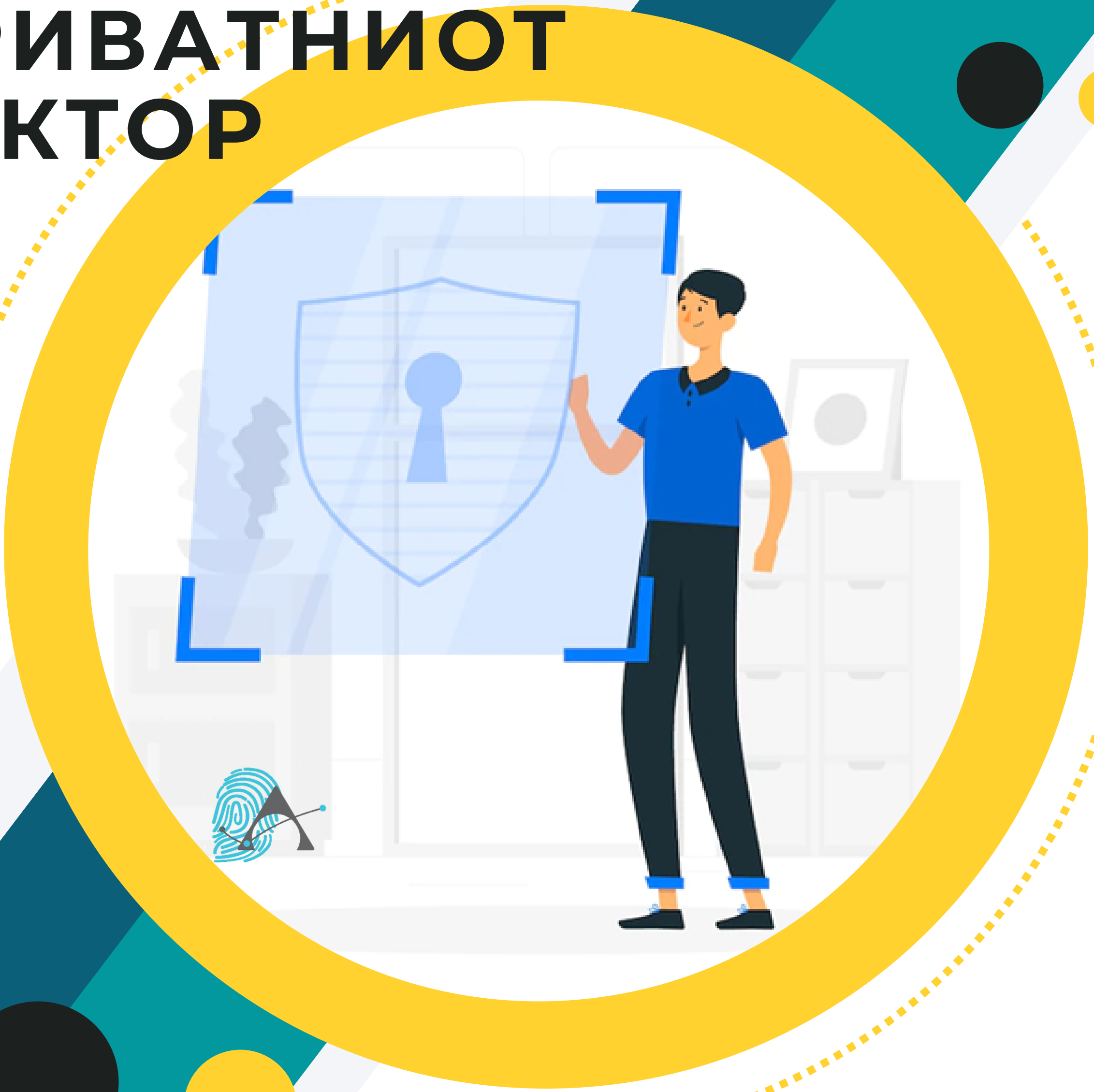
ЕУ твининг-проект „Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“

ВОДИЧ ЗА ОФИЦЕРИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЈАВНИОТ И ПРИВАТНИОТ СЕКТОР



Октомври 2022

Овој проект е финансиран од Европската Унија

СПИСОК НА КРАТЕНКИ И АКРОНИМИ

- **ОЗЛП** Офицер за заштита на личните податоци
- **ЗЗЛП** Закон за заштита на личните податоци
- **АЗЛП** Агенција за заштита на личните податоци
- **РГ29** Работна група за член 29 од Директивата 95/46
- **ЕУ** Европска Унија
- **ЕК** Европска комисија
- **ЕЕЗ** Европска економска заедница
- **ГДПР** Општа регулатива за заштита на личните податоци

Овој проект е финансиран од Европската Унија

СОДРЖИНА

КОНЦЕПТОТ НА ПРИВАТНОСТ И ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЕРАТА НА ДИГИТАЛИЗАЦИЈА 5
Значење и дефиниции на термините што се користат во Водичот 6
Која е целта на овој водич и за кого е наменет? 7
ДЕЛ 1: ОБВРСКА НА КОНТРОЛОРИТЕ ЗА ОПРЕДЕЛУВАЊЕ ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ 9
1. Која е улогата и кои се задачите на офицерот за заштита на личните податоци? 10
1.1. Кои лица треба да бидат определени за офицери за заштита на личните податоци? Какви вештини и квалификации треба да поседуваат? 10
1.2. Како е регулирано определувањето на офицер за заштита на личните податоци во ЗЗЛП? 11
1.2.1. Задолжително определување на офицер за заштита на личните податоци 11
1.2.2. Доброволно определување офицер за заштита на личните податоци. 13
1.2.3. Дали може надворешно лице да се определи како офицер за заштита на личните податоци? 14
1.2.4. Еден офицер за заштита на личните податоци за еден или повеќе контролори/обработувачи 14
1.3. Кои професионални стандарди треба да ги исполнува офицерот за заштита на личните податоци? 16
1.4. Позиција и статус на офицерот за заштита на личните податоци 17
1.4.1. Стручност и вештини 17
1.4.2. Вклучување на офицерот за заштита на личните податоци во сите прашања поврзани со заштитата на личните податоци 18
1.4.3. Гаранции за независноста на офицерот за заштита на личните податоци 18
1.4.4. Судир на интереси 19
1.5. Определување и разрешување на офицер за заштита на личните податоци 20
1.6. Препораки за контролори со различна големина на организација 23

Овој проект е финансиран од Европската Унија

ДЕЛ 2: ЗАДАЧИ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ 24

2. ИНФОРМИРАЊЕ ЗА И ПОСТАПУВАЊЕ ПО БАРАЊА ЗА ЗАШТИТА НА ПРАВАТА НА СУБЈЕКТИТЕ НА ЛИЧНИ ПОДАТОЦИ **24**

2.1. Права на субјектите на лични податоци 24

2.2. Обврски на контролорот/обработувачот 25

2.2.1. Почитување на начелата за заштита на личните податоци 25

2.2.2. Законски основ за обработка на личните податоци 26

2.2.3. Известување за ОБРАБОТКА (НА личниТЕ податоци) СО ВИСОК РИЗИК 28

2.2.4. Нова обврска: известување за нарушување на безбедноста на личните податоци 28

2.2.5. Евиденција на активностите за обработка 30

2.3. Следење на усогласеноста со ЗЗЛП 30

2.4. Подигнување на свеста за заштитата на личните податоци 31

2.5. Обука на вработените 31

2.6. Давање совети и препораки на контролорот/обработувачот 32

2.7. ревизии/контроли/проверки 32

2.8. Проценка на влијанието врз заштитата на личните податоци 32

2.9. Соработка со АЗЛП и дејствување како контакт точка 35

2.10. Технички и организациски мерки за безбедност на личните податоци 36

2.11. Приод што се базира на ризик38

ДЕЛ 3: АЛАТКИ ЗА ЗАЈАКНУВАЊЕ НА ПОЗИЦИЈАТА НА ОФИЦЕРИТЕ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ 41

3.1. Пакет водичи 41

3.2. Катче за офицери 41

3.3. Мрежа на офицери 42

3.4. Е-форум 42

3.5. Здружение на офицери 43

3.6. Нова програма за обуката на офицери 43

3.7. Стратегија за комуникација 43

3.8. Денови на свест за улогата на офицерите 43

Овој проект е финансиран од Европската Унија

КОНЦЕПТОТ НА ПРИВАТНОСТ И ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЕРАТА НА ДИГИТАЛИЗАЦИЈА

Културата на почитување на приватноста и заштитата на личните податоци се смета за голема вредност на демократските општества кои се развиваат преку примена на основните стандарди воспоставени од Обединетите нации, [1]Советот на Европа[2] и Европската комисија[3], кои пак се елаборирани во меѓународните договори и националното законодавство за заштитата на личните податоци.

Почитувањето на правото на приватност на физичките лица е карактеристично за поразвиените земји со долга традиција на владеење на правото и демократски практики, но големо значење се припишува и на почитувањето на ова право во општествени средини кои се стремат кон постигнување повисоко ниво на политичко, правно, економско и културно живеење.

Со донесувањето на Законот за заштита на личните податоци (ЗЗЛП)[4] кој претставува lex generalis во оваа област, Северна Македонија го вгради правото на заштита на личните податоци во правниот систем на земјата и воведе нов концепт кој ја нагласува важноста на ова право како дел од основните права и слободи на граѓаните и како суштинска вредност на секое модерно и технолошки развиено општество. Овој концепт подразбира приватност и личен интегритет на сите лица, во сите ситуации кои подразбираат обработка на лични податоци.

Од суштинско значење за остварување на овој концепт и за воспоставување повисоки стандарди за почитување на приватноста е контролорите од јавниот и од приватниот сектор да определат офицер за заштита на личните податоци, заедно со јасно дефиниција на работната позиција и потребните квалификации за вршителите на оваа функција, и да ја интензивираат соработката со Агенцијата за заштита на личните податоци (АЗЛП).

