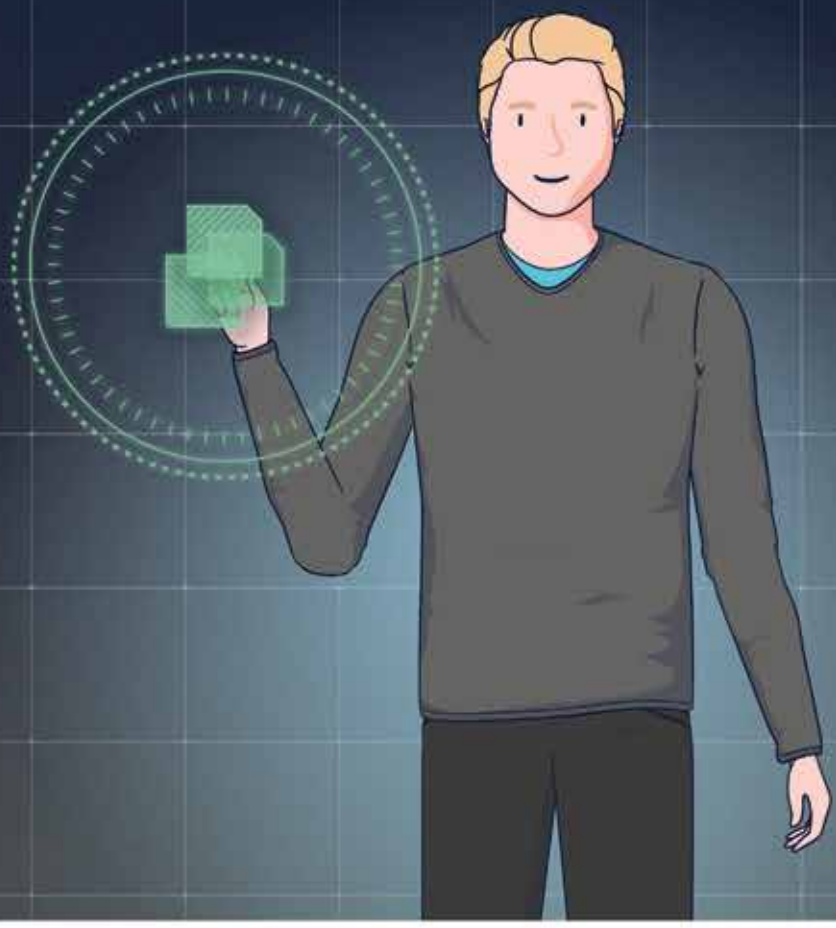
1

ВОДИЧ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ



ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

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

342.738(497.7)(036)

ТОШКОВА, Десислава
Водич за заштита на личните податоци / автори на документот Десислава Тошкова. - Скопје : Дирекција за заштита на личните податоци, 2018. - 83 стр. : илустр. ; 21 см

ISBN 978-608-4682-31-8

а) Заштита на лични податоци - Македонија - Водичи COBISS.MK-ID 108238858

ВОДИЧ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Издавач
Дирекција за заштита на личните податоци

Автори на документот
Десислава Тошкова

Лектура
Дијана Ристова

Дизајн
Маја Димеска-Крпач

Печатење
Пропоинт

Тираж
50 примероци

Февруари, 2018

ЕУ за ТЕБЕ!

Овој документ е изработен во рамки на проектот „Поддршка за пристап до правото на заштита на личните податоци“ EuropeAid 135668/IH/SER/MK, финансиран од Европската Унија преку ИПА ТАИБ 2012 програмата и спроведен од Vialto Consulting од Унгарија, во соработка со IPS Институт од Словенија и Националното тело за заштита на личните податоци и слобода на информации од Унгарија. Ставовите и мислењата наведени во овој прирачник во ниеден случај не ги изразуваат ставовите на Европската Унија.

СОДРЖИНА

1. Вовед

Заштитата на податоците е дел од државната политика за гарантирање на приватноста и безбедноста на поединците. Тоа е комплексен систем на права, обврски и овластувања што ги спроведуваат трите главни играчи: поединците (лицата на кои им припаѓаат личните податоци), контролорите на податоците (телата, институциите, ентитетите или лицата кои обработуваат лични податоци во текот на нивните секојдневни активности и чии вработени имаат пристап до таквите податоци) и надзорните органи (јавните институции кои ја контролираат обработката на лични податоци и изрекување санкции во случај на прекршување на правилата за заштита на личните податоци).

Правната рамка за заштита на личните податоци во светот ги воспоставува сопствените специфични правни концепти и идеи чие познавање е неопходен предуслов за правилно разбирање и правилна примена на задолжителните правила и во оваа област. Овој Водич за заштита на личните податоци има за цел да обезбеди основни информации и подигнување на свеста за знаење поврзано со заштитата на податоците со цел да им се олесни на контролорите на податоци, обработувачите на податоци и нивните вработени во процесот на ракување со лични податоци и оттаму обезбедување на нивна соодветна заштита.

Дефинициите на правните поими објаснети во овој Водич, како и правата на субјектите на податоците и обврските на контролорите/обработувачите на податоците се во согласност со новата Регулатива (ЕУ) 2016/679 на Европскиот парламент и на Советот од 27 април 2016 година за заштита на физичките лица во поглед на обработката на личните податоци и слободен проток на тие податоци и за укинување на Директивата 95/46/ЕК (Општа регулатива за заштита на лични податоци) и Предлог - законот за заштита на лични податоци со кој се транспонираат законските одредби од наведената Регулатива во Република Македонија.

2. Дефиниции

ЛИЧНИ ПОДАТОЦИ

Под поимот „лични податоци“ се подразбира која било информација поврзана со физичко лице (субјект на лични податоци) со која ова лице е неспорно идентификувано (идентификувано физичко лице) или може да се идентификува директно или индиректно (физичко лице кое може да се идентификува).

Дефиницијата за лични податоци содржи четири елементи како што се наведени подолу, кои треба сите да бидат присутни за одредени информации да се сметаат за лични податоци:

Секоја информација

Поимот лични податоци вклучува секоја информација за физичко лице (поединец), без оглед на неговиот капацитет (потрошувач, пациент, клиент, вработен) и без оглед на карактеристиките на информацијата - објективна (на пр. постоење на одредена супстанција во крвта) или субјективна (на пр. кредитоспособноста на банкарски клиент). Информацијата може да биде во различна форма - дигитална, графичка, фотографска, пишана, акустична и слично, а формата на податоците не е одлучувачка за утврдување дали информацијата е лична или не.

Поврзани со

За да се сметаат за лични податоци, информациите треба да бидат сродни/поврзани со одредено лице. Во повеќето случаи, поврзаноста со конкретно лице може да се утврди несомнено, на пр. податоци во личната папка на вработеното лице или податоците на пациентите содржани во медицинските досиеја. Меѓутоа, во некои случаи поврзаноста помеѓу одредени информации и конкретното физичко лице не е толку јасна. На пример, информациите за вредноста на недвижен имот вообичаено се однесуваат на самата недвижност, но исто така можат да бидат поврзани со сопственикот на имотот, бидејќи оваа вредност може да ја открие неговата/нејзината економска и финансиска состојба.

Идентификувано лице или лице кое може да се идентификува

Едно лице може да се смета за препознатливо (лице кое може да се идентификува) ако во рамките на една заедница на луѓе се издвојува од другите членови на заедницата. Идентификацијата се постигнува преку т.н. идентификатори, како што се име, идентификациски број, податоци за локација и онлајн идентификатор. Идентификацијата може да се направи и со еден или повеќе фактори специфични за физичкиот, физиолошкиот, генетскиот, менталниот, економскиот, културниот или социјалниот идентитет на физичкото лице. Таквите специфични фактори може да бидат име и презиме, постојана адреса, место на раѓање, информации за лична карта, семејни односи итн.

Законот не предвидува конкретна листа на информации што може да предизвикаат идентификација на лицето. Дали одредени информации претставуваат лични податоци, треба да се одлучува од случај до случај. Понекогаш одредени информации може да се сметаат за лични податоци, а понекогаш истото парче информација не може да биде заштитено како лично. Типичен пример е името на лицето - во некои случаи самото полно име на поединецот не може да го открие неговиот/нејзиниот идентитет директно или индиректно, особено во случај на многу вообичаени (што често се среќаваат) имиња, со тоа што може да бидат потребни и други дополнителни информации. Од друга страна, кога полното име на лицето е многу ретко, може да се смета дека е доволно да го истакне лицето од заедница на луѓе и на тој начин да го идентификува директно или индиректно.

Физичко лице

Само физички лица (поединци) поседуваат лични податоци. Правните лица, другите структури и/или организации немаат лични податоци и се исклучени од заштитниот режим на правилата за заштита на личните податоци.

ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Обработката е општ термин кој се користи за опишување на активностите/операциите што ги презема контролорот на податоците во однос на личните податоци под негова/нејзина контрола. Оваа операција или збир на операции може да се врши со автоматски или неавтоматски средства. Обработката може да биде во форма на собирање, евидентирање, организација, структурирање, зачувување, прилагодување или менување, пребарување, консултирање, употреба, објавување преку пренос, ширење или на друг начин правење на податоците да бидат достапни, усогласување или комбинирање, ограничување, бришење или уништување на лични податоци. Законодавецот ги има наведено исцрпно операциите за обработка и извршувањето на само една од нив и тоа е доволно за да се сметаат постапките на контролорите на податоците како обработка.

Практиката покажува дека најчести облици на обработка се собирање, зачувување и откривање на трети лица. Многу често контролорите на податоците кои престанале да вршат активности или повеќе не вработуваат вработени, сметаат дека не обработуваат лични податоци. Во практика, доколку ги задржуваат евиденциите на поранешните вработени за целите на трудот или даночното законодавство, тие и понатаму обработуваат лични податоци (во форма на зачувување на податоци) и покрај недостатокот на активности или на тековниот персонал.

Прекршочна одговорнос се врши за секоја операција за обработка на податоци која не е во согласност со Законот за заштита на личните податоци и релевантната форма на обработка може да се разгледува само во поглед на отежнувачки и / или олеснувачки околности на конкретен случај. На пример, откривањето на податоци на неидентификуван број на лица без правна основа е поризична операција на обработка отколку зачувување на податоците (без законска основа) со ограничен пристап до нив од страна на неколку вработени лица на контролорот на податоците и обезбедување на безбедносни мерки за тоа.

Законот за заштита на лични податоци се однесува на обработката на лични податоци, целосно или делумно со автоматски средства за обработка освен со автоматски средства на лични податоци кои се дел од системот за поднесување или се наменети да формираат дел од системот за поднесување.

Правилата и барањата за заштита на личните податоци не се однесуваат на обработка на лични податоци од страна на физичко лице во текот на чисто лична или домашна активност и на тој начин без никаква поврзаност со професионална или комерцијална активност. Личните или домашните активности може да вклучуваат кореспонденција и чување на адреси, или социјално вмрежување и интернет-активности кои се преземаат во рамките на контекстот на таквите активности. Сепак, режимот на заштитата на личните податоци се применува на контролори или обработувачи кои обезбедуваат средства за обработка на лични податоци за такви лични или домашни активности.

КОНТРОЛОР НА ЛИЧНИ ПОДАТОЦИ

Контролор на лични податоци е главниот субјект кој обработува лични податоци. Потребата за обработка или произлегува од законската обврска на контролорот или е потребна за извршување на неговите/нејзините главни активности. Контролорот на личните податоците може да биде физичко или правно лице, јавен орган, агенција или друго тело кое самостојно или заедно со други ги определува целите и средствата за обработка на лични податоци. Кога целите и средствата за обработка на податоци се утврдени со закон, контролорот или специфичните критериуми за неговото/нејзиното назначување се утврдени со закон.

Правната организациска форма на контролорот не е релевантна. Основни критериуми за утврдување на капацитетот на контролорот на личните податоци е дали тој/таа всушност одржува систем за поднесување.

Контролорот може да ги обработува податоците самостојно или со назначување на друг субјект кој е наречен обработувач на лични податоци.

Примери за контролори на лични податоци: работодавачот во контекст на труд во однос на личните податоци на вработените; мобилниот оператор во врска со податоците на клиентите; медицинската установа во врска со податоците на пациентите.

Во ситуации каде што е тешко да се идентификува точниот контролор на личните податоци, треба да се земат предвид следните прашања:

- кој ги одредува целите и средствата за обработка на личните податоци;
- кој ги контролира временските рокови за обработка на личните податоци;
- кој го одредува видот и категориите на лични податоци кои се предмет на обработка;
- кој ги одредува лицата кои можат да пристапат до податоците, како и третите лица кои можат да ги примат податоците.

Оној кој го воспоставува сето горенаведено е контролорот на личните податоци.

Правилното одредување на контролорот на лични податоци е од клучно значење во однос на идентификување на субјектот одговорен во случај на злоупотреба на личните податоци или повреди на правата на субјектите на податоците.

Во областа на заштита на личните податоци, контролорите имаат само обврски.

ОБРАБОТУВАЧ НА ЛИЧНИ ПОДАТОЦИ

Обработувач на податоци е физичко или правно лице, јавен орган или друго тело кое ги обработува личните податоци во име на контролорот.

Потребни се два предуслови за да се квалификува еден субјект како обработувач на лични податоци:

1. да биде одделен од контролорот на личните податоци и
2. да обработува лични податоци во име на контролорот на личните податоци.

Еден ист субјект може да има капацитет и како - контролор на податоци за некои од неговите/нејзините активности и како обработувач на податоци - за другите. Разликата е направена врз основа на видот и содржината на податоците, како и на конкретните операции за обработка на личните податоци. На пример, компанија чија главна дејност е наплата на побарувања и која е доделена од друга компанија (кредитна компанија) за наплата на побарувања на одделни должници, дејствува како контролор на лични податоци во однос на сопствените вработени и како обработувач на лични податоци во врска со податоците на должниците. Во случај на отстапување, тој има капацитет на контролор на лични податоци за двете категории на физички лица (вработени и должници), бидејќи повеќе не дејствува во име на доверителот (кредитната компанија), туку самостојно.

Односите помеѓу контролорот на лични податоци и обработувачот на лични податоци треба да се регулираат со договор или друг правен акт во согласност со законот кој е обврзувачки за обработувачот во однос на контролорот. Договорот или другиот правен инструмент треба да ја утврди содржината и траењето на обработката, природата и целта на обработката, видот на личните податоци, категориите на субјекти на податоци и обврските и правата на контролорот.

Слично на контролорите на лични податоци, обработувачите имаат само законски обврски.

СУБЈЕКТ НА ПОДАТОЦИ

Субјект на податоци е физичко лице (поединец) чии лични податоци се обработуваат и со кои тој или таа несомнено се идентификува или може да се идентификува, директно или индиректно. За да се утврди дали физичкото лице може да се идентификува, треба да се земат предвид сите средства кои можат да се користат, како што е издвојување, било од контролорот или од друго лице за да се идентификува физичкото лице, директно или индиректно. За да се утврди дали средствата можат да се користат за идентификување на физичкото лице, треба да се земат предвид сите објективни фактори, како што се трошоците за тоа и времето потребно за идентификација, земајќи ја предвид достапната технологија за време на обработката и технолошките достигнувања.

Субјектите на податоци уживаат широк спектар на права и законот не наметнува никакви обврски врз нив. Со остварување на правата во областа на заштита на личните податоци, законодавецот воведува правни гаранции дека субјектите на податоците имаат контрола врз нивните лични податоци.

Националноста на субјектите на податоци не е релевантна. Правилата за заштита на личните податоци се однесуваат на сите субјекти на податоци чии лични податоци се обработуваат од страна на контролорите на лични податоци на кои се однесува Законот за заштита на лични податоци. Додатно на тоа, субјектите на податоците уживаат заштита, без оглед на средствата за обработка на податоци - автоматска или рачна (доколку личните податоци се содржани или се наменети да бидат содржани во системот за поднесување).

