречува истрагата за кривичното дело. Иако законот утврдува одредени ограничувања по правата на поединците, овие ограничувања не може да станат правило. Оттаму, субјектот на личните податоци има право на заштита преку управна и/или судска постапка.

Заштитни мерки и отстапувања поврзани со обработката за целите на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели

1. При обработката за цели на архивирање од јавен интерес, за научни или историски истражувања или за статистички цели,

контролорот е должен да примени соодветни заштитни мерки за правата и слободите на субјектот на личните податоци во согласност со Законот за заштита на личните податоци. Овие заштитни мерки обезбедуваат применување на технички и организациски мерки, особено во однос на почитувањето на начелото на обработка на минимален обем на податоци. Овие мерки може да вклучуваат псевдонимизација под услов, наведените цели да може да се постигнат на овој начин. Кога наведените цели може да се постигнат преку понатамошна обработка, која што не дозволува или повеќе не дозволува идентификација на субјектите на лични податоци, тие цели се постигнати на овој начин.

2. Кога личните податоци се обработуваат за научни или историски истражувања или за статистички цели, со закон можат да се предвидат отстапувања од правото на пристап, правото на исправка, правото на ограничување на обработката, и правото на приговор, во согласност со условите и заштитните мерки наведени во точката еден, до степен до кој постои веројатност овие права да го направат невозможно или сериозно да го попречат остварувањето на конкретните цели, а наведените отстапувања се потребни за постигнување на овие цели.

3. Кога личните податоци се обработуваат за целите на архивирање од јавен интерес, со закон можат да се предвидат отстапувања од правото на пристап, правото на исправка, правото на ограничување на обработката, обврската за известување при исправка или бришење на личните податоци или ограничување на обработката, правото на преносливост и правото на приговор, во согласност со условите и заштитните мерки наведени во точката еден, до степен до кој постои веројатност овие права да го направат невозможно или сериозно да го попречат остварувањето на конкретните цели, а наведените отстапувања се потребни за постигнување на овие цели.

4. Кога обработката наведена во точките 2 и 3 се користи истовремено и за друга цел, отстапувањата се применуваат единствено за обработката извршена за целите наведени во овие точки.

Во однос на обработката извршена за новинарски цели или за целите на академско, уметничко или литературно изразување, правата на субјектот на личните податоци, може да се исклучат или да се отстапи од нив, доколку тоа е потребно заради

балансирање на правото на заштита на личните податоци со слободата на изразување и информирање.

Ова особено се применува во однос на обработката на личните податоци во аудиовизуелната област и во новинските архиви (news archives), како и во библиотеките со печатени изданија (press libraries).

Остварувањето на правата на субјектите на личните податоци нема да се применува врз обработката на личните податоци што се врши за новинарски цели, само во случај ако јавниот интерес преовладува над приватниот интерес на субјектот на лични податоци.

При процесот на балансирање на правото на заштита на личните податоци со слободата на изразување и информирање се земаат предвид следните критериуми:

- природата на личните податоци,
- околности под кои се добиени личните податоци,
- влијанието на објавената информација кон дискусијата за јавниот интерес,
- колку е познато засегнатото физичко лице и кој е предметот на информацијата,
- претходно поведение на засегнатото физичко лице,
- претходна согласност на засегнатото физичко лице,
- содржината, формата и последиците од објавувањето на информацијата.

Правото на заштита на личните податоци и слободата на изразување и информирање се основни човекови права од категоријата на неапсолутни права. Има случаи кога е неопходно да се изнајде вистинската рамнотежа во реализацијата на различните еднакви права и оттаму е неопходно да се воведат посебни правила и критериуми. Новиот закон определува одредени отстапувања за посебни случаи. За обработката спроведена за новинарски цели или академски уметнички или литературен израз, може да се дозволат исклучоци или отстапувања од начелата за обработка на личните податоци од правата на субјектот на личните податоци, од обврските на контролорите и обработувачите, од некои

од условите во однос на преносот на личните податоци, доколку се потребни за да се оствари правото на заштита на личните податоци со слободата на изразување и информирање. Ваквите отстапувања посебно ќе се применуваат за обработка на личните податоци во аудиовизуелната област и во новинските архиви како и во библиотеките со печатени изданија. Кога обработката се извршува за новинарски цели само во случи кога јавниот интерес преовладува над личниот интерес на субјектот на личните податоци, законските правила нема да се применуваат. Паралелно со заштитата на правото на заштита на личните податоци и слободата на изразување и информирање, треба да се земат предвид погоре наведените критериуми.

Треба да се земе предвид дека отстапувањата од правата на субјектот на личните податоци ќе се применуваат само во случаи кои се изречно определени со закон.

Во оваа анализа детално се елаборирани сите права на субјектите на личните податоци кои ги гарантира новиот Закон за заштита на личните податоци, кој што во суштина го шири опсегот на обврски на контролорите а истовремено ги зајакнува и проширува правата на субјектите на личните податоци. Невладините организации како контролори треба да донесат процедура во која што детално ќе ги опишат постапката и процедурата за остварување на овие права. Истовремено, невладините организации ќе треба да изработат и изјава, односно политика за приватност која ќе треба да ја објават на своите веб страници или ќе ги направат јавно достапни на друг начин, а во која ќе бидат јасно дадени потребните информации за постоењето, но и остварувањето на овие права и насоки, каде и како субјектите на личните податоци може да се обратат за да добијат подетални информации за своите права.

IV.5.6 СПЕЦИФИЧНОСТИ ВО ЗАШТИТАТА НА ЛИЦА СО ПОПРЕЧЕНОСТ КОИ ШТО ИМААТ ПРЕЧКИ ВО ТЕЛЕСНИОТ ИЛИ МЕНТАЛНИОТ РАЗВОЈ ИЛИ КОМБИНИРАНИ ПРЕЧКИ (НАЧИН НА ДОБИВАЊЕ НА СОГЛАСНОСТ, РИЗИЦИ, ПРАВИЛА, ЗАШТИТНИ МЕРКИ И ПРАВА ВО ОДНОС НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ОДНОС НА АКТИВНОСТИТЕ КОИ СЕ НАСОЧЕНИ КОН ОВИЕ ЛИЦА)

Согласно Законот за заштита на личните податоци, обработката на посебните категории на лични податоци е забранета и само во одредени исклучоци кои концизно се наброени во законот, може да се врши нивна обработка. Еден од исклучоците согласно кои може да се врши обработка на посебните категории на лични податоци се однесува на случаите кога обработката се извршува во рамките на легитимните активности со соодветни заштитни мерки од одредена фондација, здружение или некоја друга непрофитна организација со политичка, филозофска, религиозна или синдикална цел и под услов обработката да се однесува само на членови на овие организации или на нивни поранешни членови или на лица кои имаат редовни контакти со нив во врска со нивните цели и под услов личните податоци да не се откриваат надвор од таа организација без согласност на субјектите на личните податоци.