[1] Обединети нации, Европска конвенција за човековите права од 1950 година
[2] Совет на Европа, Конвенција за заштита на физичките лица во однос на автоматска обработка на личните податоци бр. 108/81.
[3] Европска комисија, Директива 95/46/ЕС на Европскиот парламент и на Советот за заштита на физичките лица во однос на обработката на лични подароци и слободното движење на таквите податоци, донесена на 24 октомври 1995 година, која од 25 мај 2018 година се заменува со Регулативата (EU) 2016/679 на Европскиот парламент и на Советот за заштита на физичките лица во однос на обработката на лични податоци и слободното движење на таквите податоци со која се укинува Директивата 95/46/ЕС, донесена на 27 април 2016 година (Општа регулатива за заштита на личните податоци – ГДПР).
[4] Закон за заштита на личните податоци, „Службен весник на Република Северна Македонија“ бр. 42/20 и 294/21).

Овој проект е финансиран од Европската Унија

ЗНАЧЕЊЕ И ДЕФИНИЦИИ НА ТЕРМИНИТЕ ШТО СЕ КОРИСТАТ ВО ВОДИЧОТ

Значење и дефиниции на термините што се користат во Водичот

За целите на утврдување на значењето на термините што се користат во овој Водич подолу се дадени соодветните дефиниции, онака како што постојат во Законот за заштита на личните податоци. Дефинирањето на овие термини ги појаснува основите врз кои се темели правото на заштита на личните податоци, го помага разбирањето на суштината на законот и го олеснува спроведувањето.

ЛИЧЕН ПОДАТОК е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, при што физичко лице кое може да се идентификува е лица чијшто идентитет може да се утврди директно или индиректно, посебно врз основа на идентификатори како што се име/презиме, матичен број, податоци за локацијата, итн., или повеќе обележја специфични за физичкиот, физиолошкиот, генетскиот, менталниот, културниот или социјалниот идентитет на тоа лице.

ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ значи секоја операција или збор на операции кои се извршуваат врз личните податоци или врз група на лични податоци, автоматски или на друг начин, како што се: собирање, евидентирање, организирање, структурирање, чување, приспособување или промена, повлекување, консултирање, увид, користење, откривање преку пренос, објавување или достапност на личните податоци на друг начин, усогласување, комбинирање, ограничување, бришење или уништување.

СУБЈЕКТ НА ЛИЧНИ ПОДАТОЦИ е кое било физичко лице на кое се однесуваат личните податоци што се обработуваат.

КОНТРОЛОР е физичко или право лице, орган на државната управа, државен орган или правно лице основано од државата за вршење јавни овластувања, агенција или друго тело кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци.

ОБРАБОТУВАЧ НА ЗБИРКА НА ЛИЧНИ ПОДАТОЦИ значи физичко или правно лице, орган на државата управа, државен орган или правно лице основано од државата за вршење јавни овластувања, агенција или друго тело кое ги обработува личните податоци во име на контролорот.

Овој проект е финансиран од Европската Унија

ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ е лице овластено од контролорот за обезбедување усогласеност со регулативите за заштита на личните податоци и за следење на нивната примена.

СОГЛАСНОСТ НА СУБЈЕКТОТ НА ЛИЧНИ ПОДАТОЦИ е слободно дадена, конкретна, информирана и недвосмислено изјавена волја на субјектот преку изјава или јасно потврдено дејствие преку кои се изразува согласност за обработка на неговите/нејзините лични податоци за претходно утврдени цели.

ПОСЕБНИ КАТЕГОРИИ НА ЛИЧНИ ПОДАТОЦИ (осетливи податоци) се лични податоци кои откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања, или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци за здравјето, или податоци за сексуалниот живот или сексуалната ориентација на лицето.

Која е целта на овој водич и за кого е наменет?

Овој водич е наменет за контролорите и офицерите за заштита на личните податоци кои се определени од контролорите, во јавниот и во приватниот сектор.

Водичот има за цел да го објасни значењето на заштитата на личните податоци и начинот на кој новото законодавство ги опфаќа најновите технологии и технолошки решенија наспроти предизвиците со кои се соочуваат офицерите за заштита на личните податоци.

Конкретните цели на Водичот се да ја претстави улогата на офицерите за заштита на личните податоци, односно:

- да ги информира за нивните задачи кои произлегуваат од националното законодавство, односно од Законот за заштита на личните податоци;
- да ги појасни законските обврски кои се однесуваат на определување офицер за заштита на личните податоци, како и одредбите кои ги дефинираат потребните квалификации за извршување на оваа позиција;
- да ги објасни работните задачи на офицерите за заштита на личните податоци, вклучително и одговорностите на контролорите и обработувачите кои се должни да определат вакви офицери во рамките на нивната организација.

Овој проект е финансиран од Европската Унија

Водичот претставува корисна образовна и практична алатка за контролорите и за офицерите за заштита на личните податоци преку:

- појаснување на релевантните одредби од ГДПР кои се транспонирани во националното законодавство на Северна Македонија;
- детално запознавање на офицерите со нивната улога и работните задачи, како и на законски обврски на контролорите;
- давање насоки на контролорите/обработувачите како да ги исполнат обврските кои произлегуваат од ЗЗЛП/ГДПР, вклучително и преку определување офицер за заштита на личните податоци; и
- препораки за најдобри практики од релевантните искуства во државите-членки на Европската Унија (ЕУ), но и од домашната практика.

Овој документ е организиран во три дела, при што ДЕЛ 1 дава преглед на законските одредби кои се однесуваат на определување офицер за заштита на личните податоци како и потребните квалификации за извршителите на таа работна позиција, ДЕЛ 2 детално ги објаснува работните задачи на офицерите, обврските на контролорите и обработувачите кои произлегуваат од новото законодавство, како и преглед на правата на субјектите на лични податоци, и ДЕЛ 3 вклучува пакет алатки кои се корисни за зајакнување на позицијата на офицерите за заштита на личните податоци.

Овој проект е финансиран од Европската Унија

ДЕЛ 1: ОБВРСКА НА КОНТРОЛОРИТЕ ЗА ОПРЕДЕЛУВАЊЕ ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Офицерите за заштита на личните податоци ги балансираат интересите на контролорите и обработувачите со интересите на субјектите чиишто лични податоци се обработуваат, обезбедуваат исполнување на обврските кои произлегуваат од законот, и се првата точка за контакт со Агенцијата за заштита на личните податоци (АЗЛП).

Оттука, улогата на овие офицери е специфична и уникатна, а нивната позиција во рамките на контролорот треба да биде уредена на начин кој гарантира независност и спречува можни политички или други влијанија врз извршувањето на нивните должности.

Овој дел од Водичот се обидува да даде одговори на следниве прашања:

- Која е улогата и кои се задачите на офицерот за заштита на личните податоци?
- Кои лица треба да бидат определени за офицери за заштита на личните податоци?
- Какви вештини и квалификации треба да поседуваат?
- Како е регулирано определувањето на офицер за заштита на личните податоци во ЗЗЛП?
- Задолжително определување на офицер за заштита на личните податоци
- Доброволно определување офицер за заштита на личните податоци
- Доброволно определување офицер за заштита на личните податоци
- Дали може надворешно лице да се определи како офицер за заштита на личните податоци?
- Еден офицер за заштита на личните податоци за еден или повеќе контролори/обработувачи
- Кои професионални стандарди треба да ги исполнува офицерот за заштита на личните податоци?
- Позиција и статус на офицерот за заштита на личните податоци.
- Стручност и вештини на офицерот за заштита на личните податоци.

Овој проект е финансиран од Европската Унија

- Вклучување на офицерот за заштита на личните податоци во сите прашања поврзани со заштитата на личните податоци.
- Гаранции за независноста на офицерот за заштита на личните податоци[5].
- Судир на интереси.
- Определување и разрешување на офицер за заштита на личните податоци.

Препораки за контролори со различна големина на организација.

1. Која е улогата и кои се задачите на офицерот за заштита на личните податоци?

Задачите на офицерот за заштита на личните податоци се пропишани во член 43 од Законот за заштита на личните податоци и вклучуваат:

- информирање и советување на контролорот или обработувачот и на вработените кои вршат обработка на лични податоци за нивните обврски што произлегуваат од законот;
- следење на усогласеноста со законот, со други релевантни закони кои се однесуваат на заштитата на личните податоци во Република Северна Македонија, како и со политиките за заштита на личните податоци на контролорот или обработувачот, вклучително и во однос на доделување работни одговорности, градење на свеста и обучување на вработените кои вршат обработка на лични податоци, како и во однос на спроведување соодветни ревизии/контроли на заштитата на личните податоците;
- давање совети, кога е потребно, за проценката на влијанието врз заштитата на личните податоци и следење на извршувањето на таквата проценка во согласност со член 39 од ЗЗЛП;
- соработка со Агенцијата;
- контакт точка за Агенцијата во врска со прашања кои се однесуваат на обработката на личните податоци, вклучително и како дел од претходна консултација регулирана во член 40 од ЗЗЛП, и консултации/советувања за сите други прашања, кога е потребно.

[5] Водичот често го користи терминот „позицијата на офицер за заштита на личните податоци“, кој значи пакет задачи на офицерите, онака како што се регулирани во ЗЗЛП/ГДПРи треба да бидат вградени во документот/актот за определување/именување офицер и во описот на работното место.

Овој проект е финансиран од Европската Унија

Офицерите треба да стапат во редовна комуникација и соработка со АЗЛП која вклучува поддршка од Агенцијата за прашања што се однесуваат на исполнување на нивната позиција, споделување корисни информации, итн. Таквата соработка им овозможува на офицерите за заштита на личните податоци полесно усогласување со прописите во ова поле.

Освен тоа, офицерите за заштита на личните податоци треба да учествуваат на обуките што ги организира АЗЛП кои не претставуваат само начин за проширување и продлабочување на нивното знаење, туку и дополнителна форма за зајакнување на соработката со Агенцијата.