При утврдување дали субјектот на податоците може да се идентификува, треба да се земе предвид дека физичките лица можат да бидат доведени во врска со онлајн идентификатори обезбедени од нивните уреди, апликации, алатки и протоколи, како што се адреси на интернет-протокол, идентификатори за колачиња или други идентификатори, како што се ознаки за радиофреквенција. Ова

може да остави траги кои, особено кога се комбинирани со единствени идентификатори и други информации добиени од серверите, може да се користат за креирање на профили на физичките лица и нивно идентификување.

ЗБИРКА НА ЛИЧНИ ПОДАТОЦИ

Под збирка на лични податоци се подразбира секој структуриран збир на лични податоци кои се достапни според специфични критериуми, без разлика дали се централизирани, децентрализирани или дисперзирани на функционална или географска основа. Со други зборови, збирката на личните податоци е собирање на лични податоци, без оглед на неговиот формат - хартиен или автоматски информативен систем. Освен ако поинаку не е предвидено со закон, контролорот на личните податоци може да ја структурира збирката по горенаведените три алтернативни пристапи: централизиран, децентрализиран и дисперзиран. Иако сите три пристапи се законски точни и еднакви, конкретниот избор на еден од нив треба да ги одразува специфичните активности на контролорот на личните податоци, поточно видот на личните податоци и целите на обработката на податоците. Дополнително, при одредувањето на збирките на личните податоци, контролорот на податоци, исто така, може да ги земе предвид категориите на субјекти на податоци, правната основа за обработка на личните податоци и периодот на зачувување.

Практиката покажува дека повеќето контролори на лични податоци претпочитаат дисперзиран функционален критериум бидејќи ја олеснува обработката на личните податоци. Инспекцискиот надзор е исто така подобро организиран, експедитивен и ефективен во случај на збирки на лични податоци врз основа на дисперзирана функционална основа. Примери за такви системи за поднесување се „персонал“/„човечки ресурси“, „клиенти“, „пациенти“, „изведувачи“ итн.

ПОСЕБНИ КАТЕГОРИИ НА ЛИЧНИ ПОДАТОЦИ

Посебни категории на лични податоци се податоци кои откриваат расно или етничко потекло, политички мислења, верски или филозофски убедувања или членство во синдикат, генетски податоци, биометриски податоци, здравствени податоци или податоци за сексуалниот живот на физичкото лице или сексуалната ориентација. Тие се нарекуваат „посебни категории на лични податоци" поради чувствителната природа на личните податоци што изискува поголема заштита. Во принцип, обработката на таквите податоци е забранета со закон. Сепак, постојат одредени отстапувања од оваа забрана и тие се експлицитно наведени во Законот за заштита на личните податоци. Овие отстапувања се алтернатива, што значи дека постоењето на едно од нив е доволно за да биде обработката законска. Неуспехот да се потпре на барем една од законските основи утврдени во чл. 13, став. 2 од Законот за заштита на лични податоци доведува до административна казнена одговорност.

Обработката на фотографии не треба систематски да се смета за обработка на посебни категории на лични податоци, бидејќи тие се опфатени со дефиницијата за биометриски податоци само кога се обработуваат преку специфични технички средства што овозможуваат единствена идентификација или автентикација на физичкото лице.

ЗЛОУПОТРЕБА НА ЛИЧНИТЕ ПОДАТОЦИ

Злоупотребата на личните податоци претставува злоупотреба на безбедноста што доведува до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, зачувуваат или кои на друг начин се

обработуваат. Злоупотребата на личните податоци претставува сериозна закана за достапноста, интегритетот и/или доверливоста на личните податоци. Може да доведе до физичка, материјална или нематеријална штета, како што е губење на контрола на субјектот на податоците врз сопствените лични податоци или ограничување на нивните права, дискриминација, кражба на идентитет или измама, финансиска загуба, неовластено враќање на псевдонимизацијата, оштетување на угледот, загуба на доверливоста на личните податоци заштитени со професионална тајност или која било друга значајна економска или социјална неповолност за засегнатото физичко лице.

Така, во случај на злоупотреба на личните податоци, релевантниот контролор на податоците е должен да ја извести Дирекцијата за заштита на личните податоци. Известувањето треба да се изврши без непотребно одложување, но не подоцна од 72 часа откако контролорот станал свесен за прекршокот. Контролорот се смета дека станал „свесен“ за прекршок кога контролорот има причина да верува дека настанал безбедносен инцидент кој довел до загрозување на личните податоци.

Во случаи кога злоупотребата на лични податоци е идентификувана од страна на обработувачот на лични податоци, тој/таа мора да го извести контролорот на лични податоци без непотребно одложување. Фактот што известувањето е направено без непотребно одложување треба да се утврди особено земајќи ја предвид природата и сериозноста на злоупотребата на личните податоци, неговите последици и негативни ефекти за субјектот на податоците. Препорачливо е обработувачот да испрати итно известување до контролорот, со дополнителни информации за злоупотребата, што се обезбедува во фази, како што информациите стануваат достапни. Ова ќе му олесни на контролорот да го исполни барањето за известување до надзорниот орган во рок од 72 часа. Онаму каде што обработувачот обезбедува услуги за повеќе контролори кои сите се засегнати од истата злоупотреба на лични податоци, обработувачот ќе мора да ги пријави деталите за инцидентот на секој контролор.

Известувањето може да резултира со интервенција на надзорниот орган во согласност со неговите задачи и овластувања утврдени со Законот за заштита на личните податоци.

Законот за заштита на личните податоци ги утврдува барањата на известувањето за злоупотреба на личните податоци.

Во случаи кога злоупотребата на личните податоци може да резултира со висок ризик за правата и слободите на физичките лица (на пример, злоупотреба на лични податоци што вклучува чувствителни податоци), контролорот ќе ја соопшти злоупотребата на личните податоци и на субјектот на податоците без непотребно одложување (на пр. што е можно поскоро). Комуникацијата треба да ја опише природата на злоупотребата на лични податоци, како и информации за контактните податоци на офицерот за заштита на личните податоци, можните последици од злоупотребата на личните податоци и преземените мерки или предложени да се преземат од контролорот за решавање на злоупотребата на лични податоци, вклучувајќи, каде што е соодветно, мерки за ублажување на можните несакани ефекти.

При проценка на ризикот за поединци препорачливо е контролорот да ги земе предвид следните аспекти:

- ✓ видот на злоупотреба на личните податоци (на пр. повреда на доверливоста);
- ✓ природата и обемот на личните податоци;
- ✓ можност за евентуална идентификација на поединците;
- ✓ евентуални последици за поединците и нивната тежина (на пример кражба на идентитет, оштетување на угледот);
- ✓ категории на субјектите на податоци (на пример, деца или други ранливи групи на луѓе).

Нема потреба од комуникација за злоупотреба на личните податоци до субјектот на податоците, доколку се исполнети некои од следните услови:

(а) контролорот има имплементирано соодветни технички и

организациски мерки за заштита и тие мерки се применуваат на личните податоци засегнати од злоупотребата на лични податоци, особено оние што ги прават личните податоци неразбирливи на кое било лице кое не е овластено да пристапува до нив, како што е енкрипцијата;

(б) контролорот ги презел следните мерки со кои се обезбедува дека високиот ризик за правата и слободите на субјектите на податоци понатаму не е веројатно дека ќе се материјализира;

(в) вклучува диспропорционален напор. Во таков случај, наместо тоа, ќе постои јавна комуникација или слична мерка со која субјектите на податоците се информираат на подеднакво ефикасен начин.

Во согласност со принципот на одговорност, контролорите треба да бидат во можност да обезбедат доказ дека исполнуваат еден од горенаведените услови.

За да се спречи злоупотребата на личните податоци, контролорот и обработувачот се должни да преземат соодветни безбедносни мерки. Дополнително, контролорот треба да води документација за злоупотреба на податоците, вклучувајќи ги и фактите што се однесуваат на злоупотребата на личните податоци, неговите ефекти и преземените мерки за поправање.

НАДЗОРЕН ОРГАН

Надзорниот орган е независен јавен орган одговорен за следење на спроведувањето на правилата и барањата за заштита на личните податоци. За Република Македонија ваков орган е Дирекцијата за заштита на лични податоци (Дирекција). Дирекцијата е независен и самостоен орган на државната администрација надлежен за следење на законитоста на активностите преземени при обработката на личните податоци на територијата на Република Македонија,

како и за заштита на основните права и слободи на физичките лица во врска со обработката на нивните лични податоци. Таа ги надгледува и контролира сите контролори и обработувачи на податоци. Не е надлежна да ги надгледува само операциите за обработка на судовите кои дејствуваат во нивната судска надлежност. Сепак, вакви от надзор над законитоста на активностите преземени за време на други активности за обработка на лични податоци што ги вршат судовите спаѓа во надлежност на Дирекцијата.

Дирекцијата има широк спектар на задачи и овластувања меѓу кои овластување за истрага, корективни овластувања и санкции, одобрување и советодавни овластувања. Овие овластувања вклучуваат и моќ да наметнуваат привремени или дефинитивни ограничувања, вклучувајќи забрана на обработката.

Дирекцијата е одговорна за своите активности пред Собранието на Република Македонија. Нејзините одлуки се предмет на судска заштита.

ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Офицер за заштита на личните податоци (ОЗЛП) е лице назначено од контролорот на податоците или обработувачот да му помогне во следење на внатрешната усогласеност со барањата за заштита на личните податоци и да дава совети и консултации за прашањата за заштита на личните податоци. Таквиот офицер за заштита на личните податоци, без разлика дали е вработено лице на контролорот/обработувачот, има право да ги врши своите обврски и задачи на независен начин и никој не може да му/ѝ даде инструкции во врска со извршувањето на тие задачи. Независноста на ОЗЛП е загарантирана со законска забрана за отпуштање или казнување од страна на контролорот или обработувачот за извршување на неговите/нејзините задачи. Офицерот е, исто така, должен да поднесува из-

вештаи директно до највисоко ниво на управување на контролорот или обработувачот.

Законот за заштита на личните податоци му дозволува на ОЗЛП да биде или вработено лице кај контролорот или обработувачот или да ги исполни задачите врз основа на договор за услуги. Конкретниот избор на начин на назначување на ОЗЛП останува на одлуката на релевантниот контролор на лични податоци или обработувач со цел да се одразат посебностите на нејзината организација на работа и да се избегне непотребното административно оптоварување.

Законодавецот наметнува обврска на контролорот и обработувачот да обезбеди дека офицерот за заштита на личните податоци е вклучен, правилно и навремено, во сите прашања поврзани со заштитата на личните податоци. Тие, исто така, треба да му/ѝ ги обезбедат сите ресурси потребни за извршување на задачите и пристап до личните податоци и операциите за обработка, како и да го одржат своето стручно знаење.

Означувањето на ОЗЛП е задолжително во кој било од следниве случаи:

- кога обработката ја врши јавно тело, освен за судовите кои дејствуваат во нивната судска надлежност;
- основните активности на контролорот или обработувачот се состојат од операции за обработка кои според својата природа, нивниот опфат и/или нивните цели, бараат редовно и систематско следење на субјектите на податоци во голем обем;
- основните активности на контролорот или обработувачот се состојат од обработка во голем обем на посебни категории на податоци и лични податоци кои се однесуваат на кривични пресуди и прекршоци.

Со цел да се обезбеди флексибилност за контролорите и обработувачите на лични податоци, законот предвидува можност за група на правни лица да назначат еден единствен офицер за заштита на личните податоци под услов офицерот за заштита на личните

податоци да биде лесно достапен за секое правно лице. Истото е обезбедено и за јавните тела - единствен офицер за заштита на лични податоци може да биде назначен за неколку такви тела, водејќи сметка за нивната организациска структура и големина.

Субјектите на податоците можат да го контактираат офицерот за заштита на личните податоци во врска со сите прашања поврзани со обработката на нивните лични податоци и остварувањето на нивните права според овој закон.

Офицерот за заштита на личните податоци е одговорен за следните задачи:

- да го информира и советува контролорот или обработувачот и вработените кои вршат обработка во согласност со нивните обврски согласно со прописите за заштита на личните податоци, како и според други прописи кои се однесуваат на заштита на личните податоци;
- да го следи усогласувањето со Законот за заштита на личните податоци и со другите одредби за заштита на личните податоци и со политиките на контролорот или обработувачот во врска со заштитата на личните податоци, вклучувајќи ја и распределбата на одговорности, подигнување на свеста и обука на персоналот во операциите за обработка, како и ревизии за заштита на личните податоци;
- каде што е потребно, да дава совети за проценка на влијанието врз заштитата на податоците и да го следи неговото работење;
- да соработува со Дирекцијата за заштита на лични податоци и да дејствува како контакт-точка за прашања во врска со обработката, вклучувајќи ги таканаречените претходни консултации и да консултира, онаму каде што е соодветно, во однос на сите други прашања.

ДИРЕКТЕН МАРКЕТИНГ

Директен маркетинг е секој тип на комуникација која се одвива на кој било начин со цел да се пренесат рекламни, маркетинг или огласни материјали кои се директно насочени кон одреден субјект на податоци. Обработката на лични податоци за цели на директен маркетинг е дозволена само со согласност на субјектот на податоците, освен ако со закон не е поинаку определено. Субјектот на лични податоци има право да ја повлече својата согласност за обработка на лични податоци за целите на директен маркетинг во секое време и бесплатно, а со користење на едноставни средства.

Додатно на тоа, кога личните податоци се обработуваат за цели на директен маркетинг, субјектот на податоците има право на приговор во секое време на обработката на лични податоци кои се однесуваат на него или неа за таков маркетинг, вклучувајќи профилирање до степенот до кој е поврзан со таквиот директен маркетинг.

Правото на приговор се однесува на почетната и на понатамошната обработка, а може да се остварува во секое време и е бесплатно. Контролорот е должен експлицитно да обрати внимание на субјектот на податоците до тие информации и да го прикаже јасно и одделно од секоја друга информација.

Кога субјектот на податоците приговара на обработката за цели на директен маркетинг, контролорот е должен да ја прекине обработката на лични податоци за такви цели.

Најосновните елементи на директен маркетинг се следниве:

- Содржината на типот на комуникација - содржината може да варира. Може да се однесува на понуда на добра и услуги, обезбедување на рекламни и маркетинг- материјали, консултации и истражување на понудените добра и услуги;
- Видот на средствата за комуникација - комуникацијата може да се врши по телефон, пошта или кој било друг директен начин на комуникација;

- Примателите на директен маркетинг - конкретно одредено и директно насочено кон физичко лице/лица. Овој елемент е од витално значење за диференцијација помеѓу директен маркетинг и рекламирање. Примателите на рекламирањето не се директно идентификувани, додека директниот маркетинг е секогаш насочен кон одредено физичко лице. Рекламната брошура не содржи никакви лични податоци; не е директно упатена кон идентификувано лице и не обезбедува никаков одговор во име на конкретно физичко лице. Рекламата рекламира добра или услуги и/или поттикнува реализација на такви добра и услуги на широка неидентификувана публика.

ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ПОДАТОЦИТЕ

Проценка на влијанието врз заштитата на податоците (ПВЗП) е процес дизајниран да ја опише обработката на личните податоци, да ја процени потребата и пропорционалноста на обработката и да помогне во справувањето со ризиците за правата и слободите на физичките лица кои произлегуваат од обработката на личните податоци.

Целта на ПВЗП е да се зголеми усогласеноста со правилата за заштита на личните податоци, каде што операциите за обработка веројатно ќе резултираат со висок ризик за правата и слободите на физичките лица. Со спроведување на ПВЗП контролорите на личните податоци ги оценуваат потеклото, природата, посебноста и сериозноста на високите ризици за правата и слободите на физичките лица и ги одредуваат мерките за нивно решавање.