Обработката во тој случај ќе биде законита само доколку се применат кумулативно следните услови:

- обработката се однесува само на сегашни или поранешни членови на одредена фондација, здружение или некоја друга непрофитна организација со политичка, филозофска, религиозна или синдикална или за лица кои имаат редовни контакти со нив во врска со нивните цели;
- личните податоци да не се откриваат надвор од таа организација без согласност на субјектите на личните податоци (контролорите не смеат да обработуваат податоци во форма на откривање врз база на кој било друг законски основ без согласност); и

- во текот на обработката да се применат соодветни заштитни мерки од страна на споменатите организации (контролори).

Целта на оваа правна основа е да им се овозможи на различните контролори (фондации, граѓани или други непрофитни организации со политичка, филозофска, религиозна или синдикална мисија) слободно да ги обработуваат податоците кои се однесуваат на членувањето во организациите кои самите субјекти ги направиле достапни.

Пример: Здружение кое ги штити правата на лицата кои имаат телесен инвадилитет, може да обработува посебни категории на лични податоци кои се однесуваат на здравствената состојба на овие лица кои што самите ја откриваат при зачленувањето во здружението. Во текот на обработката на личните податоци треба да се применат соодветни заштитни мерки од страна на здружението, а во случаите кога здружението има оправдана потреба личните податоци да ги открие надвор од здружението, може да открие лични податоци на своите членови само со претходно дадена изречна, јасна, недвосмислена и информирана согласност, поединечно од секој член за кого ќе се откријат личните податоци.

Во случаите каде здружението штити односно застапува права на лица на кои што што делумно или целосно им е одземена деловната способност, а кои поради душевно заболување, слабоумност, употреба на алкохол или други нервни отрови, наркотични дроги, психотропни супстанци и прекурсори, не се во состојба да се грижат за себеси и за заштита на своите права и интереси, согласноста за обработка на личните податоци во име на членовите на здружението треба да ја дадат нивните законски застапници (доколку се работи за целосно одземена деловна способност) или истата да ја одобрат (доколку е дадена од делумно неспособно лице).

Во наведениот случај, информациите за постоењето на правата од аспект на заштитата на личните податоци и начинот на остварување на правата на субјектите на личните податоци ќе треба да бидат насочени кон законските застапници на членовите на здружението.
Но, во секој случај здружението треба да вложи разумен напор да им ги објасни целите и ризиците за обработка на личните податоци, како и правата кои произлегуваат од законот за заштита на личните податоци на самите членови со методи преку

кои што ќе овозможат полесно разбирање, на пример преку визеуализација, слики, цртежи, анимирани видео клипови и слично.

Исто така и во случаите кога се нудат некои услуги на наведените категории на лица, контролорите треба да вложат напор и да применат најсоодветен начин, особено од аспект на транспарентноста, и да им ги објаснат колку што е возможно, правата кои ги имаат субјектите на личните податоци.

Според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозноста за правата и слободите на физичките лица, здруженијата се должни да применат соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот, а особено имајќи ги предвид и случаите кога се обработуваат и посебните категории на лични податоци.

V. НАОДИ И ЗАКЛУЧОЦИ

Во оваа глава се претставени наодите добиени од прашалникот за обработката на личните податоци поднесен до невладините организации и одговорите добиени од Агенцијата за заштита на личните податоци преку поднесени барања за слободен пристап до информации од јавен карактер.

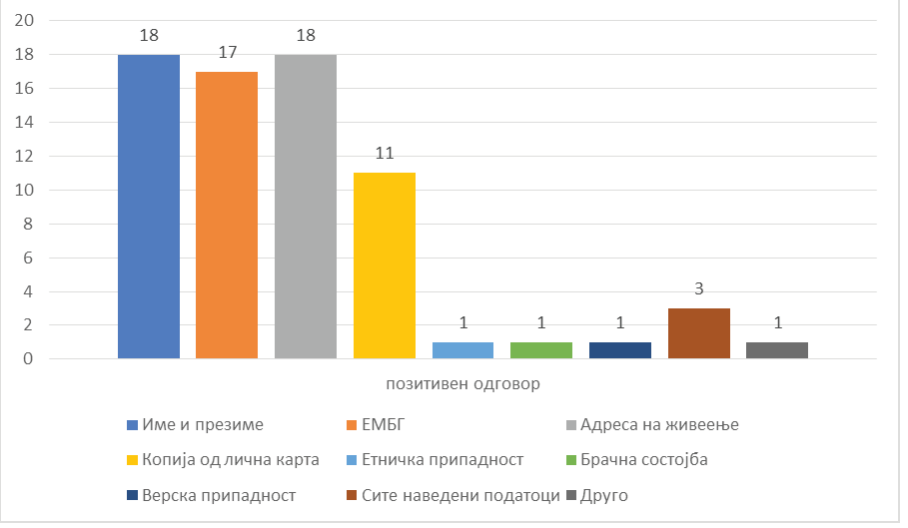
V.1 НАОДИ ОД ПРАШАЛНИКОТ ОДГОВОРЕН ОД НЕВЛАДИНИТЕ ОРГАНИЗАЦИИ

Прашалникот беше поднесен електронски до сите релевантни организации без разлика на дејноста која ја извршуваат, ниту пак на бројот на вработените. Целиот прашалникот се состои од 10 прашања.

Од 21 организации кои одговорија на прашалникот, 12 оранизации имаат од 1-10 вработени или ангажирани лица во нивната организација, 8 организации имаат од 11-20 вработени или ангажирани лица и само една организација со вработени до 21-30 лица.