1.1. Кои лица треба да бидат определени за офицери за заштита на личните податоци? Какви вештини и квалификации треба да поседуваат?

Член 41, став (5) од ЗЗЛП ги пропишува стручните квалификации на лицата кои се определуваат за офицери за заштита на личните податоци, како што се, на пример, познавање на законодавството и практиките за заштита на личните податоци, како и способност за исполнување на задачите дадени во член 43 од ЗЗЛП.

Конкретно, за офицер за заштита на личните податоци се определува лице кое:

- ги исполнува условите за вработување утврдени во овој или во друг закон;
- активно го користи македонскиот јазик;
- во моментот на определување за офицер, да не му е изречена, со правосилна судска одлука, казна или прекршочна санкција за забрана за вршење конкретна професија, дејност или должност;
- има завршено високо образование;
- има стекнати знаења и вештини во однос на практиките и прописите за заштита на личните податоци во согласност со одредбите од ЗЗЛП.

Овој проект е финансиран од Европската Унија

На ниво на Европската Унија, работната група за член 29 (РГ29) при Европскиот одбор за заштита на личните податоци има изготвено „Насоки за офицери за заштита на личните податоци“[6], каде се наведува следново:

- офицерот за заштита на личните податоци треба да има доволно разбирање на операциите за обработка што ги врши контролорот (т.е. соодветниот сектор и организација), како и на информатичките системи, безбедноста на податоци и потребите за заштита на личните податоци;
- во случај на државен или јавен орган, офицерот за заштита на личните податоци треба да има солидно познавање на (интерните) административни правила и постапки во рамките на организацијата.

1.2. Како е регулирано определувањето на офицер за заштита на личните податоци во ЗЗЛП?

Контролорите и обработувачите се должни да определат офицер за заштита на личните податоци во сите случаи каде:

1. обработката на лични податоци ја врши орган на државната управа, освен судовите, но само кога постапуваат во рамките на нивните надлежности, но треба да определат таков офицер за сите други обработки на лични податоци во согласност со ЗЗЛП;
2. примарната дејност на контролорот или обработувачот ја сочинуваат операции за обработки кои, по својата природа, обем и/ или цел налагаат редовно и систематско следење на субјектите на лични податоци од голем размер; или
3. примарната дејност на контролорот или обработувачот подразбира обемна обработка на посебни категории на лични податоци или лични податоци кои се однесуваат на кривични осуди или кривични дела онака како што се дадени во член 14 од ЗЗЛП.

1.2.1. Задолжително определување на офицер за заштита на личните податоци

Согласно член 41, став 1 од ЗЗЛП, обврската за задолжително определување офицер за заштита на лични податоци се однесува на:
1. *сите јавни органи*, со исклучок на судовите но само кога постапуваат во рамките на нивните надлежности[7];

[6] Насоките на работната група се достапни на следниот линк.
[7] Сепак, судовите се обврзани да определат офицер за заштита на личните податоци кој ќе се грижи за усогласеноста со прописите за заштита на личните податоци во однос на операциите за обработка на лични податоци кои се надвор од нивните судски надлежности.

2. контролорите чијашто *примарна дејност* ја сочинуваат операции за обработка на лични податоци кои поради нивната природа, обем и/или цел налагаат *редовно и систематско следење* на субјектите на личните податоци од *голем размер*; и
3. контролорите/обработувачите кои обработуваат *посебни категории* на лични податоци или лични *податоци поврзани со кривични осуди и кривични дела*.

ГДПР не обезбедува дефиниција за она што се подразбира под примарна дејност која вклучува редовно и систематско следење на субјектите на лични податоци, или пак дефиниција за обработка на лични податоци од голем размер.

Појаснување на термините

Сепак, Насоките изработени од РГ29 подетално ги елаборираат гореспоменатите концепти, односно:

- за јавни органи[8] треба да се сметаат и сите приватни компании со јавни овластувања или компании кои вршат дејност од јавен интерес;
  - ∅ следствено, државните и јавните органи вклучуваат национални, регионални и локални власти, но концептот, според важечките национални закони, типично вклучува и широк опсег на други тела кои го применуваат јавното право. Во вакви случаи, определувањето офицер за заштита на личните податоци е задолжително без оглед на видот и на обемот на податоци што се обработуваат;
- за примарна дејност на контролорот се сметаат клучните операции кои се потребни за постигнување на целите на контролорот, при што примарната дејност не мора да биде само онаа која се однесува на обработка на лични податоци, туку и други активности кои резултираат со обработка на лични податоци;
  - ∅ пример: давање услуги во областа на електронски комуникации, профилирање, следење на локација преку мобилни апликации, следење на фитнес состојбата и податоци за здравјето преку мобилни апликации, итн.

[8] ГДПР не дефинира што значи „државен или јавен орган“. РГ29 смета дека овој термин треба да се утврди во рамки на националниот закон. Следствено, државни и јавни органи вклучуваат национални, регионални и локални власти, но концептот, според применливите национални закони, обично вклучува и широк спектар на други тела кои се опфатени од јавното право.

Овој проект е финансиран од Европската Унија

- редовно и систематско следење на субјектите на лични податоци ги вклучува сите форми на следење и профилирање на интернет, земајќи го предвид фактот дека терминот следење не е ограничен само на онлајн средината;

    Ø пример: давање услуги во областа на електронски комуникации, профилирање, следење на локација преку мобилни апликации, следење на фитнес состојбата и податоци за здравјето преку мобилни апликации, итн.

- кога се утврдува дали станува збор за обработка од голем размер, РГ29 препорачува превид да се земат следните фактори:

    Ø бројот на субјекти на лични податоци, како апсолутен број или како дел од релевантната популација;
    Ø обемот на лични податоци што се обработуваат и/или опфатот на различни делови од личните податоци;
    Ø времетраењето, или постојаноста, на обработката на лични податоци;
    Ø географската дистрибуција на обработката на лични податоци.

Обврската за определување офицер за заштита на личните податоци се однесува и на контролорите и на обработувачите.

1.2.2. Доброволно определување офицер за заштита на личните податоци

Дури и кога ГДПР, односно ЗЗЛП не налага задолжително определување офицер за заштита на личните податоци, организациите може да сметаат дека е корисно да имаат таков офицер.

РГ29 охрабрува доброволно определување на офицер за заштита на личните податоци.

Притоа, кога некоја организација доброволно определува офицер за заштита на личните податоци треба да има предвид дека таквото определување, вклучително и позицијата и работните задачи на офицерот подлежат на исполнување на одредбите дадени во член 41 од ЗЗЛП исто како неговото/нејзиното определување да било законска обврска.

Овој проект е финансиран од Европската Унија

Ништо не спречува една организација која не е законски обврзана да определи офицер за заштита на личните податоци и не сака доброволно да определи таков офицер да задолжи некое вработено лице или да ангажира надворешен консултант за вршење на задачите поврзани со заштита на личните податоци. Во таков случај, важно е да се избегне секаква забуна во однос на работната позиција, статусот, положбата и задачите.

Оттука, севкупната комуникација во рамките на компанијата, како и комуникацијата со органите за заштита на личните податоци, со субјектите на лични податоци, и со јавноста, треба јасно да упатува на фактот дека работната позиција на лицето или консултантот не е офицер за заштита на личните податоци. Без оглед дали се определени доброволно или согласно законската обврска, офицерите за заштита на личните податоци се задолжени за сите операции за обработка што ги изведува контролорот или обработувачот.

Со други зборови, освен доколку не е очигледно јасно дека контролорот или обработувачот има законска обврска да определи ваков офицер, РГ29 препорачува контролорите или обработувачите да направат интерна анализа на релевантните фактори и критериуми за да утврдат дали да определат офицер за заштита на личните податоци или не. Контролорите или обработувачите кои доброволно определиле офицер за заштита на личните податоци ги имаат истите обврски како и контролорите кои со закон се обврзани да определат офицер.

1.2.3. Дали може надворешно лице да се определи како офицер за заштита на личните податоци?

Офицерот за заштита на личните податоци може да биде лице вработено кај контролорот или обработувачот (внатрешен офицер) или таквите задачи може да ги извршува лице ангажирано со договор на дело.

Овој проект е финансиран од Европската Унија

Согласно Насоките од РГ29, тоа значи дека и надворешно лице може да биде офицер за заштита на личните податоци и во таков случај оваа функција може да се извршува врз основа на договор на дело склучен меѓу лицето и организацијата. Кога позицијата офицер за заштита на личните податоци ја извршува надворешно лице врз основа на договор на дело, работните задачи може да ги извршува тим на лица кои работат за ангажираното правно лице, под водство на физичко лице кое е определено како лидер на тимот и одговорно за конкретниот клиент.

Во таков случај, од суштинско значење е секој член на надворешната организација која е ангажирана како офицер за заштита на личните податоци да ги исполнува соодветните услови пропишани во ЗЗЛП. За поголема правна јасност и добра организација, како и за да се спречи судир на интереси меѓу членовите на тимот, Насоките на РГ29 препорачуваат договорот да вклучи јасна распределба на работните задачи во рамките на надворешниот тим кој дејствува како офицер за заштита на личните податоци и определување лидер на тимот кој е одговорен за клиентот.

Во исто време, можно е комбинирање на индивидуални вештини и силни страни со цел неколку лица, кои работат како тим, да можат поефикасно да ги опслужуваат своите клиенти.

1.2.4. Еден офицер за заштита на личните податоци за еден или повеќе контролори/обработувачи

Насоките на РГ29 даваат можност за определување еден офицер за заштита на личните податоци кој опслужува повеќе контролори/обработувачи, и тоа во следниве случаи:

- ПРИВАТЕН СЕКТОР: помали компании кои работат заедно како одредена групација може да определат еден офицер;[9]
- ЈАВЕН СЕКТОР: земајќи ја предвид нивната организациска структура и големина, повеќе државни и јавни органи може да определат еден офицер за заштита на личните податоци[10]. Исто така, овој офицер може да биде ангажиран врз основа на договор на дело за обезбедување на таквите услуги.