Спроведувањето на ПВЗП не е задолжително за секоја операција на обработка која може да резултира со ризици за правата и слободите на физичките лица, но само кога обработката „веројатно ќе резултира со висок ризик за правата и слободите на физичките лица".

ПВЗП треба да се изврши пред обработката. Периодичен преглед на ПВЗП е задолжителен во случај на промена на ризикот предизвикан од операциите на обработка.

Дирекцијата за заштита на личните податоци воспоставува и одржува список на видови операции на обработка кои се предмет на барање за проценка на влијанието врз заштитата на податоците. Дирекцијата исто така може да воспостави и да објави список на видови операции на обработка за кои не е потребна проценка на влијанието врз заштитата на податоците.

Проценка на влијанието врз заштитата на податоците е потребна во кој било од следниве случаи (списокот подолу е задолжителен, но не е целосен):

(а) во случај на систематска и детална евалуација на личните аспекти кои се однесуваат на физички лица што се засноваат на автоматска обработка, вклучувајќи профилирање и врз кои се засноваат одлуките кои произведуваат правни последици во однос на физичкото лице или кои на сличен начин значително влијаат врз физичкото лице (на пример, собирањето на податоци од јавните профили на социјалните медиуми кои ќе ги користат приватни компании кои создаваат профили за директориуми за контакт);

(б) во случај на обработка во голем обем на посебни категории на податоци или на лични податоци кои се однесуваат на кривични пресуди и прекршоци. Пример за таква обработка која бара ПВЗП е случајот кога болницата ги обработува генетските и здравствените податоци на своите пациенти во болничкиот информативен систем. Обработката на личните податоци не се смета дека е во голем обем во случај на податоци за пациенти или клиенти кои се обработуваат од страна на поединец лекар, друг здравствен работник или адвокат. Во такви случаи, проценката на влијанието врз заштитата на податоците не е задолжителна.

(в) во случај на систематско следење на јавно пристапна област во голем обем. Еден пример е употребата на систем за камера

за следење на однесувањето на возачите на автопатите. Мониторингот е систематски и претпоставува употреба на иновативни технологии или други технолошки или организациски решенија.

ПВЗП не е потребна во следните случаи:

- каде што обработката нема „веројатно да резултира со висок ризик за правата и слободите на физичките лица“;
- кога природата, обемот, контекстот и целите на обработката се многу слични на обработка за која била спроведена ПВЗП. Во такви случаи, може да се користат резултатите од ПВЗП за сличната обработка;
- кога операцијата на обработка има правна основа во законот каде што законот ја регулира конкретната операција на обработка и каде што ПВЗП веќе е извршена како дел од воспоставувањето на таа правна основа;
- кога обработката е вклучена во изборен список на операции за обработка за кои не е потребна никаква ПВЗП (доколку таквиот список го утврди Дирекцијата за заштита на лични податоци). Во такви случаи, ПВЗП не е потребна, но само ако обработката спаѓа строго во рамките на релевантната постапка наведена во списокот и продолжува целосно да се усогласува со соодветните барања.

ПВЗП мора да биде документирана и треба да ги содржи најмалку следните информации:

а) систематски опис на предвидените операции на обработка и целите на обработката, вклучувајќи го, каде што е применливо, легитимниот интерес на контролорот;

б проценка на неопходноста и пропорционалноста на операциите на обработка во однос на целите;

в) проценка на ризиците за правата и слободите на субјектите на податоците и

г) мерките предвидени за справување со ризиците, вклучувајќи

ги заштитните мерки, безбедносните мерки и механизми за обезбедување на заштита на личните податоци и за демонстрирање на усогласеност со Законот за заштита на личните податоци, земајќи ги предвид правата и легитимните интереси на субјектите на податоците и другите засегнати лица.

Во постапката на извршување на ПВЗП контролорите на лични податоци, исто така, треба да земат предвид:

- придржување кон одобрениот кодекс на однесување, особено за целите на заштита на личните податоци.
- ставовите на субјектите на податоците или на нивните претставници за планираната обработка.

Контролорот на личните податоци може да му додели на ОЗЛП да дава совети за проценката на влијанието врз заштитата на податоците и да ја следи нејзината изведба.

Единечна ПВЗП може да се користи за да се проценат повеќе операции на обработка кои се слични во однос на презентираните ризици, под услов да се даде соодветно внимание на специфичната природа, опсег, контекст и цели на обработката.

Исто така е можно да се развијат рамки за ПВЗП кои се специфични за одредени сектори. Таквите секторски ориентирани ПВЗП можат да се осврнат на специфичностите на одреден тип на операција на обработка (на пример: одредени типови на податоци, корпоративни средства, потенцијални влијанија, закани, мерки), користејќи конкретни технологии или кои било други секторски посебности кои влијаат на обработката на податоците.

Исто така е можно да се спроведе ПВЗП со широка содржина. Тоа може да биде случај кога јавните органи или тела имаат намера да основаат заедничка апликација или платформа за обработка или каде што неколку контролори планираат да воведат заедничка апликација или средина за обработка во индустриски сектор или сегмент или за широко употребувана хоризонтална активност.

3. Принципи за обработка на лични податоци и услови за законитост на обработката на податоците[2]

Постојат одредени барања кои треба да бидат присутни со цел обработката на личните податоци да биде законска. Ова се принципите кои се однесуваат на обработката на личните податоци и условите за законитост на обработката.

ПРИНЦИПИ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Во моментов Законот за заштита на личните податоци поставува 7 принципи за обработка на лични податоци: законитост, праведност и транспарентност; ограничување на целта; минимизација на податоците; точност; ограничување на зачувувањето; интегритет и доверливост; одговорност. Сите тие мора да бидат присутни во секое време на животниот циклус на обработката на лични податоци и недостатокот на дури еден од нив претставува прекршување на барањата за заштита на податоците. Принципите на заштита на податоците не треба да се применуваат на анонимни информации (информации кои не се однесуваат на идентификувано или препознатливо физичко лице) или на лични податоци кои се анонимни на таков начин што субјектот на податоците не е идентификуван или веќе не може да се идентификува.

Принцип на законитост, праведност и транспарентност

Според овој принцип, личните податоци мора да се обработуваат законски, праведно и на транспарентен начин во однос на субјектот на податоците. За да биде законска, обработката треба да

2. Референци за ова поглавје: мислења и упатства на Работната група 29: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

биде поврзана со активност која е во согласност со законот во поширока смисла. Обработувачката активност на контролорот/обработувачот на лични податоци е законска доколку се спроведува врз основа на законот и релевантната законска рамка е формулирана на јасен и прецизен начин за да може лицата да го приспособат своето однесување на неа. Ако обработката е во согласност со законот, тогаш исто така се смета дека е праведна. Понатаму, обработката на личните податоци треба да биде транспарентна за физичките лица, 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. Принципот на транспарентност бара сите информации во врска со обработката на тие лични податоци кои се однесуваат на субјектот на податоците да бидат лесно достапни и лесно разбирливи. Така, препорачливо е во сите комуникации со субјектот на податоците контролорите/обработувачите да користат јасен и едноставен јазик. Исто така е соодветна употребата на визуелизација или употреба преку веб-страница. Физичките лица 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 неговата/нејзината обврска да обезбеди транспарентни информации, контролорот/обработувачот треба да ги земе предвид специфичните околности и контекстот во кој се обработуваат личните податоци. Пример за транспарентна обработка е обврската на контролорите на личните податоци да ги информираат субјектите на податоци за постоењето на профилирање и последиците од таквото профилирање. Кога личните податоци се собираат од субјектот на податоците, субјектот на податоците исто така треба да биде информиран дали тој или таа е должен да ги достави личните податоци и на последиците, доколку тој или таа не ги достави таквите податоци. Таа информација може да се обезбеди во комбинација со стандардизирани икони со цел да му се дозволи лесно видлив, разбирлив и на јасно читлив начин, значаен преглед на планираната обработка. Каде што иконите се презентираат електронски, тие треба да бидат машински читливи.

Принцип на ограничување на целта

Овој принцип бара личните податоци да се собираат за конкретни, експлицитни и легитимни цели и да не се обработуваат понатаму на начин кој е некомпатибилен со тие цели. Како по правило, целите за кои треба да се обработуваат податоците треба да се утврдат пред нивното собирање. Тие треба да бидат специфични, законски основани и експлицитни (да не се дозволува нивно толкување). Овој принцип е многу важен во случај кога целите на обработката се идентификувани од страна на самите контролори на лични податоци (не е експлицитно утврдено во законот). 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. Меѓутоа, понатамошната обработка за цели на архивирање во јавен интерес, за научни или историски истражувачки цели или статистички цели не се смета за некомпатибилна со првичните цели.

Принцип на минимизазија на податоците

Принципот на минимизација на податоците пропишува дека личните податоци треба да бидат соодветни, релевантни и ограничени на она што е неопходно за целите за кои се обработуваат. Овој принцип бара контролорот/обработувачот на личните податоци да го обработува само минималниот обем на податоци апсолутно неопходни за постигнување на релевантната цел на обработката на податоците. Сите други податоци надвор од таа граница се сметаат за прекумерни и непропорционални. Понатаму, личните податоци треба да бидат обработени само ако целта на обработката не може разумно да се постигне со какви било други средства. На пример, вработените на контролорот на податоците кои се одговорни за контрола на пристапот често прават копија од пасошите на посетителите, ги скенираат или дури ги задржуваат документите. За целите на контрола на пристап, доволно е да се потврди иденти-

тетот на лицето и само да се запишат податоци за идентификација од пасошот. Правењето на копија или скенирање на документи за лична идентификација се смета за прекумерно. Истото се однесува и на услугите за хотелско сместување, каде што вработените при регистрирањето често ги задржуваат документите на посетителите и ги скенираат, наместо едноставно да ги запишат потребните податоци за идентитетот на гостите на хотелот.

Дури и ако постои претходна согласност од субјектот на податоците за обработка на повеќе информации отколку што е неопходно (на пример, контролорот на податоци има валидна правна основа за обработка на лични податоци), контролорот/обработувачот на податоците ќе биде сметан како одговорен за кршење на принципот на минимизација на податоците. Ова е така затоа што тој/таа нема потреба да има знаење за тоа одредено парче податоци што е прекумерно и без кое целите на обработката во секој случај би се постигнале.

Принцип на точност

За да биде законско обработувањето на лични податоци, контролорот на податоци треба да обработува точни и ажурирани информации. Поради тоа, личните податоци мора да бидат точни, а кога е тоа потребно, да се ажурираат. Понатаму, податоците треба да се избришат или отстранат ако се утврди дека тие се неточни или непропорционални во однос на целите за кои се обработени.

Практичната имплементација во име на контролорот/обработувачот на овој принцип понекогаш зависи од праведното однесување на субјектот на податоците. На пример, кога едно лице отвора банкарска сметка, од него/неа се бара да изнесе одредена количина на лични податоци за цели на идентификација. Вообичаено, постапката на идентификација бара обезбедување на податоци снимени во личните карти на клиенти. По истекот на личната карта или промена на постојаната адреса, клиентот треба да ги достави овие информации до банката за да ѝ овозможи на банката да обработува точни податоци поврзани со него. Ако не, вработе-

ните во банката се должни да ги ажурираат податоците веднаш штом ќе откријат дека информациите се променети и дека информациите што ги имаат повеќе не се релевантни.

Принцип на ограничување на зачувувањето

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. Принципот на ограничување на зачувувањето бара да се осигура дека периодот за кој се чуваат личните податоци е ограничен на строгиот минимум, со други зборови дека секогаш постои рок за зачувување. Со цел да се осигура дека личните податоци не се чуваат подолго отколку што е неопходно, контролорот треба да утврди конкретни временски ограничувања за зачувувањето по истекот за тоа кои податоци треба да се избришат или за периодичен преглед на неопходноста на податоците.

Понекогаш самиот закон одредува конкретни временски рокови за зачувување на одредени лични податоци. Нормативен рок, на пример, е утврден во Законот за трговските друштва според кој сметководствените документи се чуваат најмалку пет години по истекот на годината во која се користат за изработка на трговски книги, со исклучок на документите за пресметка на платите, кои се чуваат трајно.

Личните податоци може да се чуваат подолго време, сè додека личните податоци се обработуваат исклучиво за цели на архивирање во јавен интерес, за научни или историски истражувачки цели или за статистички цели, предмет на спроведување на соодветни технички и организациски мерки, со цел да се заштитат правата и слободите на субјектот на податоците.

Принцип на интегритет и доверливост

Личните податоци треба да се обработуваат на начин кој обезбедува соодветен интегритет и доверливост на личните податоци, вклучувајќи и спречување на неовластен пристап или незаконска

обработка, случајно губење, уништување или оштетување, или користење на лични податоци и опрема за обработката. Имплементацијата на овој принцип е обезбедена со преземање на соодветни технички или организациски мерки.

Принцип на одговорност

Принципот на одговорност има за цел да гарантира дека контролорите на личните податоци се во контрола и во позиција да обезбедат и демонстрираат усогласеност со принципите за заштита на личните податоци во пракса. Целта на овој принцип е да ја потврди и да ја зајакне одговорноста на контролорите за обработката на личните податоци.

Принципот на одговорност се состои од два главни елементи:

(I) одговорноста на контролорот да преземе соодветни и ефективни мерки за спроведување на принципите за заштита на личните податоци во пракса;

(II) способноста да се демонстрира, по барање, на надворешните засегнати страни, вклучувајќи ги и надзорните органи, дека се преземени соодветни и ефективни мерки за спроведување на принципите во пракса. Контролорот е должен да обезбеди докази за тоа.

Принципот на одговорност се однесува на сите контролори на лични податоци и на сите ситуации за обработка на податоци. Меѓутоа, препорачливо е конкретните мерки преземени од страна на контролорите да одговараат на ризиците претставени со обработката на податоците и на природата на личните податоци.

Препорачливо е контролорите да применуваат и механизми за проценка на ефикасноста (или неефикасноста) на мерките: следење, внатрешни и надворешни ревизии итн.

Следното е неисцрпна листа на заеднички мерки за одговорност кои можат да се применат од контролорите на личните податоци:

- Поставување на политики за заштита на личните податоци кои треба да им бидат достапни на субјектите на податоците и да се врзат за вработените на контролорите;
- Именување на офицер за заштита на личните податоци во случаи кога назначувањето на таквиот службеник не е задолжително;
- Обука, едукација на вработените и спроведување на програми за подигнување на свеста;
- Имплементација на механизми за сертификација;
- Поставување на внатрешни процедури за примена на правата на субјектите на податоците кои треба да бидат транспарентни на субјектите на податоците;
- Поставување на внатрешни процедури за ефикасно управување и известување на злоупотреба на податоците.

УСЛОВИ ЗА ЗАКОНИТОСТ НА ОБРАБОТКАТА НА ПОДАТОЦИТЕ

Обработката на лични податоци е законска само ако барем еден од условите утврдени во чл. 10, став. 1од Законот за заштита на лични податоци е присутен (законска основа за обработка на податоци). Важно е да се нагласи дека овие законски основи за обработка на податоците се еднакви, алтернативни и законот не ги рангира според нивната важност. Сите тие се однесуваат на контролорите на податоците во јавниот и приватниот сектор. Информациите подолу го појаснуваат обемот и содржината на секој од нив.

Согласност на субјектот на податоците

Согласност на субјектот на податоците значи секое слободно дадено, специфично, информирано и недвосмислено назначување на

желбите на субјектот на податоците со кое тој или таа, со изјава или со јасно потврдување на дејството, означува согласност за обработка на лични податоци кои се однесуваат на него/неа. Согласноста како правна основа за обработката на личните податоци традиционално е поврзана со концептот дека субјектите на податоците треба да имаат контрола врз нивните лични податоци. Важно е да се спомене дека достапноста на согласноста од субјектот на податоците не ја укинува обврската на контролорот на податоците да обработува податоци во согласност со принципите за заштита на личните податоците како што се наведени погоре.