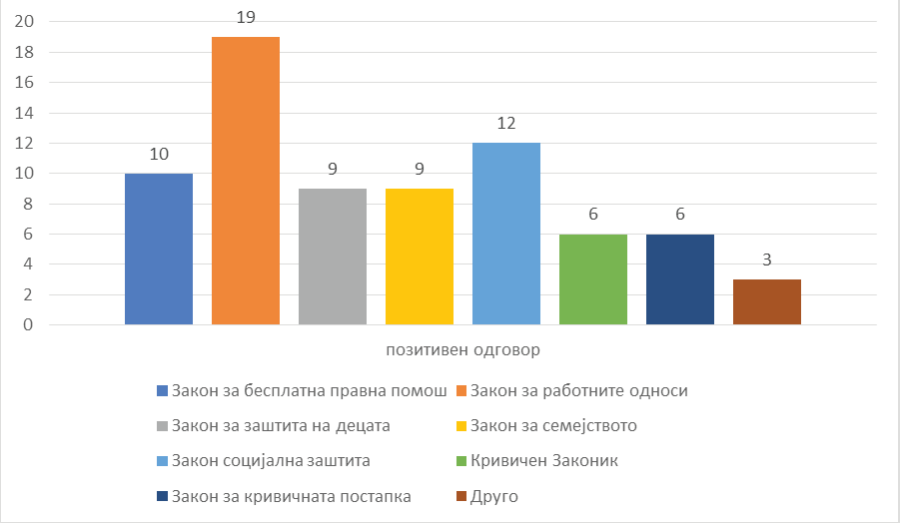
Тоа што е алармантно и бара повеќе внимание е тоа што веќе на второто прашање дури 11 организации одговориле дека обработуваат копија од лична карта за вработените/ангажирани лица, што е во спротивност со Законот за заштита на личните податоци, и претставува преобемна обработка за целта за која се прибира овој податок. Во табелата број 1 се претставени сите податоци кои овие невладини организации ги имаат одбрано дека ги обработуваат.

Табела 1. Лични податоци кои ги обработуваат за вработени/ангажирани лица



Поголемиот дел од невладините организации јасно ги препознаваат законите врз основа на кои ги прибираат личните податоци, така што на прашањето врз кои закони го засноваат нивното секојдневно функционирање, најголем дел одговориле дека како основа на работењето им претставуваат Законот за работните односи, Законот за социјална заштита, Законот за бесплатна правна помош, Законот за заштита на децата и Законот за семејството. Имајќи ги предвид ранливите категории со кои најчесто работат невладините организации, овие закони и претставуваат основа во нивното работење.

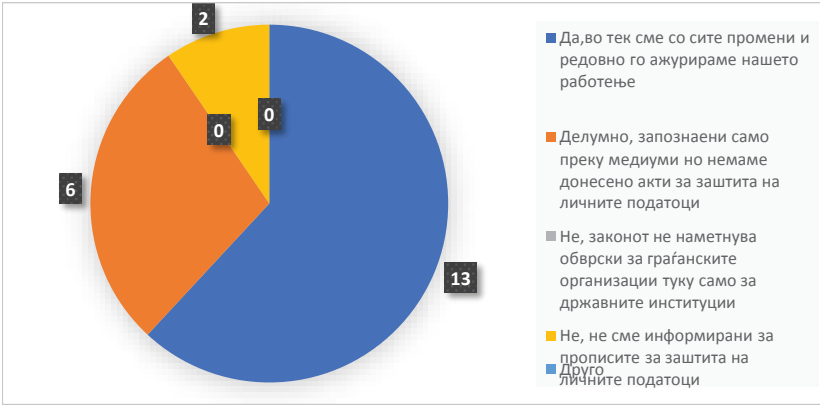
Табела 2. Закони врз кои се заснова на секојдневното работење на невладините организации



Изненадува високиот процент на организации кои одговориле дека се во тек со сите промени во легислативата и редовно го ажурираат своето работење, дури 13 организации, а 6 одговориле дека се делумно запознаени преку медиуми, но немаат донесено акти за заштита на личните податоци. Но, веќе во наредното прашање кое се однесува на носење на интерни акти 7 невладини организации одгориле дека имаат донесено акти и истите ги ажурираат, а 5 невладини дека имаат донесено акти но, истите не се ажурирани. Овие одговори не соодветуваат со тоа дека дури 17 невладини организации одговориле дека немаат назначено офицер за заштита на личните податоци, што е првата обврска која треба да ја исполнат при носење и имплементирање на интерните акти.

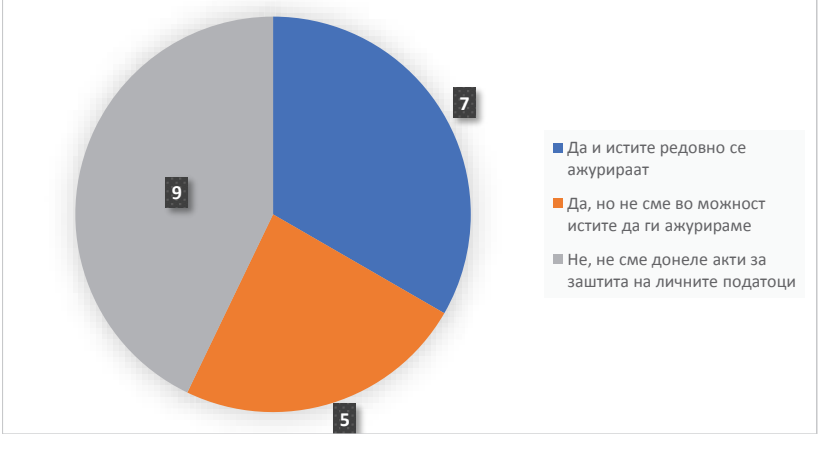
За подетално околу овие податоци погледенете ги табелите број 4, 5 и 6.

Табела 3. Дали невладината организација е запознаена со правата и обврските кои произлегуваат од прописите за заштита на личните податоци

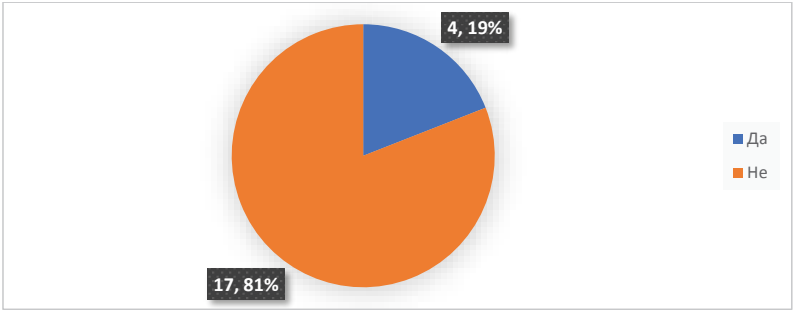


Иако голем процент на невладините организации одговорија дека се во тек со промените во легислативата и редовно го ажурираат своето работење, истите согласно одговорите на другите прашања немаат донесено акти за заштита на личните податоци и немаат назначено офицер за заштита на личните податоци.