[9] Доколку определеното лице е лесно достапно за секоја од компаниите
[10] Лицето може да биде ангажирано со договор за обезбедување на услугите.

Овој проект е финансиран од Европската Унија

Согласно Насоките на РГ29, офицерот за заштита на личните податоци треба да биде достапен на субјектите на лични податоци, надзорниот орган (АЗЛП), и треба да биде достапен за вработените во рамките на контролорот или обработувачот. Појаснувањето за достапноста на офицерот за заштита на личните податоци кој е определен за повеќе контролори се однесува и на јавниот и на приватниот сектор.

За да се обезбеди дека офицерот за заштита на личните податоци е достапен, без оглед дали станува збор за внатрешно или надворешно лице, важно е неговите контакт детали да бидат јавно објавени и споделени. Офицерот, со помош на тим кога тоа е потребно, мора да биде во позиција ефективно да комуницира со субјектите на лични податоци и да соработува со надзорниот орган. Меѓу другото, тоа значи дека комуникацијата мора да се одвива на јазикот/јазиците што ги користи АЗЛП и засегнатите субјекти на лични податоци. Достапноста на офицерот, без оглед дали станува збор за физичка достапност во рамките на деловните простории, преку интернет или преку некое друго безбедно средство за комуникација, е од суштинско значење за да се осигури дека субјектите на лични податоци можат да го контактираат.

Обврска за објавување на контакт деталите на офицерот

Член 41, став (7) од ЗЗЛП пропишува дека контролорот или обработувачот јавно ги објавува контакт деталите на офицерот за заштита на личните податоци и ја известува Агенцијата.

Целта е обезбедување лесен директен контакт и комуникација меѓу офицерот и субјектите на лични податоци и надзорниот орган. Контакт деталите на офицерот треба да ги вклучат следниве информации: телефонски број и електронска пошта, како и посебна форма за контакт на веб-страницата на контролорот. Оваа одредба не упатува на потребата за наведување на личното име на офицерот за заштита на личните податоци како дел од неговите/нејзините контакт детали.[11]

РГ29 препорачува надзорниот орган (АЗЛП) да биде информирана за името и контакт деталите на офицерот за заштита на личните податоци и истите да бидат објавени на веб-страницата на контролорот/обработувачот, во интерен телефонски именик или како дел од органограмот.

[11] Може да се користи и генеричка адреса за електронска пошта.

Овој проект е финансиран од Европската Унија

Обврска за тајност и доверливост на податоците

Освен тоа, офицерот за заштита на личните податоци има обврска за тајност и доверливост при извршување на неговите/нејзините задачи, но во исто време не подлежи на забрана за контактирање со и барање совет од АЗЛП.

1.3. Кои професионални стандарди треба да ги исполнува офицерот за заштита на личните податоци?

Со новото законодавство офицерот за заштита на личните податоци добива стратегиска и независна позиција за да се обезбеди поголема ефективност во извршувањето на оваа работна позиција и повисоко ниво на заштита на личните податоци.

Новиот закон пропишува дека офицерот за заштита на личните податоци треба да поседува професионални квалификации, стручно знаење за прописите и практиката, и способност за извршување на работните задачи како и да добие гаранции од раководството на контролорот за независно извршување на неговите/нејзините задачи.

Овој Водич ги дефинира сите професионални стандарди што треба да ги исполнуваат кандидатите за офицер за заштита на личните податоци, онака како што се утврдени во ЗЗЛП.

Главната цел на ваквите професионални стандарди е:

- утврдување на профилот на вешто и стручно лице кое се именува како офицер за заштита на личните податоци;
- дефинирање на минималните стандарди поврзани со позицијата офицер за заштита на личните податоци кои треба да бидат дизајнирани на начин кој ја обезбедува неговата/нејзината независност.

Овој проект е финансиран од Европската Унија

При определувањето офицер за заштита на личните податоци се препорачува контролорите да ги применат професионалните стандарди (услови) дефинирани подолу.

УСЛОВИ ЗА ОПРЕДЕЛУВАЊЕ ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 41, став (5) од ЗЗЛП пропишува дека офицерот за заштита на личните податоци се определува врз основа на неговите/нејзините професионални квалификации, а особено врз основа на стручни познавања на законот и практиките во областа на заштита на личните податоци и способноста да ги извршува задачите наведени во член 43 од ЗЗЛП.

Професионални барања:

- да ги исполнува условите за вработување утврдени во ЗЗЛП или некој друг закон;
- активно да го користи македонскиот јазик;
- во моментот на определување, со правосилна одлука да не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност;
- да има завршено високо образование;
- да има стекнати знаења и вештини поврзани со практиките и прописите за заштита на личните податоци во согласност со одредбите од ЗЗЛП.

Лични квалитети:

- лични вештини: интегритет, иницијативност, организираност, дискреција, истрајност, интерес и мотивација за извршување на оваа функција, како и високо ниво на професионална етика, развивање вештини и спроведување конкретни практики со наметнување промени кога тоа е потребно, и способност за извршување на пренесување на знаења и јасна позиција, како и лична и афирмација на позицијата кога е потребно;
- интерперсонални вештини: комуникација, способност за преговарање и решавање конфликти.

Овој проект е финансиран од Европската Унија

СЕРТИФИКАЦИЈА НА ОФИЦЕРИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ, ОДРЖУВАЊЕ И НАДГРАДУВАЊЕ НА СТРУЧНИТЕ ЗНАЕЊА

Законска обврска за сертификација

- издавање сертификат* за завршена обука за офицер за заштита на личните податоци како доказ за стекнати стручни знаења за прописите и практики во оваа област и како услов за определување на позиција офицер за заштита на лични податоци.

Законска обврска за одржување и надградување на стручните знаења
По именувањето на работната позиција, офицерите за заштита на личните податоци треба:

- да ги следат редовните обуки што ги организира АЗЛП, како и сертифицираните обуки што ги организираат други даватели на услуги кои се акредитирани за организација и испорака на обуки (професионални организации), како домашни така и од државите-членки на ЕУ;
- да воведат нови форми на обука како начин за само-подобрување преку мрежата на офицери.

1.4 Позиција и статус на офицерот за заштита на личните податоци

1.4.1. Стручност и вештини

Контролорите се одговорни да обезбедат примена и да демонстрираат усогласеност со прописите за заштита на личните податоци, при што офицерот за заштита на личните податоци е клучната фигура преку која контролорот ја исполнува оваа обврска.

Според член 42 од ЗЗЛП, контролорот и обработувачот се должни да обезбедат дека офицерот за заштита на личните податоци е соодветно и навремено вклучен во сите прашања поврзани со заштитата на личните податоци.

Овој проект е финансиран од Европската Унија

Освен тоа, контролорот и обработувачот се должни да обезбедат поддршка на офицерот за заштита на личните податоци при извршувањето на работните задачи наведени во член 43 од ЗЗЛП, преку обезбедување ресурси кои се неопходни за извршување на тие задачи и пристап до личните податоци и операциите за работа, и преку одржување на неговото/нејзиното стручно знаење.

Субјектите на лични податоци може да го контактираат офицерот за заштита на личните податоци за сите прашања поврзани со обработката на нивните лични податоци и за остварување на правата што им следуваат согласно ЗЗЛП.

Според ГДПР, односно ЗЗЛП, офицерот за заштита на личните податоци треба да биде независен во рамките на организацијата. Новото законско решение е изработено на начин кој обезбедува независност на офицерот или на извршувањето на таа позиција без какво било влијание и инструкции.

Сепак, независноста на офицерот за заштита на личните податоци не значи дека извршителот на оваа функција има овластувања за донесување одлуки бидејќи тоа би значело пречекорување на неговите/нејзините задачи и должности.

Фактот дека офицерот за заштита на личните податоци е дел од контролорот дава идеална можност за обезбедување усогласеност со прописите за заштита на личните податоци одвнатре, преку давање совети или интервенирање во случаи кога тоа е потребно за да се избегнат акции од страна на АЗЛП.

Доколку контролорот донесе одлука што е некомпатибилна со правилата и со советот од офицерот, тогаш офицерот за заштита на личните податоци треба да биде во можност да даде издвоено мислење.

1.4.2. Вклучување на офицерот за заштита на личните податоци во сите прашања поврзани со заштитата на личните податоци

Офицерот за заштита на личните податоци треба да биде соодветно и навремено вклучен (уште во раните фази) во сите прашања поврзани со заштита на личните податоци.

Овој проект е финансиран од Европската Унија

1.4.3. Гаранции за независноста на офицерот за заштита на личните податоци

Член 42, став (2) од ЗЗЛП пропишува дека контролорот и обработувачот мора да обезбедат дека офицерот за заштита на личните податоци не добива никакви инструкции во однос на извршување на неговите/нејзините работни задачи.

Член 42, став (3) од ЗЗЛП воспоставува одредени основни гаранции кои им помагаат на офицерите за заштита на личните податоци да бидат во можност да ги извршат нивните работи задачи со задоволително ниво на самостојност во рамките на организацијата. Појаснувачката белешка бр. 97 (рецитал) кон ГДПР додава дека „без оглед дали се вработени лица кај контролорот или не, офицерите за заштита на личните податоци треба да бидат во позиција да ги извршуваат своите должности и задачи на независен начин“.

Насоките на РГ29 појаснуваат дека офицерите не смеат да добиваат инструкции како да се справат со некои работи, на пример, кои резултати треба да се постигнат, како да се истражи некоја поплака, или дали да се консултираат со надзорниот орган.

Контролорот и обработувачот остануваат одговорни за усогласеноста со законот за заштита на личните податоци и мора да го демонстрираат тоа.