Согласноста е само една алтернатива меѓу сите законски основи за обработка, така што не е неопходно, а понекогаш дури и несоодветно, операциите за обработка да се засноваат на согласност. Сепак, согласност е секогаш потребна кога не се применува ниту една друга законска основа за обработка на личните податоци.

Не постои одреден временски рок за согласност. Колку долго ќе трае зависи од контекстот на обработката на податоците. Оттука, препорачливо е периодично да се прегледува согласноста и секогаш кога се појавуваат промени во параметрите за обработка на податоците, како што се промена во целите на обработката, природата на податоците, временските рокови за зачувување, примателите на податоци, итн.

Доказот за достапност на согласноста е товар на контролорот на податоците и оваа обврска се покренува поради принципот на одговорност.

Општи барања

За да биде валидна правната основа за обработка на личните податоци, согласноста на субјектот на податоците мора да ги исполнува следниве барања:

- Согласноста мора да биде слободно дадена

Согласноста се смета за валидна само ако поединецот ја изразува својата слободна волја без никаков ризик од закана, присила или

негативни последици врз него/неа. Согласноста не треба да се смета за слободно дадена ако субјектот на податоците нема вистински или слободен избор или не е во можност да одбие или да ја повлече согласноста без штета на него/неа. Контролорот треба да покаже дека е можно да се одбие или да се повлече согласноста без штета (на пример, повлекувањето е без трошоци за субјектот на податоците).

Ако некое лице е под надзор на контролорот на лични податоци, на пример во контекст на вработување или кога контролорот е јавно тело, постои одредена нерамнотежа помеѓу субјектот на податоците и контролорот. Фактот што тој/таа може да биде во зависен статус во однос на контролорот фрла основани сомнежи врз слободата на неговото/нејзиното изразување. Поради тоа, во такви случаи, по правило, согласноста не треба да се смета дека е слободно дадена. Сепак, тоа не значи дека работодавците или јавните власти никогаш не можат да се потпрат на согласноста како законска основа за обработка. Потребно е да се земе предвид врз основа од случај во случај.

Се претпоставува дека согласноста не е слободно дадена ако не дозволува да се дава одделна согласност за различни операции за обработка на лични податоци.

Кога се проценува дали согласноста е слободно дадена, треба да се води најголема сметка дали, меѓу другото, извршувањето на договорот, вклучувајќи го и обезбедувањето на услугата, е условено на согласност за обработка на личните податоци што не се неопходни за извршување на тој договор. Така, по правило, согласноста не може да биде предуслов за пријавување за некоја услуга. Ако согласноста е во комплет како непреговарачки дел од правилата и условите, се претпоставува дека не е слободно дадена.

- Согласноста мора да биде одредена

Согласноста за обработка на лични податоци мора да ја даде одредено лице за одредени цели. Општа согласност без наведување на конкретната цел за обработка на податоците не се смета за одредена индикација за волјата на субјектот на податоците. Доколку

во подоцнежната фаза се изврши промена во целите за обработка на податоците, субјектот на податоците мора да биде соодветно информиран и треба да му се даде можност да ја изрази својата одредена согласност за новата (или натамошна) обработка на податоци.

Нејасната или општа согласност не е доволна и не може да се смета за одредена.

Контролорот кој бара согласност за различни цели треба да обезбеди посебна одлука (opt-in) за секоја цел за да им овозможи на субјектите на податоците да изразат одредена согласност за одредени цели.

Ако согласноста на субјектот на податоците е дадена во контекст на писмена изјава која исто така се однесува и на други прашања, барањето за согласност треба да се презентира на начин кој е јасно различен од другите прашања, во разбирлива и лесно достапна форма, со користење на јасен и едноставен јазик. Секој дел од таквата изјава што претставува прекршување на Законот за заштита на личните податоци нема да биде обврзувачки.

- Согласноста мора да биде информирана

Со цел согласноста да биде валидна од гледна точка на заштитата на личните податоци, субјектот на податоците има право на сите достапни информации поврзани со обработката на податоците пред да се изрази согласност. Поточно, тој/таа треба да го знае идентитетот на контролорот на податоците или неговиот застапник, целта на обработката на податоците, информациите за операциите за обработка на податоци, примателите или категориите на примател на кои може да им се откријат податоците, информации за временските ограничувања на зачувувањето, информации за евентуални преноси на податоци до трети земји или меѓународни организации, информации за тоа дали обезбедувањето на информации е задолжително или доброволно и можните последици за неуспехот на субјектот на податоците да обезбеди такви податоци, информации за правото на пристап, право на исправка, правото на субјектот на податоците да поднесе тужба пред Дирекцијата за

заштита на лични податоци и правото да ја повлече согласноста во кое било време.

Горенаведените информации треба да им се обезбедат на субјектите на податоците според следниве барања:

- ✓ Треба да се објасни на едноставен јазик без употреба на специјализирана терминологија или жаргон;
- ✓ Треба да бидат достапни, на пр. да му бидат директно обезбедени на субјектот на податоците, не само да бидат достапни каде било;
- ✓ Треба да бидат лесно видливи (во однос на видот и големината на фонтот на писмената информација).
- ✓ Треба да се разликуваат од сите други работи.

- Согласноста мора да биде недвосмислена

Како правило, не постои ограничување на форматот на согласноста. Минималниот неопходен услов за дејство што треба да се смета за недвосмислена согласност е достапноста на акција или индикација во име на субјектот на податоците што јасно ја покажува неговата/нејзината волја и е разбирлива од контролорот на податоците. Пример за таква недвосмислена согласност е потпис на лицето на хартиен документ, усни изјави што укажуваат на согласност или однесување со кое може да се изготви разумен заклучок за експлицитно изразување на согласност (на пример, оставање на визит-картичка во кутија за извлекување на награди во продавница). Исто така, постои недвосмислена согласност кога некое лице го испраќа неговото/нејзиното име и адреса на одредена организација, со цел да добијат одредени информации и документи.

Од гледна точка на заштита на податоците, пасивното однесување не се смета за недвосмислено укажување на согласност за обработка на податоци. Потребно е секогаш да се направат некои конкретни активности или јасни укажувања во име на субјектот на податоците.

Кога обработката се заснова врз согласност на субјектот на податоците, контролорот треба да биде способен да докаже дека субјектот на податоците дал согласност за операцијата на обработка. Иако писмена форма на согласноста не се бара од правната рамка за заштита на податоците, изречни писмени укажувања се соодветни алатки за докажување на достапноста на недвосмислена согласност на субјектите на лични податоци. Во онлајн средината, согласноста може да се изрази со електронски или дигитален потпис.

Во зависност од контекстот, други прифатливи средства за изразување на потврдување се следниве: квадратчиња за означување (ticking boxes) при посета на интернет-страницата, избор на технички прилагодувања за услугите на информатичкото општество или друга изјава или однесување кои јасно укажуваат во онлајн контекст на прифаќање од страна на субјектот на личните податоци за обработката на неговите или нејзините лични податоци.

Во спротивно, тишината, претходно означените квадратчиња или неактивноста не претставуваат согласност. Не е дозволено да се користи ниту еден метод на согласност по себе, на пр. претходно означени квадратчиња или opt-out избирања кои бараат интервенција од субјектот на лични податоци за да се спречи спогодбата (opt-out boxes - избери за да откажеш квадратчиња).

Согласноста треба да ги опфати сите активности на обработката извршени за истата цел или цели. Кога обработката има повеќе цели, треба да се даде согласност за сите нив. Ако согласноста на субјектот на лични податоци е дадена по барање преку електронски пат, барањето мора да биде јасно, концизно и не непотребно збунувачко за користењето на услугата за која е обезбедена.

Разбирливо, контролорот на податоците треба еднаш да побара согласност од субјектот на податоците. Меѓутоа, во случај на промена на целите на обработка или на појавување на нови цели, контролорот мора да добие нова согласност.

- Согласноста мора да ја даде субјектот на податоците на кого се однесуваат личните податоци

За да биде важечка правната основа за обработка на личните податоци, согласноста мора да ја даде само лицето чии лични податоци се предмет на обработка. Обезбедувањето на согласност од друго лице ја прави обработката незаконска. Овој специфичен услов за важечка согласност е многу тешко да се докаже во случаите на доставување согласност од далечина, вклучувајќи го и интернетот. Иако квадратчињата за означување се сметаат за недвосмислена согласност, контролорот на податоците не е во можност да го потврди идентитетот на лицето кое го означува квадратчето и да потврди дека тој/таа е едно исто лице со лицето чии податоци се обработуваат.

Општи услови што се применуваат за согласност за дете во однос на услугите на информатичкото општество (услуги што се бараат и доставуваат преку интернет)

Кога субјектот на податоците дал согласност за обработка на податоци за една или повеќе одредени цели, во врска со понуда на услуги на информатичкото општество директно на дете, обработката на личните податоци на детето е законска кога детето има најмалку 14 години. Кога детето е на возраст под 14 години, таквата обработка е законска само ако и до тој степен до кој согласноста ја дава или е овластена од страна на имателот на родителска одговорност над детето. Во овие случаи, контролорот ќе вложи разумни напори да потврди дека имателот на родителска одговорност им дава или одобрува согласност за детето, земајќи ја предвид достапната технологија. Сепак, контролорите треба да избегнуваат решенија за верификација кои вклучуваат прекумерно собирање на лични податоци.

По достигнувањето на возраста на зрелост, контролорот мора да добие важечка согласност од самиот субјект на лични податоци.

Изречна согласност

Законот за заштита на личните податоци го воведува концептот на „квалификувана согласност“ (т.н. изречна согласност) во ситуации во кои се јавува сериозен ризик за заштита на личните податоци и затоа е потребна повисока контрола во име на субјектот на податоците. Таквата изречна согласност е потребна во следниве случаи: обработка на посебни категории на податоци, автоматизирано индивидуално донесување одлуки, вклучувајќи профилирање и во случај на пренос на податоци до трети земји или меѓународни организации во отсуство на соодветни заштитни мерки.

Терминот „изречно“ го означува начинот на кој субјектот на податоците ја изразува својата волја. Изречната согласност бара субјектот на податоците да даде јасна изјава за согласност (на пример писмена изјава, пополнување на електронска форма, испраќање на е-пошта, испраќање на скениран документ потпишан од субјектот на податоците, користење на електронски потпис). Во пракса, исто така, може да се користи двостепена проверка на согласност (на пример, давање согласност преку е-пошта во комбинација со кликање на линк за верификација или текстуална порака со шифра за верификација за да се потврди договорот).

Сепак, усната изјава исто така може да се смета за изречна, но препорачливо е за контролорот да чува доказ за фактот дека усната согласност ја исполнува правната потреба од изречна изјава.

Повлекување на согласност

Многу важен аспект на согласноста на субјектот на податоците е фактот дека согласноста може да се повлече во кое било време по желба на субјектот на податоците. Повлекувањето на согласноста не влијае на законитоста на обработката која била врз основа на согласноста пред нејзиното повлекување - нема ретроактивно дејство. Повлекувањето на согласноста мора да биде едноставно како нејзиното давање. Во случај на повлекување и во недостаток на други правни основи за обработка на личните податоци, повлеку-

вањето претставува апсолутна правна пречка за секоја понатамошна обработка на податоците. Во таков случај, обработката на личните податоци треба веднаш да се прекине. Препорачливо е да се воспостават едноставни и ефикасни механизми за повлекување - како што се телефонски број на услуга за клиенти, онлајн формулар за повлекување на согласност, отпишување на линк во е-пошта итн.

Поединците мора да бидат во можност да ја повлечат својата согласност за обработка без никаква штета по нив. Не е дозволено да се воведе казна за повлекување на согласност.

Контролорот мора да го информира субјектот на податоците за неговото/нејзиното право за повлекување на согласноста пред да даде согласност.

Во случај на повлекување на согласноста, а не постоење на друга легитимна основа за обработка, контролорот мора да ја прекине обработката на податоците или барем да ги направи податоците анонимни или да ги избрише.

Обработката е неопходна за извршување на договор на кој субјектот на податоците е странка или за преземање чекори на барање на субјектот на податоците пред склучување на договор

Овој услов за законска обработка има две независни хипотези. Првата се однесува на случаите кога личните податоци на субјектот на лични податоци се обработуваат за целите на договорот со контролорот на лични податоци на кој е странка субјектот на личните податоци. Вообичаено, ова опфаќа ситуации како што е потребата за обработка на информации за постојаната адреса на субјектот на податоци со цел да му/ѝ се испорача стока и/или услуги; обработка на информации за кредитна картичка на субјектите на податоците со цел плаќање на испораката.

Оваа хипотеза не ги опфаќа ситуациите кога обработката на податоците не е директно поврзана со исполнувањето на обврски од договорот, туку е само потребна едностранo од контролорот на податоците. Поради тоа, препорачливо е да се оцени применливоста на оваа правна основа од случај до случај.

Втората хипотеза ги обработува случаите на обработка на податоците кои се вршат пред склучување на договорот. Овој случај ги опфаќа таканаречените преддоговорни односи, под услов тие да бидат преземени на барање на субјектот на податоците, а не од контролорот на податоците. Намерите на субјектите на податоците за склучување на договорот ја потврдуваат обработката на неговите/нејзините лични податоци од страна на релевантните контролори на податоците.

Обработката е неопходна за усогласување со законската обврска на која е предмет контролорот

Важно е да се нагласи дека обработката на податоците во овој случај произлегува од обврската на контролорот на податоците во законот во широка смисла, а не од законска договорна обврска. Вообичаено, законската обврска произлегува од државното законодавство. Законската обврска утврдена во закон од друга држава може да се примени само ако и до степен до кој е законски инкорпориран во државното законодавство - на пр. со склучување и стапување во сила на меѓународен договор. Покрај тоа, законската обврска мора да биде јасна и експлицитна - да не се дозволува никаква слобода на толкување за тоа кои лични податоци треба да ги обработува контролорот на податоците и зошто. Оваа законска основа за обработка не се применува ако релевантните законски одредби пропишуваат законска можност, а не законска обврска за контролорите на податоците.

Типичен пример за обработка на податоци што произлегува од законската обврска на контролорот на податоците е обработката на личните податоци на вработените во контекст на вработување. Работодавците имаат широк спектар на законски обврски за обработка на лични податоци, вклучувајќи и посебни категории на лични податоци. На иста законска основа, финансиските институции обработуваат податоци на клиентите и го потврдуваат идентитетот на клиентите согласно Законот за спречување на перење пари и други кривични приноси и финансирање на тероризам.

Обработката е неопходна за да се заштитат виталните интереси на субјектот на податоците или на друго физичко лице

Оваа законска основа за обработка на податоци има многу строг контекст - податоците може да се обработуваат само ако е неопходно да се заштитат виталните интереси на субјектот на податоците или на друго физичко лице. Иако не постои правна дефиниција за терминот „витални интереси", очигледно е дека оваа хипотеза се однесува на прво место за животни и здравствени ситуации. Не е важно дали заканата за виталните интереси е неизбежна или не. Пример за неопходност од обработка на лични податоци на таа законска основа може да биде случај со обработка на податоци за авионски патници во случај на опасност од епидемиолошка болест.

Обработката е неопходна за извршување на задача којашто е извршена во јавен интерес или при вршење на службена надлежност доделена на контролорот

Овој услов за законска обработка на лични податоци има два алтернативни аспекти: обработката е неопходна или за извршување на задача што се врши во јавен интерес или за вршење на службена надлежност на контролорот на податоци.