Табела 4. Дали имате донесено акти за заштита на личните податоци

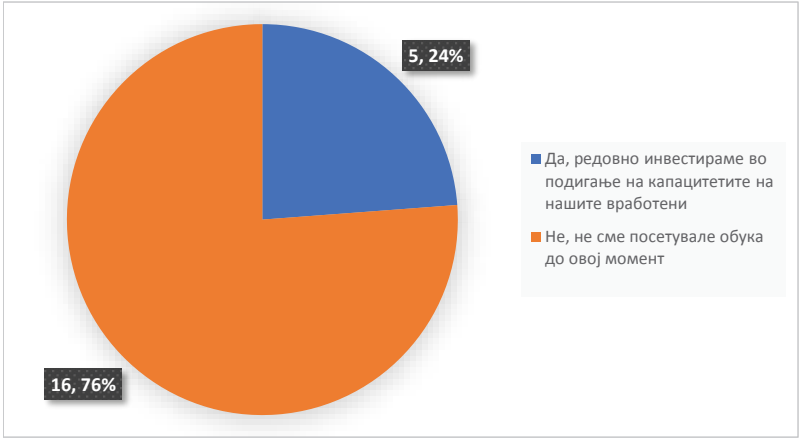


Табела 5. Дали имате назначено офицер за заштита на личните податоци?



За жал, многу мал процент од невладините организации имаат назначено офицер за заштита на личните податоци, што се потврдува и во податоците добиени од Агенцијата за заштита на личните податоци. Поради високата флуктуација на вработените во невладиниот сектор, многу често овој податок и не е ажуриран. Оваа обврска е клучна за донесување на сите други политики за заштита на обработката на личните податоци и имплементирање на законските прописи. Со тоа што токму овој елемент недостасува го прави потешко и целокупното усогласување на работењето на невладините организации со законските прописи за заштита на личните податоци.

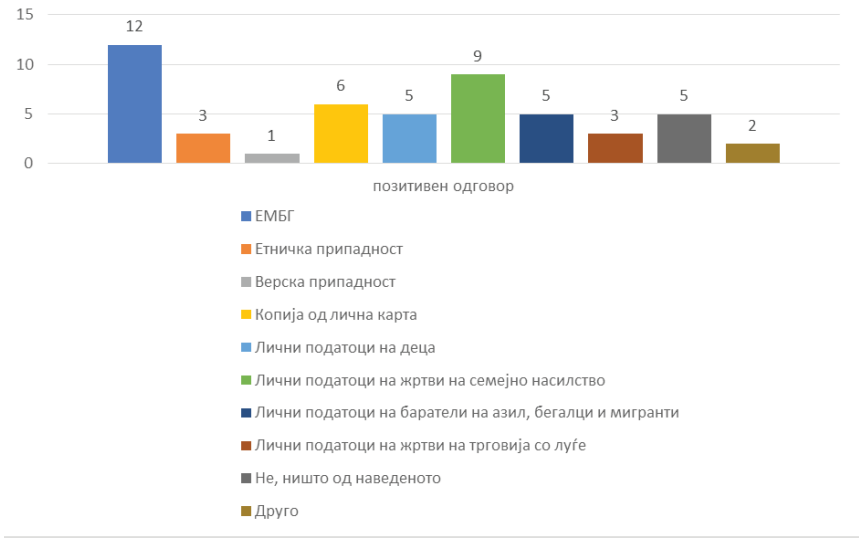
Табела 6. Дали некој од Вашите вработени/ангажирани лица имаат посетено обука за заштита на личните податоци?



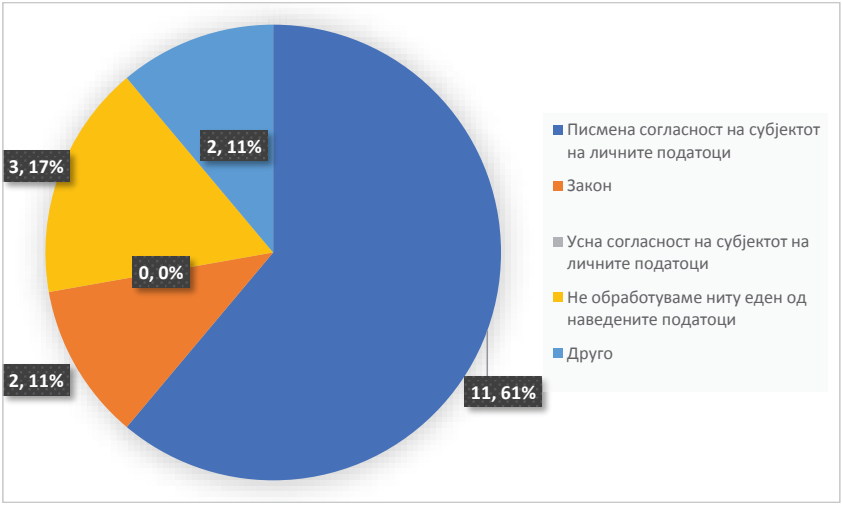
Останува загрижувачко и обучувањето на вработените односно ангажираните лица во невладините организации. Имајќи предвид дека самите невладини организации не располагаат со сопствени средства и најчесто претставува голем проблем да се издвојат средства за обучување на своите вработени/ангажирани лица, се препорачува да се пронајде соодветен модус на соработка помеѓу Агенцијата и невладините организации со цел да се олесни пристапот до обуки на вработените во невладиниот сектор.

Во табелата број 7 можеме да забележиме дека чувствителни податоци кои се обработуваат од страна на невладините организации се: единствениот матичен број на граѓанинот, потоа личните податоци на жртви на семејно насилство и на трето место е копија од лична карта. Како основ за обработка на овие лични податоци, 11 здруженија одговориле дека имаат обезбедено писмена согласност од субјектот на личните податоци. Овие податоци дополнително укажуваат на нерегуларности при обработката на чувствителните податоци од страна на невладините организации и дека е потребна обука за вработените односно ангажираните лица со цел усогласување со Законот за заштита на личните податоци, а особено имајќи предвид дека обработуваат чувствителни податоци на ранливи категории на граѓани по повеќе основи.