Доколку контролорот или обработувачот донесат одлуки кои се некомпатибилни со ГДПР/ЗЗЛП и со советот од офицерот, тогаш офицерот за заштита на личните податоци треба да биде во можност да даде издвоено мислење до највисокото раководно ниво и до лицата кои донесуваат одлуки.

1.4.4. Судир на интереси

Член 42, став (6) од ЗЗЛП пропишува дека офицерот за заштита на личните податоци може да врши и други задачи и должности. Контролорите и обработувачите се должни да обезбедат дека таквите задачи и должности не доведуваат до судир на интереси.

Овој проект е финансиран од Европската Унија

Отсуството на судир на интереси е тесно поврзано со барањето за независно извршување на функцијата. Иако на офицерите за заштита на личните податоци им е дозволено да извршуваат други задачи и должности, таквите задолженија не треба да доведат до судир на интереси.

Според Насоките на РГ29 тоа посебно се однесува на фактот дека офицерот за заштита на личните податоци не може да извршува позиција во рамките на организацијата која може да го доведе во ситуација да ги утврдува целите на и средствата за обработка на личните податоци. Поради специфичната организациска структура на една организација, оваа одредба треба да се разгледува на основа од-случај-до-случај.

Согласно позитивните практики, позиции во рамките на организацијата кои може да бидат во судир со ова правило вклучуваат високи раководни позиции (на пример, извршен директор, оперативен директор, финансиски директор, раководител на одделение за маркетинг, раководител на одделение за човечки ресурси, или раководители на одделение за информатичка технологија), но и други пониски позиции во рамките на организациската структура доколку истите подразбираат утврдување на целите и средствата за обработка на лични податоци.

Освен тоа, судир на интереси може да се јави, на пример, доколку од надворешно ангажиран офицер за заштита на личните податоци се бара да го претставува контролорот или обработувачот пред суд во предмети кои вклучуваат прашања поврзани со заштита на личните податоци.

Во зависност од дејноста, големината и структурата на организацијата, добри практики за контролорите или обработувачите вклучуваат:

- идентификување работни позиции кои се некомпатибилни со работните задачи на офицерот за заштита на личните податоци;
- изготвување интерни правила за спречување судир на интереси;
- обезбедување погенерално објаснување за судир на интереси;

Овој проект е финансиран од Европската Унија

- депонирање изјава дека офицерот за заштита на личните податоци нема судир на интереси во однос на извршувањето на таа функција како начин за градење на свеста за овој услов;
- вградување заштитни мерки во интерните правила на организацијата за да се обезбеди дека огласот за пополнување на работната позиција офицер за заштита на личните податоци или договорот на дело за таа функција се доволно прецизни и детални за да се избегне судир на интереси.

Во овој контекст, треба да се има предвид дека судирот на интереси може да има различна форма во зависност од тоа дали офицерот е ангажиран од рангот на вработените или како надворешно лице.

1.5. Определување и разрешување на офицер за заштита на личните податоци

Според член 42 од ЗЗЛП, офицерот за заштита на личните податоци не смее да биде отпуштен од работното место или казнет од контролорот или обработувачот за извршување на своите работни задачи. Офицерот за заштита на личните податоци директно одговара пред највисокото раководно ниво на контролорот или обработувачот.

Неколку добри практики кои обезбедуваат усогласеност на контролорите и обработувачите со барањата пропишани во член 42 од ЗЗЛП вклучуваат:

Определување/разрешување

- определување на носителот на функцијата офицер за заштита на личните податоци за неопределено време или за колку што е можно подолг временски период;
- доставување на контакт информациите за определениот офицер за заштита на личните податоци до АЗЛП;
- отповикување/разрешување на носителот на функцијата офицер за заштита на личните податоци само доколку лицето повеќе не ги исполнува условите за извршување на работните задачи и должности.

Овој проект е финансиран од Европската Унија

Човечки и други ресурси

- обезбедување на потребните човечки и други ресурси за извршување на работните задачи, вклучително и пристап до операциите за обработка на личните податоци, како и овозможување одржување и унапредување на стручните знаења на офицерот за заштита на личните податоци;
- изработување работен план за проценка на потребите за човечки и други ресурси;
- активна поддршка од највисокото раководно ниво во однос на обезбедување на потребниот персонал, финансиски ресурси и инфраструктура кои се соодветни за позицијата офицер за заштита на личните податоци.

Ослободување од други работни задачи и должности

- соодветно ослободување на офицерот за заштита на личните податоци од други задачи и должности со цел да се фокусира на задачите кои се поврзани со вршењето на оваа функција.

Соодветна внатрешната структура во рамките на контролорот

- соодветно организирање на внатрешната структура според која офицерот за заштита на личните податоци раководи со одделението за заштита на личните податоци (доколку е воспоставено), или ја извршува таа функција како самостојно лице со соодветно ниво во рамките на хиерархијата на контролорот кое гарантира независно делување, односно раководење на оваа функција на начин кој спречува какво било влијание или добивање инструкции за извршувањето на работните задачи;
- исклучување на можноста за отповикување или казнување на носителот на функцијата офицер за заштита на личните податоци поради извршување на неговите/нејзините работни задачи.

Регулирање на соработката со највисокото раководно ниво како дел од интерните прописи

- информирање на највисокото раководно ниво за важни прашања од областа на заштитата на личните податоци, во најмала рака на секои три месеци, и одржување тематски состаноци кога тоа е потребно;
- директна одговорност на офицерот за заштита на личните податоци пред највисокото раководно ниво;
- обезбедување видливост на функцијата офицер за заштита на личните податоци во рамките на организациската структура;
- регулирање на обврската за сите вработени да соработуваат со офицерот за заштита на личните податоци без да бараат претходна дозвола за тоа од нивните надредени;
- усвојување интерни прописи кои ги уредуваат случаите на задолжителна консултација со офицерот за заштита на личните податоци;
- овластување на офицерот за заштита на личните податоци да ја парафира кореспонденцијата која се однесува на заштитата на личните податоци;
- определување заменик офицер за заштита на личните податоци за да се обезбеди континуитет во извршувањето на оваа функција во случаи на отсуство на офицерот, при што заменикот треба да ги има истите гаранции за независно извршување на неговата/нејзината функција.

Регулирање на спроведувањето ревизии/контроли/проверки

- донесување детални правила за спроведување ревизии/контроли/проверки од страна на офицерот за заштита на личните податоци;
- овозможување пристап на офицерот за заштита на личните податоци до просториите и системите каде се извршуваат операциите за обработка, и воведување обврска за комуникација со лицата кои поднеле поплака за повреда на законодавството во областа на заштита на личните податоци.

ЕЛЕМЕНТИ КОИ ЈА ОСЛАБУВААТ ПОЗИЦИЈАТА НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Доколку офицерот извршува и други работни задачи дополнително на оние поврзани со неговата функција, тој/таа може да се соочи со конфликт во однос на времето поминато на извршување на задачите кои не се директно поврзани со неговата/нејзината функција и намерата за извршување на задачите поврзани со заштитата на личните податоци. Оттука, во ситуации каде претпоставените даваат поголема тежина на другите задачи тоа може да создаде притисок врз офицерот за заштита на личните податоци да се фокусираат на тие задачи и може да доведе до неефикасно извршување на задачите поврзани со неговата/нејзина функција. Освен тоа, постои голема веројатност таквите задачи да доведат до судир на интереси.

Кога офицерот за заштита на личните податоци има договор за работа на определено време, тој/таа е ставен во понеповолна позиција и веројатно ќе покаже помала упорност и посветеност на извршување на задачите за разлика од офицер кој има договор за работа на неопределено време поради загриженоста дали договорот за работа ќе биде продолжен или не.

Веројатно е дека офицерите кои се директно одговорни пред или се под контрола на друго претпоставено лице може да чувствуваат притисок, при што нивното независно извршување на оваа функција може негативно да влијае врз напредувањето во кариерата. Имено, коректно и соодветно извршување на задачите на офицерот за заштита на личните податоци честопати налага тие да заземат цврст став кој е спротивен на надредените лица и да бараат исполнување на обврските од лица кои имаат повисоки функции во рамките на контролорот, и од тие причини може да бидат перципирани како „бирократи“ или „создавачи на проблеми“.

Офицерите за заштита на личните податоци треба да имаат независен статус што им помага да ги издржат притисоците и тешкотиите кои се поврзани со оваа важна функција. Оттука, за да се олесни таквиот притисок, офицерите треба да бидат директно одговорни пред највисокото раководно ниво во рамките на контролорот.

Овој проект е финансиран од Европската Унија

Офицерите за заштита на личните податоци кои се во позиција да бараат човечки и други ресурси од директно претпоставените лица може да се соочат со тешкотии доколку претпоставените лица не се целосно посветени на постигнување усогласеност со прописите за заштита на личните податоци. Таквата ситуација може да се избегне доколку офицерот има сопствен буџет и неговите/нејзините барања се предмет на одобрување од страна на највисокото раководно ниво во рамките на контролорот.

1.6. Препораки за контролори со различна големина на организација

Критериуми за категоризација

Утврдувањето критериуми за категоризација на контролорите во зависност од нивната големина е тешко бидејќи постојат контролори со мал број вработени, но голем број операции за обработка на лични податоци или обработка на посебни категории на лични податоци, и обратно, постојат контролори со голем број вработени кои не извршуваат обработка на лични податоци освен онаа поврзана со личните податоци на нивните вработени.

Од тие причини, тешко е да се утврдат помал број обврски поврзани со извршувањето на функцијата офицер за заштита на личните податоци кај помалите наспроти поголемите контролори.

Од друга страна, факт е дека помалите контролори немаат доволно човечки и финансиски ресурси за да ги исполнат законските обврски поврзани со извршувањето на оваа функција.

Мали контролори

- еден офицер за заштита на личните податоци може да се определи за повеќе помали контролори кои работат заедно како група на контролори или кои немаат сложена организациска структура;
- офицерите за заштита може да се ангажираат со договор на дело;
- во случај кога офицерот врши и други задачи, контролорите треба да обезбедат гаранции дека не постои судир на интереси со нивната примарна функција.