Законот за заштита на личните податоци не содржи законска дефиниција на терминот „јавен интерес". Поради тоа, можат да се појават тешкотии во одлучувањето дали одредени активности се предизвикани од јавен интерес и при проценката на применливоста на оваа законска основа за конкретна операција за обработка на податоци. Концептот на јавен интерес бара претходна проценка од случај до случај во врска со очекувањата на општата јавност, вклучувајќи ги и придобивките за општеството и контролорот на податоците, произлезени од обработка на лични податоци на конкретен субјект на податоци. Јавниот интерес треба да се заснова на законот (што значи дека тоа не е само љубопитност на јавноста), треба да биде јасно дефиниран со цел да се овозможи проценка на супериорноста и распространетоста на јавниот интерес над правата на конкретниот субјект на податоците или неговита права, а да биде вистински, а не шпекулативен.

Иако не е предвидено со закон, препорачливо е, кога планираната обработка на податоци е заснована на задача која е спроведена во јавен интерес, да се направи проценка на рамнотежата помеѓу јавниот интерес и интересите на засегнатото физичко лице. Честа ситуација во која обработката е базирана на оваа законска основа, е обработката на лични податоци на јавни личности.

Во зависност од контекстот, секоја задача во врска со следните области на односи со јавноста (листата не е целосна) може да се врши во јавен интерес: јавна безбедност, одбрана, надворешни односи, јавно здравство, финансиска стабилност, животна средина, интелектуална сопственост, заштита на националното културно и историско наследство, социјална и културна политика, образование, подигнување на транспарентноста и отчетноста на јавните тела, заштита од катастрофи, транспортна инфраструктура.

Другиот случај во оваа законска основа за обработка е кога на контролорот на податоците му се доделуваат определени овластувања и обработката на податоците е неопходна за извршување на неговите службени должности. Обработката на лични податоци е предуслов за целосно извршување на службените овластувања на органот што ја легитимизира обработката на податоците. Оваа законска основа за обработка е применлива само за јавни органи или за други службени лица кои имаат определени јавни функции, како што се нотари, судски извршители итн.

Обработката е неопходна за целите на легитимните интереси што ги следи контролорот или третите лица, освен кога таквите интереси се заменети од интересите или основните права и слободи на субјектот на податоците за коишто е потребна заштита на личните податоци, особено кога субјектот на податоците е дете

Оваа законска основа за обработка бара праведна рамнотежа помеѓу легитимните интереси на контролорот или на трето лице и интересите на субјектот на податоците на кого се однесуваат податоците. Достапноста на легитимен интерес на контролорот на податоци е само почетна точка. Дали оваа законска основа ќе ја

потврди законитоста на обработката зависи од заклучоците кои произлегуваат од споредбата помеѓу легитимниот интерес на контролорот и интересите на засегнатиот субјект на податоците.

Наоѓањето на соодветна рамнотежа значи оценување од случај до случај на следните фактори:

- Природата и изворот на легитимниот интерес на контролорот на податоците (дали обработката на податоците е неопходна за остварување на основните права на контролорот или е поврзана со правна, социјална, културна потреба на друг контролор);
- Влијанието на обработката на податоците врз субјектот на лични податоци чии лични податоци се планираат да бидат обработени (треба да се оценат позитивни и негативни последици);
- Природата на личните податоци (на пример, чувствителни податоци, податоци кои произлегуваат од јавен извор);
- Начин на обработка на податоци (на пример, откривање на неограничен опсег на примачи, зачувување на податоци со цел за профилирање итн.);
- Односите помеѓу контролорот на податоци и субјектот на податоците (на пример, дали постои хиерархиска врска; дали субјектот на податоците е дете или дали тој/таа припаѓа на ранлива група луѓе како што се бегалци, постари лица, ментално болни);
- Мерки за спречување на какво било негативно влијание врз субјектот на податоците;
- Анализа на планираните технички и организациски мерки за заштита на личните податоци од страна на контролорот, на пр. техники на анонимизација или псевдонимизација.

Треба да се има предвид дека оваа законска основа не се применува за обработка на лични податоци од страна на телата на државната администрација при вршењето на нивните задачи.

Општи забелешки за правните основи за обработка

Како што споменавме погоре, сите законски основи за обработка на податоци наведени се алтернативно во законот. Достапноста на само една од нив е доволна за да се потврди обработката на податоците. Сепак, тоа не значи дека на контролорот на податоците му е забрането да се потпре на повеќе од еден законски услов за законска обработка - законските основи може да се кумулираат во одредени ситуации.

Контролорот на податоци треба да ја примени релевантната законска основа за обработка на податоци во текот на целиот животен циклус на личните податоци - на пр. законската основа треба да биде присутна од почетокот на обработката на податоците до нејзиниот крај. Се разбира, возможно е дека законските основи може да се сменат во меѓувреме, на пример, обработката започнала врз основа на согласност на субјектот на податоците, но подоцна стапила во сила регулатива која го обврзува контролорот на податоци да ги обработува истите податоци на истиот субјект на податоци за исти цели. Обработката на податоците би била законска и во двата случаи.

4. Права на субјектите на податоците

ОСНОВНИ ПРАВА НА СУБЈЕКТИТЕ НА ПОДАТОЦИТЕ

Во областа на заштита на личните податоци, субјектите на податоците имаат само права. Тие ги уживаат следните права:

Право на информации

Правото на информации е основно право на субјектот на податоците, чија цел е да му обезбеди на субјектот на податоците детални информации за сите аспекти на обработката на податоците со цел да му се овозможи ефективно да ја контролира обработката и да ужива во неговите/нејзините други права за заштита на личните податоци. Информациите кои субјектот на податоците има право да ги знае за обработката на неговите/нејзините лични податоци ги вклучуваат следните категории:

1) идентитетот и податоците за контакт на контролорот и, доколку е применливо, на овластениот застапник на контролорот во Република Македонија;
2) детали за контакт на офицерот за заштита на личните податоци, во случаи кога е определен таков офицер за заштита на личните податоци;
3) целите на обработката за која се наменети личните податоци, како и законската основа за обработката;
4) категориите на засегнатите лични податоци - во случај личните податоци да не се добиени од страна на субјектот на податоците;
5) примателите или категориите на приматели на лични податоци, доколку ги има;
6) намерата на контролорот на податоците да пренесува лични податоци во трета земја или меѓународна организација. До-

колку трансферот се заснова на соодветни заштитни мерки, обврзувачки корпоративни правила или според чл. 53, став (1), втор потстав од Законот за заштита на личните податоци, субјектот на податоците има право на повикување на одредени или соодветни заштитни мерки и информации за начините како да се добие копија од нив или каде се ставени на располагање;

7) периодот за кој ќе се чуваат личните податоци или ако тоа не е можно, критериумите што се користат за одредување на тој период;

8) информации за легитимните интереси што ги следи контролорот или на третото лице во случај кога обработката на податоците се заснова на чл. 10, став 1, алинеја 6 од Законот за заштита на личните податоци;

9) постоење на правото да се повлече согласноста во кое било време, без да се влијае врз законитоста на обработката врз основа на согласност пред нејзиното повлекување каде што обработката е заснована на точка (1), став (1), член 10 од Законот за заштита на лични податоци или врз основа на член 13, став (2) точка (1) од законот;

10) право да поднесе барање до Дирекцијата за заштита на лични податоци;

11) информации за тоа дали добивањето на лични податоци е законско или договорно барање или барање што е неопходно за склучување на договор, како и дали субјектот на податоците е должен да ги обезбеди личните податоци и за можните последици од неуспехот да ги обезбеди тие податоци;

12) изворот на личните податоци и, доколку е применливо, дали произлегува од јавно достапни извори - доколку податоците не се добиени од субјектот на податоците;

13) постоење на автоматско донесување одлуки, вклучувајќи и профилирање, барем во тие случаи, каде има значајни информации за вклучената логика, како и значењето и пред-

видените последици од таквата обработка за субјектот на податоците;

14) постоењето на правото да се побара од контролорот пристап до и поправање или бришење на лични податоци или ограничување на обработката во врска со субјектот на податоците или да приговара на обработката, како и право на преносливост на податоци - се применуваат само во случај кога се собираат лични податоци од субјектот на податоците.

Информациите во врска со обработката на личните податоци кои се однесуваат на субјектот на податоците треба да му/ѝ се дадат во моментот на собирање од субјектот на податоците или, кога личните податоци се добиени од друг извор, во разумен рок, во зависност од околностите на случајот. Кога контролорот има намера да ги обработува личните податоци за друга цел освен за онаа за која биле собрани, контролорот треба да го обезбеди субјектот на податоците, пред таа понатамошна обработка, со информации за таа друга цел и други потребни информации. Меѓутоа, не е неопходно да се наметне обврската да се обезбедат информации кога субјектот на податоците веќе ги има тие информации, кога евидентирањето или објавувањето на личните податоци е јасно определено во законот или кога доставувањето на информации до субјектот на податоците се покажува дека е невозможно или би вклучило непропорционален напор. Второто особено може да биде случај кога обработката се спроведува за цели на архивирање во јавен интерес, научни или историски истражувачки цели или статистички цели. Во тој поглед, треба да се земат предвид бројот на субјектите на податоци, возраста на податоците и сите соодветни прифатени заштитни мерки.

Право на пристап

Субјектот на податоците има право на пристап до личните податоци што се собрани во врска со него или неа. Тој/таа може лесно да го искористи тоа право и во разумни интервали, со цел да биде свесен за тоа и да ја потврди законитоста на обработката.

Правото на пристап се состои од правото на субјектот на податоците да добие потврда од контролорот за тоа дали личните податоци кои се однесуваат на него или неа се обработуваат или не, за пристап до личните податоци и за добивање на следните информации:

1) целите на обработката;
2) категориите на лични податоци што се обработуваат;
3) примателите или категориите на приматели на кои личните податоци биле или ќе бидат откриени, особено приматели во трети земји или меѓународни организации;
4) каде што е можно, предвидениот период за кој ќе се чуваат личните податоци или, ако не е можно, критериумите што се користат за одредување на тој период;
5) постоењето на правото да се побара од контролорот да се поправат или избришат личните податоци или да се ограничи обработката на личните податоци во врска со субјектот на податоците или да приговара на таквата обработка;
6) право да поднесе барање до Дирекцијата;
7) кога личните податоци не се собираат од субјектот на податоците, сите достапни информации за нивниот извор;
8) постоење на автоматско донесување одлуки, вклучувајќи и профилирање, барем во тие случаи, каде има значајни информации за вклучената логика, како и значењето и предвидените последици од таквата обработка за субјектот на податоците.
9) во случај на пренос на податоци во трета земја или во меѓународна организација, информации за соодветните заштитни мерки кои се применуваат при преносот.

Правото на пристап исто така ги обврзува контролорите да обезбедат копија од личните податоци кои се подложени на обработка. Меѓутоа, правото да се добие копија не смее негативно да влијае на правата и слободите на други субјекти на податоци, вклучувајќи трговски тајни или интелектуална сопственост.

Кога контролорот обработува големо количество информации во врска со субјектот на податоците, контролорот треба да има можност да побара, пред да биде доставена информацијата, од субјектот на податоците да ги специфицира информациите или активностите за обработка на кои се однесува барањето.

Право на исправка

Субјектот на податоците го има правото да добие од контролорот, без непотребно одложување, исправка на неточни лични податоци кои се однесуваат на него или неа. Имајќи ги предвид целите на обработката, субјектот на податоците има право да му/ѝ ги комплетира нецелосните лични податоци, вклучително со обезбедување на дополнителна изјава.

Право на бришење („право да се заборави“)

Субјектот на податоците има право да добие од контролорот право на бришење на личните податоци кои се однесуваат на него или неа без непотребно одложување кога се применува една од следните причини:

1) личните податоци повеќе не се потребни во врска со целите за кои биле собрани или на друг начин обработени;

2) субјектот на податоците повлекува согласност врз основа на која се заснова обработката и каде што не постои друга законска основа за обработката;

3) субјектот на податоците приговара на обработката и нема преовладувачки легитимни основи за обработката;

4) личните податоци се незаконски обработени;

5) личните податоци треба да бидат избришани заради усогласување со законската обврска, утврдена со закон, на која подлежи контролорот;

6) личните податоци се собрани во врска со понуда на услуги на информатичко општество директно на дете.

Правото на бришење во онлајн средината е зацврстено и е познато како „право да се заборави". Во овој случај, правото на бришење е проширено на таков начин што контролорот кој ги направил личните податоци јавно достапни и е должен да ги избрише личните податоци по еден од горенаведените услови, е одговорен, имајќи ја предвид достапната технологија и трошоците за имплементација, да преземе разумни чекори, вклучувајќи и технички мерки, да ги информира другите контролори кои ги обработуваат личните податоци кои субјектот на податоците побарал од таквите контролори да ги избришат линковите до нив, или копирање или репликација на тие лични податоци.

Меѓутоа, правото на бришење не се применува до степен до кој обработката е неопходна по една од следните основи:

а) за остварување на правото на слобода на изразување и информации;

б) за усогласување со законската обврска утврдена со закон, на која подлежи контролорот, барајќи обработка, или за извршување на задача која е извршена во јавен интерес или при извршување на службена надлежност на контролорот;

в) поради јавен интерес во областа на јавното здравје;

г) за цели на архивирање во јавен интерес, научни или историски истражувачки цели или статистички цели, доколку остварувањето на правото на бришење веројатно ќе го оневозможи или сериозно ќе го наруши остварувањето на целите на таа обработка или

д) за утврдување, извршување или одбрана на законски барања.

Право на ограничување на обработката

Ограничувањето на обработката значи означување на зачувани лични податоци со цел да се ограничи нивната обработка во иднина. Правото на ограничување на обработката може да се врши од страна на субјектите на податоци каде што е присутен еден од следниве услови:

а) точноста на личните податоци ја оспорува субјектот на податоците на одреден период што му овозможува на контролорот да ја потврди точноста на личните податоци;

б) обработката е незаконска, а субјектот на податоците се противи на бришење на личните податоци и наместо тоа бара ограничување на нивната употреба;

в) контролорот повеќе нема потреба од личните податоци за целите на обработката, но се бара од субјектот на податоците за утврдување, извршување или одбрана на правни барања;

г) субјектот на податоците приговара во текот на проверката, дали легитимните основи на контролорот ги надминуваат оние на субјектот на податоците.

Методите кои можат да се користат за ограничување на обработката на лични податоци може да вклучуваат, меѓу другото, привремено преместување на избраните податоци во друг систем за обработка, со што избраните лични податоци стануваат недостапни за корисниците или привремено отстранување на објавените податоци од веб-страница. Во автоматизираните системи за поднесување, ограничувањето на обработката треба во принцип да се обезбеди со технички средства на таков начин што личните податоци не се предмет на понатамошни операции за обработка и не можат да се менуваат. Фактот дека обработката на личните податоци е ограничена треба јасно да се наведе во системот.

Во случај на ограничување на обработката, таквите лични податоци, со исклучок на зачувувањето, се обработуваат само со согласност на субјектот на податоците или за воспоставување, извршување или одбрана на правни барања или за заштита на правата на друго физичко или правно лице или поради причини од важен јавен интерес.

Контролорот е должен да го информира субјектот на податоците пред да се укине ограничувањето на обработката.

Контролорот е должен да ги соопшти сите исправки или бришење на лични податоци или ограничување на обработката на секој

примател на кого личните податоци биле откриени, освен ако тоа не се докаже како невозможно или вклучува непропорционален напор. Контролорот го информира субјектот на податоците за тие примателиdоколку субјектот на податоците го побара тоа.

Право на преносливост на податоци

Правото на преносливост на податоци се однесува на правото на субјектот на податоците да прима лични податоци кои се однесуваат на него или неа, што тој или таа ги доставил до контролорот, во структуриран, најчесто користен и машински читлив формат и правото да ги пренесува тие податоци на друг контролор без пречки од контролорот на кој се обезбедени личните податоци. Ова право може да се оствари ако обработката е основана на согласност од субјектот на податоците или е неопходна за извршување на договор на кој субјектот на податоците е странка и обработката се врши со автоматски средства. Пример за ситуација во која преносливоста на податоци може да се оствари е кога субјектите на податоци решаваат да ги пренесат своите мобилни услуги од еден мобилен оператор на друг.