Табела 7. Дали обработувате некој од следниве податоци?



Табела 8. Основ за обработка на податоците од табелата 7.



На последното прашање од страна на невладините организации се бараше да одговорат согласно нивната проценка дали постои ризик за злоупотреба на личните податоци и дали се доволно заштитени од внатрешни и надворешни ризици за бебедноста на обработката на личните податоци?

На ова прашање 19 организации вкупно доставија одговор од кои, 8 сметаат дека не постои никаков ризик и дека се доволно заштитени, а од друга страна 10 невладини организации сметаат дека постои ризик и дека има простор за подбрување, само една невладина организација одговорила дека немаат одговор на ова прашање.

V.2 НАОДИ ОД ПОДАТОЦИТЕ ДОБИЕНИ ОД АГЕНЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Во оваа поглавје се претставени одговорите добиени преку поднесени барања за слободен пристап до информациите од јавен карактер до Агенцијата за заштита на личните податоци.

Број	Прашање	Одговор
1.	Дали и кои граѓански организации се обврзани да се регистрираат во Агенцијата за заштита на личните податоци (АЗЛП) и да донесат интерни акти за заштита на личните податоци (злп)?	Според член 71 од новиот Закон за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20) секое здружение на граѓани кое што обработува лични податоци е обврзано да ја извести Агенцијата за заштита на личните податоци доколку обработката постои веројатност да предизвика висок ризик за правата и слободите на физичките лица. Воедно, секое здружение на граѓани кое има својство на контролор или обработувач на личните податоци имаат обврска да подготват и изработат интерни процедури во согласност со Законот за заштита на личните податоци и донесените подзаконски прописи, преку кои ќе демонстрираат дека се усогласени со Законот. Во однос на ова, Агенцијата за заштита на личните податоци има донесено „Правилник за известување за обработка на лични податоци со висок ризик“, достапен на следниот линк: https://dzlp.mk/sites/default/files/u4/pravilnik_za_izvestuvanje_za_obrabotka_na_licni_podatoci_so_visok_rizik.pdf и „Листа на видовите операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци“ достапна на: https://dzlp.mk/sites/default/files/u4/lista_na_vidovite_operacii_na_obrabotka_za_koi_se_bara_pvzlp.pdf
2.	Колку здруженија на граѓани се регистрирани во Централниот Регистар на АЗЛП?	Во Централниот регистар на Агенцијата за заштита на личните податоци регистрирани се 42 здруженија на граѓани.

3.	Колку збирки и видови на збирки на лични податоци се регистрирани од страна на граѓанските организации во Централен Регистар во АЗЛП?	Во Централниот регистар на Агенцијата за заштита на личните податоци регистрирани се 118 збирки на лични податоци од страна на граѓански здруженија. Видови на збирки на лични податоци: - Збирка на кандидти за возачи на моторни возила - Збирка на вработени - Збирка на крводарители - Збирка на корисници на услуги - Збирка за донатори - Збирка на кандидати потенцијални вработени - Збирка на надворешни соработници - Збирка на Членови на управен одбор, - Збирка на Членови на надзорен одбор - Збирка за Видео надзор - Збирка за Хонорарни соработници - Збирка за клиенти
4.	Колку здруженија на граѓани назначиле офицер за заштита на личните податоци и за истото ја известиле АЗЛП?	Во Агенцијата за заштита на личните податоци од страна на здруженија на граѓани има пријавено 45 офицери за заштита на личните податоци.
5.	Дали до 31.03.2020 година од страна на здружение на граѓани е пријавено повреда на правото за заштита на личните податоци до АЗЛП?	Во периодот од 2015 година до 31.03.2020 година во Агенцијата за заштита на личните податоци од страна на здруженија на граѓани има пријавено 31 повреда на правото за заштита на личните податоци.

6.	Дали до 31.03.2020 година од страна на здруженија на граѓани се поднесени барања за мислење во однос на прописите за злп?	Во периодот од 2015 година до 31.03.2020 година во Агенцијата за заштита на личните податоци две здруженија на граѓани имаат поднесено барање за мислење во однос на прописите за заштита на личните податоци. Во 2016 година Агенцијата за заштита на личните податоци до сите регистрирани политички партии има испратено укажување за постапување со лични податоци во време на организирање на изборите.
7.	Дали до 31.03.2020 година претставници на здруженија на граѓани имаат посетено обука за злп.?	Во 2013 година 19 претставници на здруженија на граѓани посетиле обука во ДЗЛП. Во периодот од 2015 година до 31.03.2020 година, обука за заштита на личните податоци посетиле 15 претставници на здруженија на граѓани.
8.	Дали до 31.03.2020 година против донесени решенија на АЗЛП од страна на здруженија на граѓани има поведени управни спорови и доколку има, колкав е бројот на управните спорови?	Во периодот од 2015 година до 31.03.2020 година против 9 донесени решенија на Агенцијата за заштита на личните податоци има поведено управни спорови од страна на здруженија на граѓани. За сите решенија од страна на управниот суд е донесена позитивна одлука во полза на АЗЛП.

V.3 ЗАКЛУЧОЦИ

Наодите од истражувањето иако на реалтивно мал репрезентативен примерок од само 21 невладина организација сепак можеме да извлечеме неколку заеднички заклучоци кои можат да се постават како појдовна точка за надминување на моменталната ситуација. Имено, тоа што може да се подвлече е следново:

1. Има простор за подигање на свеста за обработката на личните податоци кај невладините организации и сите заеднички треба да најдат соодветен модус на соработка помеѓу себе и Агенцијата за заштита на личните податоци, посебно во делот на можеби изготвување на соодветен кодекс за обработка на личните податоци. Ова би овозможило унифицирање на политиките за заштита на личните податоци на ниво на цел невладин сектор.
2. Потребни се соодветни обуки на невладините организации за подигње на свеста за обврските кои произлегуваат од законските прописи. Соодветен модус на соработка треба да се изготви помеѓу невладините организации, експертската јавност како и Агенцијата за заштита на личните податоци, за да се олесни пристапот на невладините организации до обуки за заштита на личните податоци.
3. Загрижувачки е нискиот број на организации кои имаат назначено офицер за заштита на личните податоци и кои имаат донесено политики за заштита на личните податоци. Треба да се изготват соодветни материјали за подигање на свеста и да се достават до сите невладини организации.
4. Мал е процентот и на пријави на злоупотреба на личните податоци поднесени од страна на невладините организации.
5. Сосема е мала и бројката на невладини организации кои се обраќаат до Агенцијата за заштита на личните податоци за мислење во однос на своите акти или за било какви други ситуации во врска со заштитата на личните податоци.