Овој проект е финансиран од Европската Унија

Големи контролори

- утврдување на позицијата офицер за заштита на личните податоци како работно место со полно работно време, што значи ослободување на извршителот на функцијата од други работни задачи и должности за да може да се посвети на работните задачи поврзани со заштитата на личните податоци;
- обезбедување на потребните човечки и други ресурси за офицерот за заштита на личните податоци да може да ги изврши работните задачи. Кога обемот на работа го налага тоа, контролорот треба да формира тим, воден од офицерот, за извршување на работните задачи поврзани со заштитата на личните податоци. Внатрешната структура на тимот, како и должностите и одговорностите на секој член на тимот, мора да бидат јасно дефинирани.
- спроведување проценка на влијанието врз заштитата на личните податоци во однос на планираните операции за обработка, кога таков процес не е претходно воспоставен во рамките на контролорот.

Овој проект е финансиран од Европската Унија

ДЕЛ 2: ЗАДАЧИ НА ОФИЦЕРОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Овој дел од Водичот детално ги елаборира задачите на офицерот за заштита на личните податоци, онака како што се регулирани во Законот за заштита на личните податоци.

2. Информирање за и постапување по барања за заштита на правата на субјектите на лични податоци

Офицерот за заштита на личните податоци е обврзан да ги информира субјектите на лични податоци за нивните права, но во исто време и да го советува контролорот за неговите обврски кои произлегуваат од прописите за заштита на личните податоци.

2.1. Права на субјектите на лични податоци

Субјектите на личните податоци согласно Законот за заштита на личните податоци ги имаат следните права:

- Право на информации
- Право на пристап до личните податоци
- Право на исправка
- Право на бришење („право да се биде заборавен“)
- Право на ограничување на обработката
- Право на пренесливост на податоците
- Право на приговор
- Право да не се биде предмет на автоматизирано донесување индивидуални одлуки, вклучително и профилирање

Повеќе за правата на субјектите може да прочитате во Информаторот на тема „Правата на граѓаните како субјекти на личните податоци“.

Овој проект е финансиран од Европската Унија

Барање за измена, модификација и бришење или прекин на обработката на лични податоци.

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

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

Во рок од 30 дена по приемот на барање, контролорот е обврзан да го извести субјектот на лични податоци за дополнувањето, изменувањето или бришењето на личните податоци.

Во овој контекст, офицерот за заштита на личните податоци е задолжен за остварување на правата на субјектите на лични податоци и за исполнување на обврските на контролорот.

2.2. Обврски на контролорот/обработувачот

2.2.1. Почитување на начелата за заштита на личните податоци

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

- **Законитост, правичност и транспарентност**

Секоја обработка на лични податоци треба да биде законита и правична. Во исто време, таа треба да биде транспарентна, што значи дека физичките лица треба да бидат информирани за собирањето, користењето, консултирањето и некоја друга обработка на нивните лични податоци, како и за степенот до кој податоците се обработуваат или ќе бидат обработени. Начелото за транспарентност налага информациите и комуникацијата во врска со обработката на лични податоци да бидат лесно достапни и разбирливи, односно да бидат дадени на јасен и едноставен јазик.

- **Ограничување на целите**

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

- **Минимален обем на податоци**

Обработката на личните податоци мора да биде соодветна, релевантна и ограничена само на она што е неопходно за постигнување на целите на таквата обработка. Личните податоци треба да се обработуваат само доколку целта на обработката не може разумно да се постигне на некој друг начин. Тоа налага ограничување на периодот за чување на личните податоци на најкраткиот можен период.

- **Точност**

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

- **Ограничување на рокот за чување**

Личните податоци треба да се чуваат во форма која дозволува идентификација на субјектите на лични податоци само во период што е потребен за целите за кои се обработуваат. За да се обезбеди дека личните податоци не се чуваат подолго од она што е потребно, контролорите треба да утврдат временски рок за бришење на личните податоци или за периодична ревизија.

- **Интегритет и доверливост**

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

Овој проект е финансиран од Европската Унија

- **Отчетност**

На крај, контролорите се одговорни за и мора да демонстрираат усогласеност со сите горенаведени начела за заштита на личните податоци. Имено, контролорите мора да преземат одговорност за нивната обработка на личните податоци и усогласеноста со ЗЗЛП, и да бидат во можност да ја докажат истата, вклучително и пред АЗЛП, со приложување соодветна евиденција и примена на мерки.

Повеќе информации за начелата за заштита на личните податоци може да прочитате во „Водичот за начелата за заштита на личните податоци“.

2.2.2. Законски основ за обработка на личните податоци

Контролорите/обработувачите мора да имаат законски основ за обработка на личните податоци.

Според ЗЗЛП, постојат шест законски основи за обработка. Контролите се обврзани да обезбедат законита обработка на лични податоци. Можните правни основи за законска обработка се:

- **Согласност од субјектот на лични податоци**

Субјектот на лични податоци дава согласност на контролорот за обработка на неговите/нејзините лични податоци за една или повеќе цели на обработка. Согласноста мора да биде слободно дадена, јасна и треба лесно да може да се повлече, па затоа контролорите треба да внимаваат кога користат согласност како правен основ за обработка на лични податоци. Во таа насока, ГДПР стави крај на практиките со автоматски штиклирани полиња за согласност.

- **Извршување на договор каде една страна е субјект на лични податоци**

Овој правен основ подразбира ситуации во кои активноста за обработка на лични податоци е потребна за склучување или извршување на договор. Доколку активноста не се поврзува со условите на договорите, тогаш обработката на лични податоци мора да биде опфатено со некој друг правен основ.

- **Законска обврска на контролорот**

Тука влегуваат ситуации каде активноста за обработка на лични податоци е потребна за исполнување на некоја обврска пропишана со закон кој се применува на контролорот, на пример, за работни односи, за заштита на потрошувачите итн.

- **Заштита на животот или суштински интерес на субјектот на лични податоци**

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

- **Вршење работи од јавен интерес или јавно овластување**

Активност за обработка на лични податоци која ја вршат органи на државната управа или организации кои извршуваат јавни овластувања во име на органите на државната управа.

- **Легитимен интерес**

Тоа подразбира активност за обработка на лични податоци која субјектот на лични податоци обично ја очекува од организацијата на која ѝ ги дава своите лични податоци, на пример маркетиншки активности или спречување измама. Кога организацијата користи легитимен интерес како правен основ за обработката, таа мора да спроведе тест за балансирање, односно да утврди дали активноста за обработка е неопходна за организацијата да функционира/да ја врши својата дејност или дали активноста за обработка има предимство пред правата и слободите на субјектот на лични податоци. Доколку одговорот на некое од овие прашања е негативен, тогаш организацијата не може да го користи легитимниот интерес како правен основ за обработката.

Повеќе информации за законитоста на обработката на личните податоци може да прочитате во „Водичот за законитост на обработката на личните податоци“.

Овој проект е финансиран од Европската Унија

2.2.3. Известување за обработка (на личните податоци) со висок ризик

Кога при користење на технологии за некој вид на обработка, земајќи ги предвид природата, обемот, контекстот и целите на обработката на лични податоци, постои веројатност истата да предизвика висок ризик за правата и слободите на физичките лица, во функција на член 9 од ЗЗЛП, контролорот ја известува Агенцијата за заштита на личните податоци преку електронската евиденција на збирки на лични податоци чија што обработка е со висок ризик достапна на следниот линк.

2.2.4. Нова обврска: известување за нарушување на безбедноста на личните податоци

Законот за заштита на личните податоци воведуваат нова обврска за контролорите во случај на нарушување на безбедноста на личните податоци[12] која подразбира известување на надзорниот орган (АЗЛП) и на засегнатите субјекти на лични податоци.

Имено, контролорите се обврзани да ја информираат Агенцијата за нарушување на безбедноста на личните податоци освен ако не постои веројатност дека нарушувањето ќе резултира со ризик по правата и слободите на субјектите на личните податоци. Оттука, за секое нарушување на безбедноста на личните податоци контролорот треба да процени дали постои обврска за известување на Агенцијата.

Пример: Контролорот треба да ја извести Агенцијата за губење на лични податоци на корисниците бидејќи таквиот настан може да доведе до кражба на идентитет, но не мора да ја извести Агенцијата во случај на губење податоци кои се однесуваат на список со телефонски броеви на вработените, бидејќи таквото нарушување не влијае врз правата и слободите на субјектите на лични податоци.

[12] „Нарушување на безбедност на личните податоци“ е секое нарушување на безбедноста, што доведува до случајно или незаконско уништување, губење, менување, неовластено откривање или пристап до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат.

Овој проект е финансиран од Европската Унија

Во случај кога постои веројатност дека нарушувањето на безбедноста на личните податоци ќе резултира во висок ризик по правата и слободите на субјектите на лични податоци[13], контролорот треба директно да ги извести и засегнатите субјекти.

Контролорите немаат обврска за известување на субјектите на лични податоци за нарушувањето на безбедноста на личните податоци во следниве случаи:

- кога контролорот применил соодветни технички и организациски мерки, вклучително и мерки во однос на личните податоци кои се засегнати од нарушувањето;
- кога контролорот преземал дополнителни мерки за да обезбеди дека не повее не постои веројатност за појава на висок ризик по правата и слободите на субјектите на лични податоци;
- кога доставувањето на такво известување претставува несразмерно голем напор, во кој случај контролорот може да направи јавно известување или некоја слична ефективна мерка за известување на субјектите.

Доколку контролорот не ги известил субјектите на лични податоци и Агенцијата за конкретно нарушување на безбедноста на личните податоци кое претставува висок ризик по правата и слободите на субјектите, Агенцијата може да побара контролорот:

- да ги извести субјектите за конкретното нарушување; или
- да докаже дека исполнува еден од условите за кои не постои обврска за известување.