При остварување на неговото/нејзиното право на преносливост на податоци, субјектот на податоците има право да ги пренесува личните податоци директно од еден контролор во друг, онаму каде што е технички изводливо.

Правото на преносливост на податоци не се применува за обработка неопходна за извршување на задача што се врши во јавен интерес или при вршење на службено овластување доделено на контролорот. Друго ограничување на ова право е законската забрана на правото на преносливост на податоците кои имаат негативно влијание врз правата и слободите на другите субјекти на податоците.

Право на приговор

Субјектот на податоците има право на приговор врз основа на неговата или нејзината особена ситуација, во секое време на обработката на лични податоци што се однесуваат на него или неа. Ова право е применливо ако обработката се основа на две специфични законски основи:

- обработката е неопходна за извршување на задача која е извршена во јавен интерес или во вршење на службено овластување доделено на контролорот;
- обработката е неопходна за целите на легитимните интереси што ги следи контролорот или трето лице, освен кога таквите интереси се преовладани од интересите или основните права и слободи на субјектот на податоците за кои е потребна заштита на личните податоци, особено кога субјектот на податоците е дете.

Правото на приговор, исто така се однесува на профилирање врз основа на двете горенаведени законски основи за обработка на податоци.

Во случај на остварување на правото на приговор на субјектот на податоците, контролорот нема повеќе да ги обработува личните податоци, освен ако контролорот не покаже релевантни легитимни основи за обработка која ги надминува интересите, правата и слободите на субјектот на податоците или за утврдување, извршување или одбрана на правни барања.

Кога личните податоци се обработени за цели на директен маркетинг, субјектот на податоците има право да приговара во секое време на обработката на лични податоци кои се однесуваат на него или неа за таков маркетинг, што вклучува профилирање до степен до кој е поврзан со таков директен маркетинг. Доколку субјектот на податоците се спротивстави на обработката за потребите на директен маркетинг, контролорот ќе престане да обработува лични податоци за такви цели.

Информациите за правото на приговор треба да бидат изречно доведени до вниманието на субјектот на податоците најдоцна до

моментот на првата комуникација со него/неа. Таа информација мора да биде претставена јасно и одделно од која било друга информација.

Во контекст на користењето на услугите на информатичкото општество, субјектот на лични податоци може да го искористи своето право на приговор преку автоматски средства со користење на технички спецификации.

Правото на приговор се однесува и на ситуации кога личните податоци се обработуваат за научни или историски истражувачки цели или за статистички цели, освен ако обработката е неопходна за извршување на задача која е извршена со цел на јавен интерес.

Право да не се биде предмет на автоматизирано индивидуално донесување одлуки, вклучувајќи и профилирање

Субјектот на податоците има право да не биде предмет на одлука основана исклучиво на автоматска обработка, вклучувајќи профилирање, што произведува правни последици кои се однесуваат на него или неа или слично значително влијае врз него или неа. Профилирање е каква било форма на автоматска обработка на лични податоци кои ги вреднуваат личните аспекти поврзани со физичко лице, особено за анализирање или предвидување на аспекти во врска со изведбата на работа на субјектот на податоците, економска состојба, здравје, лични преференции или интереси, сигурност или однесување, локација или движења, каде што создава правни последици во врска со него или неа или слично значително влијае врз него или неа.

Ова право не се применува ако одлуката:

а) е неопходна за склучување или извршување на договор помеѓу субјектот на податоците и контролорот на податоците;

б) е овластено со закон на кој контролорот е предмет и кој, исто така, поставува соодветни мерки за заштита на правата и слободите и легитимните интереси на субјектот на податоците (како што се следење и намери за заштита за спречување на

измама и даночни затајувања спроведени во согласност со посебните закони и да се обезбеди сигурност и доверливост на услугата обезбедена од страна на контролорот); или

в) се основа на изречна согласност на субјектот на податоците.

Во случаите наведени во точките (а) и (в) погоре, контролорот на податоци ќе спроведе соодветни мерки за заштита на правата и слободите и легитимните интереси на субјектот на податоците, барем правото да се добие човечка интервенција од страна на контролорот, правото да ја искаже неговата или нејзината гледна точка и правото да ја оспори одлуката.

Автоматизираните индивидуални одлуки за донесување одлуки не смеат да се базираат на посебни категории на лични податоци, освен ако субјектот на податоците не дал изречна согласност за обработка на тие лични податоци или обработката е неопходна заради значителен јавен интерес, како и воспоставување на соодветни мерки за заштита на правата и слободите и легитимните интереси на субјектот на податоците. Таквите заштитни мерки треба да вклучуваат специфични информации за субјектот на податоците и правото да се добие човечка интервенција, да се изрази неговата или нејзината гледна точка, за да се добие објаснување за одлуката донесена по таквата процена и да се оспори одлуката. Таквата мерка не треба да се однесува на дете.

ПОДНЕСУВАЊЕ НА БАРАЊЕ

Во случај на прекршување на нивните права во областа на заштита на личните податоци, субјектите на податоците имаат право на административен и правен лек. Правото на административен лек се остварува пред Дирекцијата за заштита на лични податоци и правото на судски надомест - пред соодветниот надлежен суд.

Барањето за правен лек не е во спротивност со остварувањето на правата за заштита на личните податоци во рамките на административната постапка.

Субјектите на податоците може да се обратат до Дирекцијата за заштита на лични податоци во кој било од следниве случаи:

- ако контролорот на податоците не постапи по барање на субјектот на лични податоци и не го извести во рок од еден месец од приемот на барањето за причините за неисполнување на постапката и за можноста за поднесување приговор до Дирекцијата за заштита на личните податоци и можноста за барање правен лек;
- доколку субјектите на податоците сакаат да достават барања за потврдување на повреда на правото на заштита на личните податоци;
- доколку субјектите на податоците сакаат да достават иницијативи за инспекциски надзор во случај на злоупотреба на лични податоци.

Доставувањето на барање и иницијативи за вршење инспекциски надзор на Дирекцијата за заштита на личните податоци е бесплатно.

Во случај на поплаки, товарот на докажување ќе го носи барателот-субјектот на податоците.

Дирекцијата го олеснува доставувањето на барањето/иницијативата со воведување на образец за поднесување на барање, кое исто така може да се пополни електронски без да се исклучат другите средства за комуникација. Образецот е достапен на веб-стра-

ницата на Дирекцијата на следниве линкови:

- https://dzlp.mk/node/3274

  (за барања за потврдување на повреда на правото на заштита на личните податоци)

- https://dzlp.mk/node/3278

  (за иницијативи за инспекциски надзор)

  Дирекцијата започнува со надзор за поднесеното барање/поднесената иницијатива.

Субјектите на податоците може да се обратат до надлежниот суд во следниве случаи:

- кога субјектот на податоците смета дека неговите или нејзините права според Законот за заштита на лични податоци се повредени како резултат на обработка на неговите/нејзините лични податоци со непочитување на тој закон;
- доколку субјектите на податоци имаат намера да бараат надомест на штета;
- доколку субјектот на податоците сака да бара ефективен правен лек против правно обврзувачка одлука на Дирекцијата за заштита на лични податоци во врска со нив (истото право го поседуваат контролорите на податоците);
- кога Дирекцијата не постапува по барањето или не го информира субјектот на податоците во рок од три месеци за напредокот или исходот на барањето поднесено во согласност со Законот за заштита на личните податоци.

Субјектот на личните податоци, исто така, има право да овласти здружение на граѓани да ја поднесе тужбата во негово или нејзино име во врска со заштитата на личните податоци, со цел да ги оствари своите права за заштита на податоците и, доколку е предвидено со закон, да го оствари правото на надомест наведено во член 99 од Законот за заштита на личните податоци.

5. Главни обврски на контролорите на податоците

Законот за заштита на личните податоци наметнува единствено обврски кон контролорите на податоците. Тековниот Прирачник за заштита на личните податоците ќе обезбеди општ преглед на главните одговорности на контролорите на податоците во однос на заштитата на личните податоци.

ИЗВЕСТУВАЊЕ

Употребата на нови технологии за некој вид обработка (на пример големи операции за обработка, профилирање, обработка на посебни категории на лични податоци) може да наметнат висок ризик за правата и слободите на физичките лица. При спроведување на проценка на ризик, контролорите на податоците мора да ја земат предвид природата, обемот, контекстот и целите на обработката на личните податоци. Онаму каде што проценката на ризикот покажува можност за појава на такви високи ризици, контролорите на податоците се должни да испратат известување до Дирекцијата за заштита на личните податоци за планираната обработка. Известувањето треба да се испрати пред самата обработка.

Законот за заштита на личните податоци ги поставува потребите на известувањето:

1. име на системот на поднесување;
2. име и презиме и податоци за контакт на контролорот, доколку е применливо од сите заеднички контролори, на овластениот претставник на контролорот, доколку има и на офицерот за заштита на лични податоци;
3. намена (и) за обработка;
4. правна основа за воспоставување на збирка на лични податоци;

5. опис на категории на субјекти на податоци и на категории на лични податоци кои се однесуваат на нив;
6. категории на приматели на кои треба да им бидат откриени личните податоци, вклучувајќи ги и примателите во трети земји или меѓународни организации;
7. времетраењето на чувањето на личните податоци, односно пропишаните рокови за бришење на различни категории на лични податоци;
8. пренос на лични податоци во трета земја или меѓународна организација и
9. општ опис кој овозможува првична проценка на соодветноста на техничките и организациските мерки што се преземаат за заштита на личните податоци при нивна обработка.

Контролорите на податоците се должни да ја известат Дирекцијата и во случај на промена на горенаведените категории на информации за известување. Известувањето мора да биде испратено во рок од 30 дена од промената.

Меѓутоа, ако некоја од следните ситуации се применува за релевантната обработка на лични податоци, контролорите на податоците не се должни да испратат известување:

- ако личните податоци се дел од јавно достапната евиденција во согласност со закон;
- ако е направена претходна оцена на влијанието на заштитата на личните податоци во согласност со член 39 од Законот за заштита на личните податоци;
- ако системот на поднесување се однесува на најмногу 50 вработени и кој се чува од страна на контролорот, како единствен систем;
- ако обработката се однесува на лични податоци на членови на здруженија на граѓани основани за извршување на политички, филозофски, верски или синдикални цели.

Дирекцијата за заштита на личните податоци утврдува и јавно објавува список на видот на операции на обработка кои бараат известување пред обработката на податоците. Информациите за известувањата се организираат во јавниот електронски регистар на системот на поднесување.

ПРЕТХОДНА КОНСУЛТАЦИЈА И ПРЕТХОДНО ОДОБРЕНИЕ

Обврските за претходна консултација и претходно одобрение се утврдени во законот поради високиот ризик дека одредени операции за обработка на податоци може да штетат на правата на субјектите на податоците. Високите ризици можат да се појават или поради природата на личните податоци што се обработуваат и фактот што податоците обезбедуваат единствена идентификација на субјектите на податоците или како резултат на спецификите на операциите за обработка на податоци и нивниот можен упад во приватноста на поединците. Барањето на совет и одобрение од надзорниот орган, според тоа, е важен предуслов за законска обработка на податоците и сериозна гаранција за правата на субјектите на податоците.

- Претходни консултации

Контролорот мора да се консултира со Дирекцијата за заштита на лични податоци пред обработката, кога проценката на влијанието врз заштитата на податоците укажува на тоа дека обработката ќе резултира со висок ризик во отсуство на мерки преземени од страна на контролорот за ублажување на ризикот. Доколку Дирекцијата смета дека планираната обработка ќе го прекрши Законот за заштита на личните податоци (особено кога контролорот недоволно го идентификувал или намалил ризикот), Дирекцијата

обезбедува (во период до 60 дена од приемот на барање за консултации) писмен совет до контролорот. Дополнително, Дирекцијата може исто така да користи кои било од своите овластувања (истражни, корективни овластувања или овластувања за издавање на одобренија или мислења). Периодот за консултација може да се продолжи за 40 дена, имајќи ја предвид сложеноста на планираната обработка за чие продолжување Дирекцијата го известува контролорот.

При консултации со Дирекцијата, контролорот треба да ги достави следните информации:

(а) онаму каде што е применливо, податоци за соодветните одговорности на контролорот, заедничките контролори и обработувачите вклучени во обработката, особено за обработка во група на претпријатија;

(б) целите и средствата на планираната обработка;

(в) мерките и заштитните мерки обезбедени за заштита на правата и слободите на субјектите на податоците;

(г) податоци за контакт на офицерот за заштита на личните податоци, онаму каде што е применливо;

(д) проценка на влијанието врз заштитата на личните податоци;

(ѓ) сите други информации што се сметаат за потребни од Дирекцијата за заштита на лични податоци.

Освен обврската за претходна консултација, кога обработката на податоците е неопходна за извршување на задача од јавен интерес, вклучувајќи обработка во однос на податоците за социјална заштита и за јавно здравје, релевантните контролори се должни да бараат претходно овластување од Дирекцијата.

- Претходно одобрение

Освен ако не е поинаку пропишано во законот, контролорите на податоците мора да побараат претходно одобрение од Дирекцијата кога планираат да обработуваат која било од следниве

категории на лични податоци:

- национален матичен број на субјектот на податоците;
- податоци поврзани со расна или етничка припадност на субјектот на податоците;
- генетски податоци, освен ако обработката не ја вршат експерти за потребите на превентивната медицина, медицинската дијагностика или грижа и третманот на субјектот на податоците и
- биометриски податоци.

Дирекцијата издава решение за претходно одобрение во рок од 60 дена од приемот на барањето на контролорот на податоците.

БЕЗБЕДНОСТ НА ИНФОРМАЦИИТЕ

Со цел да се зачува безбедноста на личните податоци и да се спречи обработката со прекршување на барањата за заштита на податоците, контролорот или обработувачот треба да ги процени ризиците својствени за обработката и да спроведе соодветни технички и организациски мерки со цел да ги ублажи тие ризици. Изборот на конкретните мерки треба да ги земе предвид следните параметри:

- состојбата на техниката;
- трошоците за спроведување на безбедносните мерки;
- природата на личните податоци кои се предмет на обработка (на пример чувствителни податоци);
- обемот, контекстот (вклучувајќи ја категоријата на субјектите на податоци - на пример, малолетни лица, бројот на засегнати субјекти на податоци) и целите на обработка;
- ризиците наметнати со обработка на лични податоци (случајно или незаконско уништување, губење, промена, неов-

ластено откривање или пристап до пренесени лични податоци, зачувани или на друг начин обработени) што може особено да доведе до физичка, материјална или нематеријална штета;

- ризик од различна веројатност и сериозност за правата и слободите на физичкото лице.

Употребата на технички и организациски мерки е поврзана со имплементацијата на еден од основните принципи за обработка на лични податоци - принципот на интегритет и доверливост.

Примери за такви технички и организациски мерки се:

(а) псевдонимизација и шифрирање на лични податоци;

(б) способноста да се обезбеди тековна доверливост, интегритет, достапност и отпорност на системите и услугите за обработка;

(в) способност за навремено враќање на достапноста и пристапот до лични податоци во случај на физички или технички инциденти;

(г) процес за редовно тестирање, проценка и оценка на ефективноста на техничките и организациските мерки за обезбедување на безбедност на обработката.