VI. ЗАКЛУЧОЦИ И ПРЕПОРАКИ

Со цел да се исполнат сите барања кои ги наметнува Законот за заштита на личните податоци, невладините организации треба најпрвин да извршат самоевалуација на системот за заштита на личните податоци кои го имаат воспоставено. Пример на самоевалуација е додаден како анекс на оваа анализа со цел да им послужи на невладините организации за извршување на истото. Согласно добиениот резултат од самоевалуацијата, препорачливо е да подготват акциски план кој овозможува постигнување на усогласеност со новите вредности и мерки за заштита на личните податоци за краток временски период.

Самоевалуацијата претставува своевидна интроспекција на невладините организации, како еден вид внатрешна ревизија на системот за обработка на лични податоци. Притоа, самоевалуацијата треба да ги опфати следните прашања и аспекти:

1. Кои категории на лични податоци ги обработува невладината организација? Дали се обработуваат посебни категории на лични податоци? За кои категории на субјекти на лични податоци се врши обработката на лични податоци? Дали се обработуваат лични податоци на деца? Каде се чуваат личните податоци? Како се обработуваат личните податоци (рачно и/или автоматизирано)? Дали и кои софтверски апликации се користат за обработка на лични податоци? Колкав е рокот на чување на личните податоци? Кој има пристап до личните податоци?
2. За кои цели се обработуваат личните податоци? Согласно кој основ се обработуваат личните податоци? Дали се врши пренос на лични податоци во други држави? Дали личните податоци се даваат на користење? Дали се обработуваат лични податоци врз основа на дадена согласност на субјектот на личните податоци?
3. Дали невладината организација обработува лични податоци согласно начелата за заштита на личните податоци?
4. Дали невладината организација има донесено документација за технички и организациски мерки за безбедност на личните податоци?
5. Како се остваруваат правата на субјектите на личните податоци?

6. Дали е определен офицер за заштита на личните податоци? Дали досега се вршени периодични контроли? Дали е вршена внатрешна и надворешна контрола на системот на обработка на личните податоци? Дали се вршело информирање и обуки за заштита на личните податоци?
7. Дали договорите што невладината организација ги има склучено со обработувачите содржат одредби за заштита на личните податоци?
8. Колкава е посветеноста на менаџментот во однос на спроведувањето на процедурите за заштита на личните податоци?

Сите овие прашања, а особено добиените резултати од самоевалуацијата на невладината организација ќе дадат јасна слика за примената на досегашните правила за заштита на личните податоци кои претставуваат темел на кој ќе треба да се надоградат сите новини од Законот за заштита на личните податоци, а особено во однос на:

1. Детектирање на природата, обемот, контекстот и целите на обработката на личните податоци, како и проценка на ризиците со различна веројатност и сериозност за правата и слободите на субјектите на личните податоци кои произлегуваат од обработката на нивните лични податоци;
2. Проверка и утврдување на правните основи за обработка на одделни категории на лични податоци;
3. Примена на новите начела за заштита на личните податоци;
4. Разгледување на потребата од надоградба и прилагодување на софтверски апликации и информатичката инфраструктура на невладината организација, согласно новите стандарди и заштитни мерки предвидени во Законот за заштита на личните податоци, а посебно од аспект на применливоста на техничка и интегрирана заштита на личните податоци (privacy by design and privacy by default);
5. Ажурирање на донесената документација за технички и организациски мерки за безбедност на личните податоци;
6. Нови заштитни мерки: псевдонимизација, криптирање...
7. Начин на кој ќе се овозможи остварувањето на новите права на субјектите на личните податоци. Начин на кој ќе се оствари транспарентност/видливост односно промоција

на правата на субјектите на личните податоци;

8. Проверка/ревизија на обработувачите во однос на постапувањето со личните податоци на невладините организации;
9. Периодични контроли, како и внатрешна контрола;
10. Положбата, улогата и задачите на офицерот за заштита на личните податоци;
11. Начини на информирање и обука на вработените/ангажираните лица/волонтерите /менаџментот на невладините организации;
12. Проверка на валидноста на согласноста како посебна категорија на основа за обработка на лични податоци. Постапката за барање согласност. Постапката за повлекување на согласност. Документирање. Следење на ажурираноста и валидноста на согласноста.
13. Потврдување на валидноста и ажурираноста на согласноста кога онлајн услугите се нудат директно на деца. Примена на соодветна постапка за добивање и повлекување на согласност на детето од неговиот родител или старател.
14. Посветеност на менаџментот во обезбедување безбедност при обработката на личните податоци, примена на начелата за заштита на личните податоци како предуслов за демонстрирање на отчетност.

Покрај наведените аспекти на усогласување со новата легислатива за заштита на личните податоци, предвид би требало да се имаат и следните препораки:

- Можноста за определување на заеднички офицер за заштита на личните податоци
- Изготвување и прифаќање на унифицирана изјава/политика за приватност која ќе биде објавена на веб страниците на невладините организации или направена јавно достапна на друг начин (а дополнително во интерни процедури ќе биде детално опишан начинот на остварувањето на правата на субјектите на личните податоци)
- Усвојување на иста методологија при правењето на проценка на влијанието врз приватноста од страна на сите невладини организации

- Изработка на заеднички кодекс на однесување при обработка на личните податоци имајќи ги предвид специфичните карактеристики на невладините организации
- Сертификација за заштита на личните податоци како алатка за демонстрирање на отчетност на невладините организации
- Континуирано информирање и обуки за заштита на личните податоци и континуирано вршење на ревизии во однос на обработката на личните податоци
- Заштитата на личните податоци и правото на приватност во врска со обработката на личните податоци треба да стане култура на однесување во невладините организации.