Известувањето што контролорите го доставуваат до Агенцијата треба да ги содржи следниве информации:

- опис на природата на нарушувањето и, доколку е можно, категориите и приближниот број на засегнати субјекти на лични податоци и приближниот број на засегнати евидентирани лични податоци;

[13] За висок ризик по правата и слободите на субјектите на лични податоци се смета физичка, материјална или нематеријална штета за субјектите, како што е загуба на контрола врз нивните лични податоци, ограничување на правата, дискриминација, кражба на идентитет, измама со лажен идентитет, финансиски загуби, повреда на доверливоста на личните податоци или каква било друга негативна економска или социјална последица за засегнатото лице.

Овој проект е финансиран од Европската Унија

- име/презиме и контакт детали на офицерот за заштита на личните податоци или друго лице за контакт од кое може да добијат повеќе информации;
- опис на можните последици од нарушувањето на безбедноста на личните податоци;
- опис на предложените или преземените мерки од страна на контролорот за справување со нарушувањето или за намалување на негативните ефекти.

Содржината на известувањето за субјектите на лични податоци треба да биде иста, но природата на нарушувањето треба да се опише со поедноставен јазик.

Исто така, известувањето треба да биде поднесено веднаш и не подоцна од 72 часа откако контролорот дознал за нарушувањето на безбедноста на личните податоци. Доколку контролорот не поднесе вакво известување во рок од 72 часа, тогаш заедно со известувањето што се доставува подоцна треба да се образложат и причините за доцнењето.

Обврска за документирање
Контролорите се обврзани да ги документираат сите нарушувања на безбедноста на лични податоци, вклучително и фактите поврзани со нарушувањето, последиците и активностите што биле преземени за справување со истото. Ваквата документација ѝ овозможува на Агенцијата да ја провери усогласеноста со член 37 од ЗЗЛП.

2.2.5. Евиденција на активностите за обработка

Според член 34 од ЗЗЛП, контролорите и, кога е соодветно, овластените претставници на контролорите водат евиденција за активностите за обработка на лични податоци за кои се одговорни.

Ваквата евиденција треба да ги содржи следниве информации:
(а) назив, односно име/презиме и контакт детали на контролорот и, кога е соодветно, на сите заеднички контролори, овластеното лица на контролорот и офицерот за заштита на личните податоци;
(б) целите на обработката;

(б) целите на обработката;
(в) опис на категориите на субјекти на лични податоци и категориите на лични податоци
(г) категориите на корисници на кои им се откриени или ќе им бидат откриени личните податоци, вклучително и корисници во трети земји или меѓународни организации;
(д) кога е соодветно, пренос на личните податоци во трета земја или меѓународна организација, вклучително и идентификација на третата земја или меѓународната организација, додека во случај на пренос на лични податоци според член 53, став (1), алинеја 2) од ЗЗЛП, документација за примена на соодветни заштитни мерки;
(ѓ) кога е соодветно, предвидениот рок за бришење на различни категории на лични податоци;
(е) кога е соодветно, генерален опис на техничките и организациските мерки според член 36, став (1) од ЗЗЛП.

2.3. Следење на усогласеноста со ЗЗЛП

Офицерите за заштита на личните податоци ја следат усогласеноста со ЗЗЛП, другите прописи на Република Северна Македонија и политиките на контролорот/обработувачот кои се однесуваат на заштитата на личните податоци, вклучително и распределување на одговорности, подигнување на свеста и обука на вработените кои учествуваат во операциите за обработка, како и спроведување ревизии на заштитата на личните податоци (член 43, став (1), точка (б) од ЗЗЛП).

Конкретно, офицерот помага во обезбедувањето на внатрешната усогласеност со овие прописи. Тој/таа собира информации за идентификување на операциите за обработка на лични податоци, анализа и потврда на усогласеноста, и дава информации, совети и препораки на контролорот.

Офицерот не е лично одговорен во случај на неусогласеност со прописите за заштита на личните податоци. Усогласеноста со овие прописи е одговорност на контролорот.

ЗЗЛП јасно пропишува дека контролорот обезбедува усогласеност со одредбите од законот и демонстрира дека обработката на личните податоци се врши во согласност си истите, додека офицерот за заштита на личните податоци е клучна фигура преку која контролорот ја исполнува оваа обврска.

Овој проект е финансиран од Европската Унија

Усогласеноста и следење на усогласеноста со прописите за заштита на личните податоци подразбира: почитување на начелата за заштита на личните податоци при обработката на лични податоци од страна на контролорот; подготовка на документација за и примена на технички и организациски мерки, изработка на политика/изјава за приватност и редовно ажурирање на истата; информирање за собирањето на лични податоци и почитување на правилата за видео надзор. Новото законско решение воведува и обврска за контролорите за известување на нарушување на безбедноста на личните податоци.

2.4. Подигнување на свеста за заштитата на личните податоци

Подигнување на свеста меѓу вработените кај контролорот за правото на заштита на личните податоци е една од клучните работни задачи на офицерот за заштита на личните податоци која го афирмира ова правото на физичките лица и го едуцира контролорот за обврските кои произлегуваат од прописите за заштита на личните податоци.

Офицерот за заштита на личните податоци треба да користи колку што е можно повеќе активности за подигнување на свеста во рамките на контролорот, особено меѓу вработените кои се директно вклучени во операциите за обработка на лични податоци.

2.5. Обука на вработените

ЗЗЛП пропишува обврска за офицерите за заштита на личните податоци да вршат обука на вработените во однос на заштитата на личните податоци.

Согласно член 69 од ЗЗЛП, Агенцијата подготвува и спроведува обука за вработените кај контролорите и обработувачите, како и за офицерите за заштита на личните податоци. По спроведената обука, АЗЛП издава сертификати за успешно завршена обука и води евиденција за истото. Целта на овие обуки е вработените кај контролорите и обработувачите да се стекнат со знаења во областа на заштита на личните податоци, а офицерите да се стекнат со знаења и вештини за прописите и практиките во областа на заштита на личните податоци и да развијат способности за извршување на задачите кои се уредени во член 43 од ЗЗЛП.

Овој проект е финансиран од Европската Унија

2.6. Давање совети и препораки на контролорот/обработувачот

Обврските на офицерот за заштита на личните податоци вклучува и давање совети на контролорот за исполнување на обврските кои произлегуваат од прописите за заштита на личните податоци и препораки за практично подобрување на заштитата на личните податоци.

Советите може да се дадат усно или во пишана форма. Доколку некој совет даден за конкретен случај може да се примени во други слични случаи, се препорачува тоа да биде објавено на веб-страницата на контролорот. Во случај кога офицерот има дилема за тоа како совет да му даде на контролорот, се препорачува тој/таа да се консултира со надзорниот орган (АЗЛП).

Офицерот дава препораки на контролорот/обработувачот за практично подобрување на заштитата на личните податоци. Овие препораки може да се дадат на сопствена иницијатива или на барање од контролорот/обработувачот.

2.7. Ревизии/контроли/проверки

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

Постапката и начинот на вршење ревизии/контроли/проверки од страна на офицерот за заштита на личните податоци треба да бидат регулирани со интерен акт на контролорот.

2.8. Проценка на влијанието врз заштитата на личните податоци

Користењето на алатката за проценка за влијанието на планираните операции за обработка врз заштитата на личните податоци (ПВЗЛП)[14] е најефективниот начин обезбедување усогласеност со прописите за заштита на личните податоци и за исполнување на очекувањата на субјектите на лични податоци во однос на приватноста.

[14] Правилник за процесот на проценка на влијанието врз заштитата на личните податоци, достапен на следниот линк

Имено, член 39 од ЗЗЛП пропишува дека во случаи кога се користат нови технологии за некој вид на обработка, и кога според природата, обемот, контекстот и целите на обработката, постои веројатност дека таквата обработка ќе резултира со висок ризик по правата и слободите на физичките лица, пред да почне со обработката, контролорот треба да направи проценка на влијанието врз заштитата на личните податоци. Една проценка може да однесува на серија слични операции за обработка кои претставуваат слични високи ризици.

Иако спроведување на ваква проценка е задача на контролорот, офицерот за заштита на личните податоци има важна и корисна улога преку давање конкретни совети и следење дали контролорот ги почитува дадените и прифатените совети. Доколку контролорот не го прифати советот од офицерот, тоа треба да биде соодветно документирано, заедно со образложение на причините за таквото неприфаќање.

Оваа алатка им овозможува на контролорите да ги идентификуваат и решаваат проблемите уште во раната фаза на развивање нови системи и нови производи, и да ги намалат непотребните трошоци и потенцијалната штета по нивната репутација како можни негативни последици.

Алатката веќе е воведена и се користи од страна на некои контролори во приватниот сектор, особено оние кои работат во банкарскиот сектор и во областа на електронските комуникации.

Согласно член 39, став (3) од ЗЗЛП, проценката на влијанието врз заштитата на личните податоци е задолжителна во следниве случаи:
(а) системска и сеопфатна оценка на личните аспекти кои се поврзани со физички лица, која се заснова на автоматска обработка, вклучително и профилирање, а која служи како основа за донесување одлуки што произведуваат правно дејство во врска со физичкото лице или значително влијаат врз физичкото лице;
(б) обемна обработка на посебни категории на лични податоци согласно член 13 од ЗЗЛП или на лични податоци поврзани со кривични осуди и кривични дела согласно член 14 од ЗЗЛП; или
(в) систематско набљудување на јавни простори од голем размер.

Притоа, проценката треба да ги содржи следниве информации:

а) систематски опис предвидените операции за обработка и целите на обработката, вклучително и легитимните интереси на контролорот, кога тоа е применливо;
б) проценка на неопходноста и пропорционалноста на операциите за обработка во однос на целите;
в) проценка на ризиците по правата и слободите на субјектите на лични податоци од член 39, став (1) од ЗЗЛП; и
г) предвидени мерки за решавање на ризиците, вклучително и заштитни мерки, мерки и механизми за безбедност на личните податоци и за демонстрирање усогласеност со ЗЗЛП, земајќи ги предвид правата и легитимните интереси на субјектите на лични податоци и другите засегнати лица.