Со цел да се обезбеди физичка, кадровска, документарна заштита, заштита на автоматизирани информациски системи и/или мрежи и криптографска заштита на системите за поднесување, конкретните мерки во однос на автоматизираната обработка мора да бидат дизајнирани за:

(а) да им се одрече пристап на неовластени лица до опремата за обработка која се користи за обработка („опрема за контрола на пристап“);

(б) спречување на неовластено читање, копирање, модификација или отстранување на медиуми за податоци („контрола на податоци“);

(в) спречување на неовластен внес на лични податоци и неовластено прегледување, модификација или бришење на зачувани лични податоци („контрола на зачувување“);

(г) спречување на употреба на автоматизирани системи за обработка од страна на неовластени лица кои користат опрема за комуникација со податоци („корисничка контрола“);

(д) да обезбедат дека лицата овластени да користат систем за автоматска обработка имаат пристап само до личните податоци опфатени со нивното овластување за пристап („контрола на пристап до податоци“);

(ѓ) да обезбедат дека е можно да се проверат и да се утврдат телата на кои личните податоци биле или можат да се пренесуваат или да се стават на располагање со користење на опрема за комуникација со податоци („контрола на комуникација“);

(е) да се обезбеди дека подоцна е можно да се провери и да се утврди кои лични податоци биле внесени во автоматизирани системи за обработка и кога и од кого личните податоци биле внесени („контрола на влез“);

(ж) да спречат неовластено читање, копирање, модификација или бришење на лични податоци при пренесување на лични податоци или за време на транспорт на медиумите за податоци („контрола на превоз“);

(з) да се обезбеди дека инсталираните системи можат, во случај на прекин, да бидат обновени („обновување“);

(ѕ) да се обезбеди дека функционираат функциите на системот, дека појавата на грешки во функциите се пријавуваат („сигурност“) и дека зачуваните лични податоци не можат да бидат оштетени со дефект на системот („интегритет“).

Неуспехот да се спроведат соодветни технички и организациски мерки доведува до административна казнена одговорност на релевантниот контролор/обработувач на податоци.

6. Откривање на лични податоци[3]

Личните податоци на субјектот на податоците се доверливи и не можат да бидат откриени и пристапени без важечка правна основа. Сепак, законската обработка на податоците честопати бара податоците да им бидат достапни на две групи на лица: внатрешен персонал на контролорот на податоци кој е изречно овластен да пристапи до такви податоци за исполнување на нивните цели и задачи (на принцип на потреба за знаење) и надворешни субјекти, доколку постои законска основа и оправдана потреба за такво откривање на трети лица.

Така, дефиницијата за „обработка" го определува (општо) обемот на различните форми на обезбедување на податоци на други лица, како што се открива преку пренесување, ширење или на друг начин правење на податоците да бидат достапни.

Со цел откривањето и/или ширењето на податоците да бидат законски, контролорот на податоците што ги обезбедува податоците и примателот на податоците мора да поседуваат важечка законска основа за обработка на податоците. Проценката дали двете страни во процесот на пренос поседуваат важечка законска основа за обработка припаѓа на контролорот на податоци што ги открива податоците. Тоа е оној што ја носи прекршочната одговорност.

Од поглед на територијалниот аспект, преносот на податоци може да биде кон примателите кои живеат на територијата на Република Македонија или до примателите на територијата на друга земја. Примателот исто така може да биде меѓународна организација.

Причините за откривање или пренос на лични податоци може да се разликуваат. Во контекст на вработувањето, на пример, преносот на податоци обично се врши во рамките на мултинационални компании (помеѓу седиштето и подружниците) за глобализација на одреден обем и вид на обработка на податоци или врз основа на надворешен договор (outsourcing contract).

3. Референци за ова поглавје: Канцеларијата на комесарот за информации, https://ico.org.uk/

Се користат два основни поими за да се разликуваат лицата на кои можат да им бидат откриени податоците или на кој било друг начин да бидат достапни - примачи и трети страни. Примач е физичко или правно лице, државна администрација или друго тело, кому му се откриваат личните податоци, без разлика дали е трето лице или не. Меѓутоа, органите на државната администрација кои можат да примаат лични податоци во рамките на одредена истрага во согласност со закон, нема да се сметаат за примачи. Примачот може да биде или контролор на податоци/обработувач или трето лице.

Трето лице е секое физичко или правно лице, државна администрација или друго тело, освен субјектот на податоците, контролорот, обработувачот или лицето кое под директна надлежност на контролорот или обработувачот е овластено да обработува лични податоци. Најважниот аспект во дефинирањето на статусот на третото лице е фактот дека третото лице е секогаш различно од субјектот на податоците, контролорот на податоци, обработувачот на податоци и од лицата кои се овластени да обработуваат податоци под директна надлежност на контролорот или обработувачот.

ДАВАЊЕ НА ЛИЧНИ ПОДАТОЦИ НА КОРИСТЕЊЕ

Законот за заштита на личните податоци предвидува контролорот да им ги стави на располагање личните податоци на примачите врз основа на писмено барање од примачот, доколку примачот е овластен да ги обработува тие лични податоци, во согласност со законот. Доколку обврската за обезбедување на лични податоци е утврдена со закон и се одвива со планираната динамика, примачот не му доставува писмено барање на контролорот.

Писменото барање треба да ги содржи причините, законските основи за користење на лични податоци, категоријата на субјектите

на лични податоци и бараните категории на лични податоци. Барањето може да се поднесе електронски во согласност со законот.

Забрането е да им се стават на располагање лични податоци на примателите, обработка која не може да се спроведе во согласност со одредбите поврзани со законитоста на обработката на податоците и со барањата за обработка на посебни категории на податоци и ако целта за која личните податоци се користат не е во согласност со принципот на ограничување на целта.

Личните податоци обработени за научни или историски истражувачки цели или статистички цели не смеат да им се откриваат на примателот во форма која овозможува идентификација на субјектот на податоците.

Во случај на обезбедување на лични податоци на примателите, контролорот мора да води посебна евиденција за обезбедените лични податоци, примателот на податоците, категоријата на субјектите на податоците и законската основа и причината за која се откриени личните податоци.

Личните податоци што им се откриваат на примателите може да се користат само за времетраењето потребно за исполнување на одредената цел.

ПРЕНОСИ НА ЛИЧНИТЕ ПОДАТОЦИ

- Преноси - законски само во случај на соодветно ниво на заштита на личните податоци

Пренос на податоци е доставување на лични податоци на прима тел во друга земја или меѓународна организација.

Преносот на податоци помеѓу контролорите на податоците во Република Македонија е бесплатен и не подлежи на никакви дозволи. Преносот на податоци на примателите во земјите членки на ЕУ и земјите членки на Европската економска област може да се врши по

известување до Дирекцијата за заштита на лични податоци. Малку е веројатно дека преносот на лични податоци во трета земја или меѓународна организација е законски само ако обезбедува соодветен степен на заштита на личните податоци. Во принцип, таквите одлуки за постоење на соодветно ниво на заштита на личните податоци ги презема Европската комисија. Во отсуство на таква одлука, надлежна за проценка на достапноста на соодветно ниво на заштита во третата земја или меѓународната организација е Дирекцијата за заштита на лични податоци.

Недостатокот на соодветно ниво на заштита на личните податоци претставува апсолутна забрана за спроведување на пренос на лични податоци.

- Алтернативи за пренос во случај на отсуство на соодветно ниво на заштита на личните податоци

Освен главниот принцип дека преносот на податоци е дозволен само во случај на соодветно ниво на заштита, со цел да се обезбеди размена на лични податоци во случаи кога таквите одлуки за соодветност се отсутни, Законот за заштита на личните податоци предвидува некои други алтернативи чија имплементација обезбедува релевантна заштита за пренос на субјектот на лични податоци. Најважната особеност на овие алтернативи е фактот дека иако не постои соодветно ниво на заштита обезбедена од релевантната трета земја или меѓународна организација, самиот примател во таа трета земја или меѓународна организација обезбедува соодветна заштита на конкретниот пренос на податоци. Овие алтернативи се:

- Спроведување на соодветни заштитни мерки

Контролорот или обработувачот може да пренесува лични податоци во трета земја или меѓународна организација само ако контролорот или обработувачот обезбедил соодветни заштитни мерки и под услов да постојат достапни извршни права на субјектот на податоци и достапни се ефективни правни лекови за субјектите на податоците. Постојат два вида на соодветни заштитни мерки - еден збир на заштитни мерки кои не бараат посебно овластување од Дирекцијата и друг збир што може да се примени само по овластување на Дирекцијата.

Следниве правни инструменти обезбедуваат соодветни заштитни мерки за кои не е потребно посебно овластување од Дирекцијата:

(а) правно обврзувачки и применлив инструмент меѓу јавните органи или тела;

(б) обврзувачки корпоративни правила во согласност со член 51 од Законот за заштита на личните податоци;

(в) стандардни клаузули за заштита на податоците усвоени од Дирекцијата за заштита на лични податоци или одобрени од Европската комисија;

(г) одобрениот кодекс на однесување согласно член 44 од Законот за заштита на лични податоци, заедно со обврзувачки и извршни обврски на контролорот или обработувачот во третата земја да ги применуваат соодветните заштитни мерки, вклучувајќи ги и правата на субјектите на податоците или

(д) одобрен механизам за сертификација согласно член 46 од Законот за заштита на лични податоци, заедно со обврзувачки и извршни обврски на контролорот или обработувачот во третата земја да ги применуваат соодветните заштитни мерки, вклучувајќи ги и правата на субјектите на податоците.

Следниве правни инструменти обезбедуваат соодветни заштитни мерки, но се предмет на претходно овластување од Дирекцијата за заштита на личните податоци:

(а) договорни клаузули помеѓу контролорот или обработувачот и контролорот, обработувачот или примателот на личните податоци во третата земја или меѓународната организација или

(б) одредби за административен аранжман меѓу јавните органи или тела кои вклучуваат извршни и ефективни права на субјектот на податоци.

- Имплементација на обврзувачки корпоративни правила (ОКПа)

Задолжителни корпоративни правила се политиките за заштита на личните податоци кои ги почитува контролор или обработувач воспоставени на територијата на Република Македонија за преноси или збир на преноси на лични податоци на контролор или обработувач во една или повеќе трети земји во рамки на група на претпријатија (здружени претпријатија) или група правни лица кои се вклучени во заедничка економска активност.

За да биде важечки правен инструмент за пренос на податоци до трети земји или меѓународни организации, ОКП мора да ги исполнуваат следниве критериуми:

1. ОКПа мора да ги содржат следниве информации:

(а) структурата и податоците за контакт на групата на правни лица или група на претпријатија вклучени во заедничка економска активност и на секој од неговите членови;

(б) пренос на податоци или збир на преноси, вклучувајќи ги категориите на лични податоци, видот на обработката и нејзините цели, типот на засегнатите субјекти на податоци и идентификацијата на третата земја или земји за кои станува збор;

(в) нивната правна обврзувачка природа, внатрешна и надворешна;

(г) примена на општите принципи за заштита на податоци, особено ограничување на целите, минимизирање на податоците, ограничени периоди на чување, квалитет на податоците, заштита на податоците по дизајн и по правило, правна основа за обработка, обработка на посебни категории на лични податоци, мерки за да се обезбеди сигурност на податоците и барањата во врска со понатамошните преноси на тела кои не се обврзани со обврзувачките корпоративни правила;

(д) правата на субјектите на податоци во врска со обработката и начините за остварување на тие права, вклучувајќи го и правото да не бидат предмет на одлуки основани исклучиво на автоматска обработка, вклучувајќи профилирање во сог-

ласност со член 26 од Законот за заштита на лични податоци, правото да поднесе барање до Дирекцијата и до надлежните судови согласно закон, како и правото на судска заштита и каде што е применливо, правото на надоместок за прекршување на задолжителните корпоративни правила;

(ѓ) прифаќање од страна на контролорот или обработувачот воспоставен на територијата на Република Македонија за какви било злоупотреби на обврзувачките корпоративни правила од страна на секој засегнат член кој не е основан во Република Македонија; контролорот или обработувачот се исклучува од таа одговорност, целосно или делумно, само ако докаже дека тој член не е одговорен за настанот што ја предизвикал штетата;

(е) како се обезбедуваат информации за обврзувачките корпоративни правила, особено за одредбите наведени во точките (г), (д) и (ѓ) од овој став за субјектите на податоците, покрај членовите 17 и 18 од Законот за заштита на лични податоци;

(ж) задачите на кој било офицер за заштита на лични податоци назначен во согласност со член 41 од Законот за заштита на лични податоци или кое било друго лице или субјект задолжено за следење на усогласеноста со обврзувачките корпоративни правила во групата на правни лица или група на претпријатија ангажирани во заедничка економска активност, како и следење на обуката и постапувањето по барање;

(з) постапките за приговори;

(ѕ) механизми во рамките на групата на правни лица или група на претпријатија ангажирани во заедничка економска активност за обезбедување на проверка на усогласеноста со обврзувачките корпоративни правила. Ваквите механизми вклучуваат ревизии за заштита на личните податоци и методи за обезбедување на корективни мерки за заштита на правата на субјектот на податоците. Резултатите од таквата верификација треба да се достават до лицето или субјектот од точката (ж) на овој став и до повисокото раководство на правното лице кое контролира во групата на правни лица или на групата претпријатија ангажирани во заедничка економска

активност и треба да бидат достапни на барање на Дирекцијата;

(и) механизми за известување и евидентирање на промени во правилата и известување за тие промени во Дирекцијата;

(ј) механизам за соработка со Дирекцијата за да се обезбеди усогласеност од страна на секој член на групата на правни лица или групата на претпријатија кои се вклучени во заедничка економска активност, особено со тоа што на Дирекцијата им се достапни резултатите од верификацијата на мерките наведени во точка (s);

(к) механизмите за известување до надлежниот надзорен орган за какви било законски услови кон кои член на групата на правни лица или групата на претпријатија кои се вклучени во заедничка економска активност е предмет на трета земја, за која постои веројатност да има значителни негативни последици врз гаранциите обезбедени со обврзувачките корпоративни правила и

(л) соодветна обука за заштита на податоците на вработените кои имаат постојан или редовен пристап до лични податоци.

2. ОКПа мора:

(а) да бидат правно обврзувачки и да се применуваат и да ги спроведуваат сите засегнати членови на групата на правни лица или групата на претпријатија вклучени во заедничка економска активност, вклучувајќи ги и нивните вработени;

(б) јасно ги доделува извршните права на субјектите на лични податоци во врска со обработката на нивните лични податоци.

Дирекцијата за заштита на лични податоци е надлежна за одобрување на обврзувачки корпоративни правила и по такво одобрување може да се применат како важечки инструмент за пренос на податоци.

- Преноси или откривања кои не се дозволени со закон во Република Македонија

Секоја пресуда на суд и секоја одлука на административен орган на трета земја која бара од контролорот или обработувачот пренос или откривање на лични податоци, може да се признае или да се спроведе на кој било начин само ако е врз основа на меѓународен договор, како што е договор за заемна правна помош, во сила меѓу третата земја каде што е основан контролорот или обработувачот го поднел барањето и Република Македонија, без да е во спротивност со другите основи за пренос утврдени со Законот за заштита на лични податоци.

- Други правни основи за пренос на податоци

Во отсуство на одлука за адекватноста или на соодветни заштитни мерки, вклучувајќи ги и обврзувачките корпоративни правила, пренос или збир на преноси на лични податоци во трета земја или меѓународна организација треба да се одвива само врз еден од следните услови:

(а) субјектот на податоците експлицитно се согласил со предложениот пренос, откако бил информиран за можните ризици од таквите преноси за субјектот на податоците поради отсуство на одлука за адекватност и соодветни заштитни мерки;

(б) преносот е неопходен за извршување на договор помеѓу субјектот на податоците и контролорот или спроведувањето на преддоговорни мерки преземени на барање на субјектот на лични податоци;

(в) преносот е неопходен за склучување или извршување на договор склучен во интерес на субјектот на податоците помеѓу контролорот и друго физичко или правно лице;

(г) преносот е неопходен заради важни причини од јавен интерес;

(д) преносот е неопходен за утврдување, извршување или одбрана на правни барања;

(ѓ) преносот е неопходен за да се заштитат виталните интереси

на субјектот на податоците или на други лица, кога субјектот на лични податоци е физички или правно неспособен за давање согласност;

(е) преносот се врши од регистар кој според законот е наменет да дава информации за јавноста и кој е отворен за консултации или од јавноста воопшто или од кое било лице кое може да покаже легитимен интерес, но само до степенот дека условите утврдени со закон за консултации се исполнети во конкретниот случај.