Ако појдеме од неспорниот факт дека Законот за заштита на личните податоци ја транспонира Општата регулатива за заштита на личните податоци (GDPR), а Регулативата има за цел да ги хармонизира правилата на игра за приватност во целата ЕУ, тогаш усогласеноста со Законот претставува императив за сите, па и за невладините организации, бидејќи и тие обработуваат лични податоци. Како што наведовме во воведот, Законот се однесува за профитните бизниси, но и за невладините организации, при што правилата се исти за сите, колку и да изгледаат сложени. Законот за заштита на личните податоци не е за она што е добро и благородно, туку за заштита на личните податоци на лицата и нивните права - нешто што едноставно важи без оглед дали субјектите на личните податоци ги даваат своите податоци за деловни активности или пак добротворни цели. Важно е да се нагласи дека дури и кога невладините организации се убедени дека во својата дејност прават нешто добро и општокорисно, кршењето на законот, во овој случај на Законот за заштита на личните податоци, е забрането.

Оттука, треба да се користат и применат добрите практики кои дел од невладините организации веќе ги применуваат и иако тоа на почетокот може да резултира со дополнителен „административен“ товар, на долги стази создавањето на цврсти темели за обработка на личните податоци не може да биде никако погрешно.

Имајќи ги предвид спецификите во дејствувањето на невладините организации, веројатно најчестите основи за обработка на личните податоци се, односно ќе бидат, согласноста и/или легитимниот интерес. Во однос на согласноста главната препорака е согласно

сеопфатниот опис погоре, невладините организации да се осигураат да добијат согласност од поединците за податоците кои што ги имаат и обработуваат. Невладините организации мора да ги известат точно субјектите на личните податоци за намерата што ќе направат со личните податоци и ќе ги споделат овие податоци со трети страни.

Доколку невладините организации имаат свои веб страници, правилото на однапред „штиклирани“ коцки за согласност едноставно повеќе не може да функционира. Во ваквите случаи, невладините организации ќе мора да обезбедат „opt-in“ техничко решение, односно на јасно поставени прашања и цели да добијат потврден одговор со означување на коцките од страна на субјектите на лични податоци. Комуницирајте ги правата на субјектот на јасен и разбирлив јазик. Информирајте ги субјектите колку што може посепфатно, а сепак тоа да биде на едноставен начин. Притоа, невладините организации треба да имаат предвид дека само затоа што некое лице се пријавило за нешто и побарало помош од одредена невладина организација, тоа никако не дава за право да се прави со нивните лични податоци што сака и како сака. Тоа не само што не е (повеќе) возможно, туку е и незаконито и за што се предвидени сериозни санкции. Кога станува збор за согласноста, невладините организации треба да се водат од многу едноставно правило - колку се посериозни и чувствителни податоците, толку повеќе заштитни мерки треба да се користат, а нивната обработка бара експлицитна и недвосмислена согласност.

Кога станува збор за легитимниот интерес, обработката на личните податоци никако не треба да претставува несоодветен товар и ризик за слободите на поединецот. Секогаш ќе мора да се процени објективно нивото на интерес на невладината организација и ризикот врз правата и слободите врз приватноста на поединецот кога ќе се користи легитимниот интерес како основа за обработка. Во многу случаи, легитимниот интерес ќе се поклопи со согласноста затоа што субјектот на личните податоци во некоја форма, или со некакво дејствие ќе ја изрази својата согласност кога се прибираат податоците од него, освен ако не се побараат од трето лице, но во тој случај субјектот ќе мора да биде известен, како што опширно објаснивме погоре. Во случај на директен маркетинг, ако некое лице бара оваа постапка да запре, тоа мора веднаш да биде направено, а невладината организација не може во ваков случај никако да докаже легитимен

интерес за обработка.

Секако и другите основи за обработка ќе се појават во секојдневното работење, но она што е важно е секогаш кога се обработуваат личните податоци, субјектот (оној чии податоци се обработуваат) секогаш да биде на пиедесталот, почитувајќи ги при тоа законитоста, транспарентноста и отчетноста.

Во однос на вработените во невладините организации и особено во однос на волонтерите, треба да се има предвид дека само затоа што се прави нешто општокорисно, или само затоа што се прави нешто бесплатно, не значи дека може да се прави што сака кога станува збор за обработката на личните податоци. Волонтерите имаат иста положба како и вработените. Затоа, препорака до невладините организации што треба да биде и добра практика е да се обезбеди добра едукација и тренинг за сите кои во име на невладините организации доаѓаат во контакт со, и обработуваат лични податоци. Вработените и волонтерите треба да имаат познавање за најдобрите практики за ракување со личните податоци, а невладните организации треба да воспостават контроли за пристап и редовни обуки за обновување и проширување на знаењето, бидејќи тие треба да бидат способни да го проценат влијанието и сериозноста на податоците со кои ракуваат. Ако се појде од правилото дека една организација е онолку силна колку што е силна нејзината најслаба алка, тогаш ваквите редовни тренинзи треба да станат нормална процедура за сите кои ракуваат со лични податоци.

НАМЕСТО ЗАКЛУЧОК: Поаѓајќи од тоа што веројатно правилата за заштита на личните податоци утврдени со Законот за заштита на личните податоци, не ретко изгледаат огромни и сложени, тие се всушност многу логични, ако правилно се разберат. Иако нивното првично донесување и примена може да изгледа сложено (отпор кон промени), треба да се разбере дека Законот дава и можности за негово „прилагодување“ кон спецификата на дејноста за која се применува за да биде во најдобар интерес на тие на кои конкретно се однесува, а со што ќе овозможи побезбеден начин на обработка на личните податоци. Притоа, членовите на невладините организации, но и вработените, волонтерите и оние чии податоци се обработуваат ќе бидат сигурни, знаејќи дека нивните податоци се обработуваат законски и на транспарентен и одговорен начин. Во таа смисла, една од исклучителните можности кои ги дава Законот е изработка на кодекси на однесување кои претставуваат еден вид „lex specialis“ за конкретна дејност. Имено, Законот меѓудругото утврдува дека согласно специфичните карактеристики на различните сектори на обработка на личните податоци, а со цел да се придонесе за правилна примена на овој закон, здруженијата и другите тела што ги претставуваат категориите на контролори или обработувачи можат да изработат кодекси на однесување со цел да биде прецизирана примената на законот, особено во однос на:

- правичната и транспарентна обработка;
- легитимните интереси на контролорите во специфични контексти;
- собирањето на личните податоци;
- псевдонимизацијата на личните податоци;
- информирањето на јавноста и на субјектите на лични податоци;
- остварувањето на правата на субјектите на лични податоци;

- информирањето и заштитата на децата и начинот на добивањето на согласност од законските застапници на детето;
- техничките и организациските мерки за безбедноста на личните податоци;
- известувањето на Агенцијата за заштита на личните податоци за нарушувањата на безбедноста на личните податоци и информирањето на субјектите на личните податоци за таквите нарушувања;
- преносот на личните податоци во трети земји или меѓународни организации; или
- вонсудските постапки и други постапки за решавање на спорови меѓу контролорите и субјектите на лични податоци во однос на обработката.

На ваков начин, со донесување на кодекс на однесување би се постигнал унифициран но и прилагоден и пред сè законит начин на обработка на личните податоци од страна на невладините организации.

КОРИСТЕНА ЛИТЕРАТУРА

1. Закон за заштита на личните податоци (Службен весник на Република Македонија“ бр. 7/05, 103/08, 124/08, 124/10, 135/11, 43/14, 153/15, 99/16 и 64/18)

2. Закон за заштита на личните податоци (Службен весник на Република Северна Македонија“ бр.42/20)

3. Општа регулатива за заштита на личните податоци (General Data Protection Regulation 679/16)

4. Коментари/толкување на нацрт - законот за заштита на личните податоци, Десислава Тошкова, Марија Матева, издавач: Дирекција за заштита на личните податоци

5. Водич низ правата на поединците во однос на обработка на личните податоци, Наталија Николов, издавач: Дирекција за заштита на личните податоци

6. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (ARTICLE 29 DATA PROTECTION WORKING PARTY)

7. Guidelines on Data Protection Officers (‘DPOs’) (ARTICLE 29 DATA PROTECTION WORKING PARTY)

8. Guidelines on the right to data portability (ARTICLE 29 DATA PROTECTION WORKING PARTY)

9. Guidelines on consent under Regulation 2016/679 (ARTICLE 29 DATA PROTECTION WORKING PARTY)

10. Guidelines on transparency under Regulation 2016/679(ARTICLE 29 DATA PROTECTION WORKING PARTY)

Web страници:

www.dzlp.mk

https://edpb.europa.eu/

https://www.cnil.fr/en/home

https://ico.org.uk/

https://www.aepd.es/es

АНЕКС 1 – ПРАШАЛНИК ЗА САМОЕВАЛУАЦИЈА

Листа за проверка на усогласеноста со Законот за заштита на личните податоци на граѓанските организации/ невладиниот сектор –

Прашалник за самоевалуација

Назив и седиште на здружението	
1. Дали здружението (контролорот) има воспоставено систем за заштита на личните податоци?	Да ☐ Не ☐
2. Дали менаџментот е информиран за обврските на раководството и вработените во постојниот систем за заштита на личните податоци и потребата од надоградба според новите правила предвидени во Законот за заштита на личните податоци?	Да ☐ Не ☐
3. Дали имате определено офицер за заштита на личните податоци? Да ☐ Не ☐	3.1 Дали офицерот има посетено обука за заштита на личните податоци? Да ☐ Не ☐
4. Дали вработените имаат посетено обука за заштита на личните податоци?	Да ☐ Не ☐
5. Дали водите евиденција на операциите за обработка?	Да ☐ Не ☐
6. Назив на збирката/ите на личните податоци:	- - -
7. Цел и законски основ на обработката	
8. Дали имате извршено проценка на влијанието на предвидените операции на обработка во однос на заштитата на личните податоци?	Да ☐ Не ☐
9. Дали имате збирки на лични податоци чијашто обработка е со висок ризик Да ☐ Не ☐	- - -

10. Дали вршите обработка на посебни категории на лични податоци? Наведете: Расно и етичко потекло Политички ставови Верски убедувања Генетски податоци Биометриски податоци Податоци што се однесуваат на здравјето Други: - - -	10.1 Наведете ги основите (закон, согласност...) според кои вршите обработка на посебни категории:
11. Дали вршите обработка на матичниот број на граѓаните? Да ☐ Не ☐	Наведете законски основ и цел на обработка на матичникот број (ЕМБГ):
12. Како се остваруваат правата на субјектите на личните податоци?	Опишете:
13. Дали имате донесено процедура во која е опишан начинот на остварување на правата на субјектите на личните податоци?	Да ☐ Не ☐
14. Дали имате изработено Изјава за приватност Да ☐ Не ☐	1.1. Дали истата е јавно достапна? Да ☐ Не ☐

15. Дали имате воспоставено процес на документирање на сите нарушувања на безбедноста на личните податоци? Да ☐ Не ☐	Опишете:
16. Дали имате склучено договор/и или друг правен акт во согласност со закон со обработувачот/ите?	Да ☐ Не ☐
17. Дали вршите пренос на лични податоци во други држави? Да ☐ Не ☐	17.1 Дали го имате пријавено или имате побарано одобрение за преносот од АЗЛП? Да ☐ Не ☐
18. Дали имате изработено и донесено Политика за системот за заштита на личните податоци во која се утврдени и начелата за безбедност и заштита на личните податоци?	Да ☐ Не ☐
19. Дали имате изработено и донесено подетални политики и процедури во кои се опишани техничките и организациски мерки за овластените лица кои имаат пристап до личните податоци и до информацискиот систем и информатичка инфраструктура Да ☐ Не ☐	Опишете:
20. Како се обработуваат личните податоци?	Рачно Автоматизирано Друго

21. Дали контролорот применува соодветни технички и организациски мерки за да обезбеди дека интегрирано се обработуваат само оние лични податоци кои се неопходни за секоја посебна цел на обработката (Data protection by design and by default)	Да ☐ Не ☐
22. Кои технички мерки за заштита на личните податоци ги применувате	Опишете:
23. Кои организациски мерки за заштита на личните податоци ги применувате	Опишете:
24. Дали се направени периодични и внатрешна контрола на информацискиот систем и информатичката инфраструктура	Да ☐ Не ☐
25.Дали вршите видео надзор? Да ☐ Не ☐	25.2 Дали го имате уредено начинот на вршењето на видео надзор со посебен акт? Да ☐ Не ☐
Датум на пополнување:	