Во случај на отсуство на соодветно ниво на заштита или соодветни заштитни мерки, вклучувајќи ги и одредбите за обврзувачки корпоративни правила и ниту едно од отстапувањата за одредена ситуација утврдена во чл. 53 од Законот за заштита на лични податоци се применува, преносот во трета земја или меѓународна организација може да се изврши само ако се присутни сите следни барања:

- преносот не е повторлив;
- преносот се однесува само на ограничен број на субјекти на податоци;
- преносот е неопходен поради целите на принудувачки легитимни интереси што ги следи контролорот и кои не се преовладани од интересите или правата и слободите на субјектот на податоците;
- контролорот ги оцени сите околности околу преносот на податоци;
- контролорот, врз основа на проценката, обезбеди соодветни заштитни мерки во однос на заштитата на личните податоци.

Таквите преноси се предмет на режим на известување - релевантните контролори на податоци мора да ја информираат Дирекцијата за заштита на личните податоци за преносот. Контролорот, исто така, мора да го информира субјектот на податоците за преносот и за следените релевантни легитимни интереси.

- Општи барања и забелешки

Во отсуство на одлука за адекватност, законот на Република Македонија може, од важни причини од јавен интерес, јасно да ги ограничи преносите на одредени категории на лични податоци на трета земја или меѓународна организација.

Контролорот или обработувачот мора да ја документира проценката, како и соодветните заштитни мерки во евиденцијата на операциите за обработка наведени во член 34 од Законот за заштита на личните податоци.

Дирекцијата за заштита на личните податоци донесува одлуки за соодветното ниво на заштита, одобрува обврзувачки корпоративни правила и овластува соодветни заштитни мерки во рок од 60 дена од приемот на релевантното барање.

РАЗМЕНА НА ПОДАТОЦИ

Споделувањето на податоци е откривање на податоци од една или повеќе организации на друга организација или од организации на трети лица, или размена на податоци помеѓу различни делови на една организација. Размената на податоци може да биде во форма на:

- реципрочна размена на податоци;
- една или повеќе организации кои обезбедуваат податоци на трето лице или лица;
- неколку организации здружуваат информации и ги прават меѓусебно достапни;
- неколку организации здружуваат информации и ги стават на располагање на трето лице или лица;
- исклучително, еднократно откривање на податоци во неочекувани или вонредни ситуации или

- различни делови од иста организација што ги прави податоците достапни едни на други.

Некои споделувања на податоци не вклучуваат лични податоци, на пример, кога се споделуваат само статистички податоци кои не можат да идентификуваат никого. Во овие случаи, барањата за заштита на личните податоци нема да се применуваат.

ДОСТАВУВАЊЕ НА ПОДАТОЦИ

Секој орган на државната администрација, јавна установа или друго правно лице кое ги води службените јавни регистри, јавно достапните збирки на податоци или други збирки на податоци е должно бесплатно и по барање на Дирекцијата за заштита на лични податоци да доставува податоци од регистрите и збирките на податоци за потребите на постапките кои се чуваат во согласност со Законот за заштита на личните податоци.

Комуникацијата помеѓу Дирекцијата и органите на државната администрација, јавните установи или другите правни субјекти во врска со доставувањето на податоци мора да се чува во писмена или електронска форма, во согласност со законот.

7. Социјален инженеринг[4]

Социјалниот инженеринг е аспект на безбедноста на информациите што открива претежно импликации на човечкиот фактор од чисто технолошки проблеми. Тоа го олеснува добивањето на информации (вклучувајќи информации за компјутерски системи) преку нетехнички средства. Ова е психолошки феномен во кој поединец или група на луѓе се под влијание/манипулирани да преземат конкретни дејства, кои вообичаено се против нивните најдобри интереси. Неговото значење за заштитата на податоците може да се види во фактот дека напад на социјален инженеринг може да резултира со случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до лични податоци. Фаза на подготовка на напад на социјалниот инженеринг исто така може да имплицира техники за заштита на податоци, како што е следење на однесувањето на лицата.

ТЕХНИКИ НА СОЦИЈАЛЕН ИНЖЕНЕРИНГ

„Социјален инженер“ е субјектот кој го планира и врши нападот на социјалниот инженеринг. Може да биде или поединец или група на поединци. Нападот се изведува против конкретна цел (жртва), која исто така може да биде или поединец или поголема група - организација. Социјалниот инженер користи одредени методи за спроведување на нападот. Обично тие се упатуваат кон градењето врски, доверба и/или пријателство со целта. Социјалниот инженер може да користи кој било медиум за да ја нападне жртвата - или директна комуникација, како што се лице в лице или индиректни

4. Референци за ова поглавје: Mouton, F. et al., Social Engineering Attack Framework, Information Security for South Africa, 2014, DOI: 10.1109/ISSA.2014.6950510; Ira S. Winkler, 82-10-43 Social engineering and reverse social engineering; Yavor Papazov, Social engineering, STO-MP-AVT-211; ENISA, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering; https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing; The state of security, https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/; TechTarget, http://searchsecurity.techtarget.com/definition/phishing; Phishing.org, www.phishing.org; Secure and private email service, https://blog.mailfence.com/what-is-baiting-in-social-engineering/

средства, како што се е-пошта, телефон, текстуална порака, медиум за складирање или веб-страница.

Информациите за техниките на социјалниот инженеринг и нивните основни карактеристики се дадени подолу:

- Фишинг: Фишинг (Phishing) е компјутерски криминал во кој целта или целите се контактираат преку електронска пошта, телефон или текстуална порака од некој што претставува легитимна институција за да ги привлече поединците да им обезбедат чувствителни податоци како што се информации за лична идентификација, банкарство и детали за кредитни картички и лозинки. Информациите потоа се користат за пристап до важни сметки и може да резултираат со кражба на идентитет и/или финансиска загуба. Под фишинг шемите, е-поштата и пораките се прават да изгледаат исто како оние што се испраќаат од легитимни компании. Софистицираните фишинг-напади ги користат електронските адреси на луѓе кои се регистрирани да користат одредени услуги (на пример, банка, социјална мрежа). Кога тие луѓе добиваат електронски пораки кои би требало да бидат од тие компании, има поголема веројатност да им веруваат. Измамничките електронски пораки често содржат линкови што доведуваат до измамнички/малициозни веб-страници, каде што се користат различни методи за барање и собирање финансиски и лични податоци на лицето. Напаѓачите често ги користат тактиките на заплашување или барање на брз одговор од примателите, дополнително, овие лажни пораки најчесто не се персонализирани и може да имаат слични општи својства.
- Изговор: изговор (pretexting) е употреба на изговор - лажно оправдување за одреден тек на постапување - да се стекне доверба и да се измами жртвата. Пронаоѓањето на солиден изговор го легитимира барањето за информации од целта. Добар пример за ова би бил напаѓач кој имитира надворешна ИТ-поддршка и манипулира со персоналот за физичко обезбедување на компанијата за да добие дозвола за влез во зградата и/или ја бара лозинката на жртвата за потреби на одржување.

- Намамување: намамување (baiting) е наведување на жртвата во извршување на одредена задача, преку овозможување на лесен пристап до нешто што жртвата го посакува. Честа ситуација е оставање на флеш-уреди или слични уреди заразени со малициозен софтвер на лесно достапни места и видливи за жртвата, надевајќи се дека овој хардвер ќе биде вметнат во мрежни компјутери како средство за ширење на малициозен код. Во пракса, заразените флеш-дискови се исто така презентирани на жртвата како промотивни подароци или како награда за учество во анкетата. Друг пример за намамување е случајот каде што намамувачите им нудат на корисниците бесплатни музички или филмски преземања, доколку истите ги откријат своите ингеренции за најава на одредена интернет-страница.
- Квид про кво: квид про кво значи нешто за нешто. Оваа техника ветува корист во замена за информации. Оваа придобивка обично зема форма на услуга. Еден од најчестите типови на квид про кво напади вклучува напаѓачи кои имитираат ИТ-сервисери кои притоа спам-повикуваат толку многу директни броеви кои припаѓаат на една компанија колку што можат да ги најдат. Овие напаѓачи нудат ИТ-помош за секоја од нивните жртви. Тие им ветуваат брзо отстранување на проблемот на вработените доколку ја оневозможат АВ (анти-вирус) програмата на својот компјутер со цел да му инсталираат малициозен софтвер под маска на софтверско ажурирање. Друг практичен пример може да биде случајот кога напаѓачот ја бара лозинката на жртвата, во замена за пари, претставувајќи се како истражувач кој врши експеримент.
- На задна врата: Друг тип на напади од социјален инженеринг е познат како на задна врата или „на туѓ грб“ (tailgating). Овие типови на напади најчесто вклучуваат некој кој нема соодветна автентикација, а следи некој од вработените во ограничено подрачје. Во вообичаен тип на напад на задна врата, едно лице се претставува како возач за испорака и чека

надвор од зградата. Кога некој од вработените добива безбедносно одобрение за влез и ја отвора вратата, напаѓачот бара од вработениот да ја придржи вратата и со тоа добива пристап внатре преку некој кој е овластен да влезе во компанијата.

- Други техники за социјален инженеринг може да вклучуваат собирање на информации од јавно достапни извори (на пример, социјални мрежи) или сурфање преку рамо (гледајќи преку рамото на жртвата, демнат додека некој внесува лозинка), претресување го ѓубрето во потрага по информации итн.
- Обратен социјален инженеринг: оваа форма на социјален инженеринг има три чекори: саботажа, рекламирање и помагање. Социјалниот инженер наоѓа начин да саботира мрежа или да создаде впечаток дека има саботажа на мрежата предизвикувајќи проблем (на пример, да започне мрежен напад против целна веб-локација, преку испраќање на е-пошта од измамничка е-адреса која им кажува на корисниците дека се инфицирани со вирус). Следно, социјалниот инженер ги рекламира неговите или нејзините услуги како консултант за безбедност (преку автоматизирани пораки, оставање бизнис-картички или испраќање електронски пораки кои ги рекламираат неговите или нејзините услуги). Сметајќи го напаѓачот за лице кое може да помогне бидејќи навидум го решава проблемот, персоналот на нападнатата организација му/ѝ дава информации или му/ѝ го олеснува преземањето на други злонамерни акции, како што се подметнување на кејлогери (keyloggers) или крадење на доверливи податоци.

ПРЕПОРАКИ ЗА СПРЕЧУВАЊЕ НА СОЦИЈАЛНИОТ ИНЖЕНЕРИНГ

Социјалниот инженеринг може да предизвика одредено материјално или нематеријално оштетување на жртвата. При напад врз базата на податоци на контролорот на податоците, овој феномен може да се смета како ризик или висок ризик за правата и слободите на физичките лица. Така, препорачливо е контролорите на податоците да ја разгледаат евентуалната појава на социјален инженеринг при утврдување на конкретниот список на технички и организациски мерки за заштита на личните податоци. Следните мерки се несуштински список на одредени технички и организациски мерки кои може да се спроведат во текот на обработката на личните податоци со цел да се одговори на човечкиот фактор на социјалниот инженеринг:

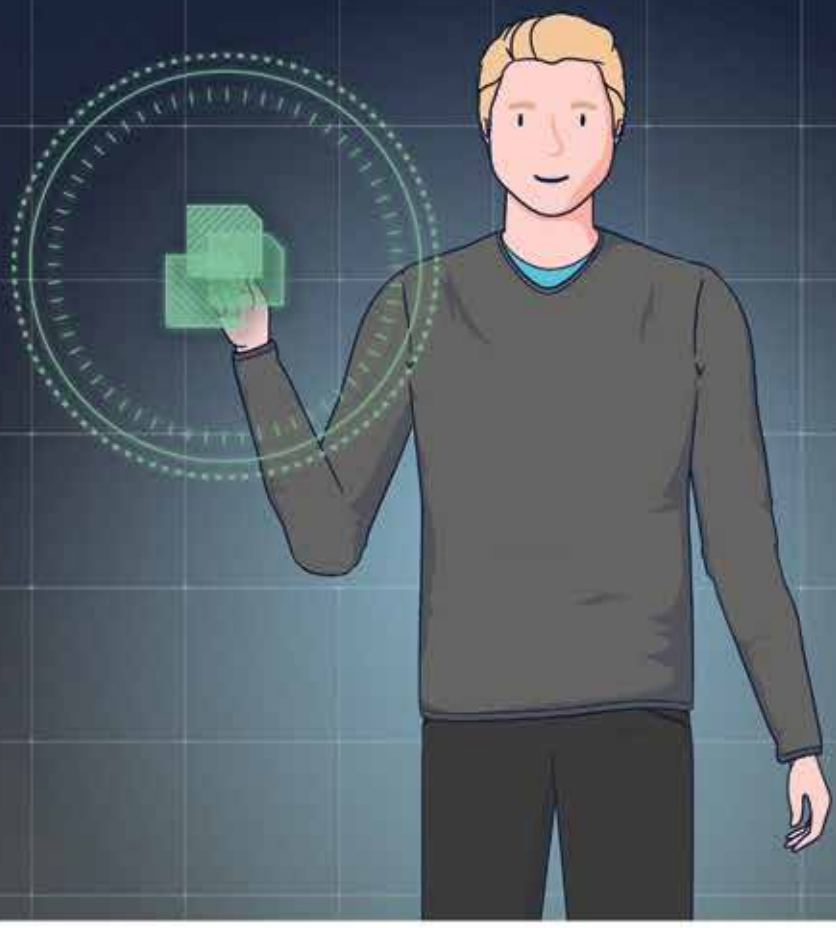
- Воспоставување и придржување кон политиката за приватност (вклучувајќи користење на решенија за автентикација на е-пошта, користење на технички безбедносни карактеристики, воведување на систем за безбедносно алармирање);
- Обука за персонал/кадри - образованието и обуката треба да се фокусираат на препознавање и справување со напади на социјален инженеринг;
- Спроведување на фишинг симулации на редовна основа;
- Периодично извршување на надворешни ревизии и тестови за пенетрација за да се утврди подложноста на организацијата кон нападите на социјалниот инженеринг, известување и постапување по резултатите.

Спроведувањето на соодветни технички и организациски мерки има за цел да ги отстрани слабостите кои го олеснуваат појавувањето на социјалниот инженеринг: недостаток на свест за безбедноста и/или безбедносни планови и процедури.

8. Заклучок

Правото на заштита на личните податоци е основно право на поединците засновано како такво во чл. 89 од Повелбата за фундаментални права на Европската Унија. Оттаму, националниот режим за заштита на личните податоци базиран на acquis на ЕУ е многу строг со многу ограничен простор за маневрирање. Познавањето на императивните барања за заштита на податоците и нивната правилна имплементација е важен предуслов за демонстрирање на усогласеноста на контролорите на податоците/обработувачите и гаранција за правата и слободите на поединците. Овој Водич за заштита на личните податоци ги поставува основните поими во областа на заштитата на податоците и ја одредува улогата што ја имаат различните засегнати страни во обработката и заштитата на личните податоци. Тој е дизајниран како информативна алатка за контролорите на податоците, обработувачите на податоци и нивните вработени за да им помогнат да ги обработуваат личните податоци законски и оправдано.

ВОДИЧ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ



ДИРЕКЦИЈА ЗА ЗАШТИТА
НА ЛИЧНИТЕ ПОДАТОЦИ