Согласно член 39, став (4) и став (5) од ЗЗЛП, Агенцијата за заштита на личните податоци заедно со правилникот има донесено и објавено две листи на видови операции за обработка на лични податоци кои налагаат/не налагаат задолжителна проценка на влијанието врз заштитата на личните податоци.[15][16]

Согласно Насоките за офицери за заштита на личните податоци изработени од работната група 29 (РГ29), спроведувањето проценка на влијанието врз заштитата на личните податоци (член 35, став (1) од ГДПР) е задача на контролорите, не на офицерите. Сепак, офицерите може да имаат многу важна и корисна улога преку советување на контролите за исполнување на оваа обврска.

Кој е обврзан да спроведе проценка на влијанието?
ЗЗЛП пропишува дека обврската за спроведување на проценка на влијанието врз заштитата на личните податоци паѓа на контролорите, и таа треба да се направи во консултација со офицерот за заштита на личните податоци и со обработувачите (член 39, став (1) и став (2)). Проценката на влијанието може да ја направи и некое друго лице, во и вон организацијата, но крајната одговорност за исполнување на оваа обврска останува на контролорот.[17]

[15] Листата на видовите операции на обработка за кои не се бара проценка на влијанието врз заштитата на личните податоци е достапна на следниот линк
[16] Листата на видовите операции на обработка за кои се бара проценка на влијанието врз заштитата на личните податоци е достапна на следниот линк
[17] Правилник за процесот на проценка на влијанието врз заштитата на личните податоци, достапен на следниот линк.

Овој проект е финансиран од Европската Унија

Кога има определено офицер за заштита на личните податоци, контролорот е должен да побара совет при спроведувањето на проценката на влијанието (член 39, став (2) од ЗЗЛП), при што советот, како и одлуката на контролорот дали го прифаќа или одбива, треба да биде документиран во ПВЗЛП. Од друга страна, офицерот го следи спроведувањето на проценката на влијанието (член 43, став (1), алинеја (в)) од ЗЗЛП) Доколку контролорот има ангажирано обработувач кој е задолжен за целосна или делумна обработка на лични податоци, обработувачот му помага на контролорот во спроведувањето на проценката на влијанието и ги обезбедува сите потребни информации (член 32, став (3), алинеја (ѓ) од ЗЗЛП).

РГ29 препорачува контролорите да побараат совет од офицерот за заштита на личните податоци за следниве прашања:

- дали треба да се спроведе проценка на влијанието врз заштитата на личните податоци;
- која методологија да се примени за спроведување на проценка на влијанието врз заштитата на личните податоци;
- дали спроведувањето на проценката на влијанието да биде направена во самата организација или да се ангажира надворешно лице;
- какви заштитни мерки, вклучително и технички и организациски мерки, да се применат за ублажување на можните ризици по правата и интересите на субјектите на лични податоци;
- дали проценката на влијанието е коректно спроведена и дали заклучоците од истата во однос на продолжувањето на обработката и заштитните мерки што ќе се применат се во согласност со ЗЗЛП.

Доколку контролорот не се согласува со советот даден од офицерот за заштита на личните податоци, документацијата поврзана со проценката на влијанието врз заштитата на личните податоци треба да вклучи образложение на причините зошто советот на офицерот не бил земен превид.

Подетални упатства се дадени во Насоките за офицери за заштита на лични податоци издадени од РГ29.

Овој проект е финансиран од Европската Унија

2.9. Соработка со АЗЛП и дејствување како контакт точка

Согласно член 43 од ЗЗЛП, офицерот за заштита на личните податоци дејствува како контакт точка за Агенцијата во однос на прашања поврзани со обработката, вклучително и претходно консултација согласно член 40 од ЗЗЛП, како и советување за други прашања, кога е соодветно.

Офицерите за заштита на личните податоци од јавниот и приватниот сектор веќе имаат воспоставено соработка со АЗЛП која вклучува поддршка од Агенцијата за прашања поврзани со извршувањето на нивната функција, споделување информации и друга комуникација. Ваквата соработка ѝ овозможува на АЗЛП доследно да ја следи усогласеноста со прописите за заштита на личните податоци. Освен тоа, офицерите учествуваат и во обуките што ги организира АЗЛП кои не се сметаат само како алатка за продлабочување и надградување на нивните стручни знаења, туку и како начин за зајакнување на соработката со Агенцијата и меѓу офицерите.

Зајакнување на соработката меѓу АЗЛП и контролорите е од суштинско значење за воспоставување повисоки стандарди во однос на почитувањето на правото на заштита на личните податоци, а офицерите имаат централна улога во зајакнувањето на таквата соработка.

Офицерите за заштита на личните податоци дејствуваат како контактна точка која ја олеснува комуникацијата меѓу АЗЛП и контролорите.

Ваквата улога на „олеснувачи“ е дадена и во воведот од Насоките на РГ29. Имено, преку дејствување како контакт точка, офицерите го олеснуваат пристапот на надзорниот орган до документи и информации за исполнување на задачите наведени во член 65 од ЗЗЛП, како и за извршување на истражните и корективните овластувања, давањето одобренија и мислења според член 66 од ЗЗЛП.

Како што веќе беше споменато, офицерите за заштита на личните податоци се обврзани на тајност и доверливост при извршување на нивните задачи, во согласност со законот (член 42, став (5) од ЗЗЛП).

Сепак, обврската за тајност и доверливост не ги спречува офицерите да го контактираат и да побараат совет од надзорниот орган. Имено, член 43, став (1) точка (г) од ЗЗЛП, пропишува дека офицерот за заштита на личните податоци може да го консултира надзорниот орган за сите прашања, кога тоа е соодветно.

2.10. Технички и организациски мерки за безбедност на личните податоци

За целите на исполнување на обврската од ЗЗЛП и Правилникот за безбедност на обработката на лични податоци, контролорите донесуваат документација и применуваат технички и организациски мерки за безбедност и доверливост на обработката на лични податоци од случајно или неовластено пристапување, менување, откривање, загуба и уништување на податоците.

Една од примарните задачи на офицерот за заштита на лични податоци е да ја следи усогласеноста на контролорот со оваа документација.

Според член 28, став (1) од ЗЗЛП, земајќи ги предвид природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозност за правата и слободите на физичките лица, контролорите применуваат соодветни технички и организациски мерки за да обезбедат и да бидат во можност да докажат дека обработката се врши во согласност со законот. По потреба, техничките и организациските мерки се предмет на ревизија и ажурирање.

Според член 36, став (1) од ЗЗЛП, земајќи ги предвид најновите технолошки достигнувања, трошоците за спроведување, природата, обемот, контекстот и целите на обработката, како и ризиците до различен степен на веројатност и сериозност за правата и слободите на физичките лица, контролорите и обработувачите применуваат соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот, вклучително и:
(а) псевдонимизација и криптирање на личните податоци;
(б) способност за обезбедување континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка;

Овој проект е финансиран од Европската Унија

(в) способност за навремено, повторно воспоставување на достапноста на личните податоци и пристапот до нив во случај на физички или технички инцидент;
(г) процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки за да се обезбеди безбедност на обработката.

КАКО ДА СЕ УТВРДИ КОИ ТЕХНИЧКИ И ОРГАНИЗАЦИСКИ МЕРКИ СЕ СООДВЕТНИ ЗА КОНТРОЛОРОТ?

Чекор 1: Опишете ги активностите за обработка на лични податоци
Каков вид на лични податоци се обработуваат? Кој, кога и за која цел? Какви системи се користат за обработка на личните податоци?

Чекор 2: Проверете ги правните основи за обработката на лични податоци
Дали личните податоци се собираат и обработуваат на законит начин? Дали личните податоци се евидентираат за конкретна цел и дали се следат насоките за обработка на лични податоци?

Чекор 3: Утврдете кои деловни процеси налагаат поголема безбедност
Кои услуги, системи, простории и податоци треба да бидат заштитени? Како тие се поврзани едни со други?

Чекор 4: Анализирајте ги потенцијалните ризици
Идентификување на ризиците: Дали безбедноста на личните податоци е подложна на ризици како што се природни катастрофи, нејасно дефинирани одговорности во рамки на организацијата, или потенцијални технички проблеми?
Проценка на можните последици: Колкава е сериозноста на последиците во случај на инцидент? Дали сценариото за најлош случај влијае врз податоците кои треба посебно да бидат заштитени, на пример, податоци за здравјето или детали од досието на вработено лице?
Проценка на веројатноста: Колкава е веројатноста да се случи некој инцидент? Какво искуство има организацијата коешто може да ја олесни проценката на сериозноста на штетата од таков настан? Какви информации треба да се земат предвид за да се утврди можната штета?

Овој проект е финансиран од Европската Унија

Утврдување на степенот на ризик: Кои ризици подразбираат висок степен на сериозност и висок степен на веројатност? Кои ризици би предизвикале помала штета и за кои ризици постои помала веројатност да се појават?

Чекор 5: Изберете ги соодветните технички и организациски мерки
Кои ризици треба прво да се решаваат поради високиот степен на сериозност и веројатност? Земајќи ги предвид најновите технолошки достигнувања, кои конкретни мерки треба да се разгледаат за минимизирање на овие ризици? Кои мерки можат да се спроведат во разумен обем (претставуваат рационален трошок, на пример)?

Пример: Ако некој јавен орган иницијално собира високо осетливи лични податоци во хартиена форма, може да се претпостави дека таквата практика подразбира висок ризик. Бидејќи оваа организација е отворена за јавноста, пополнетите формулари може да завршат во погрешни раце. Во таков случај, потенцијалните мерки што треба да се применат вклучуваат:
- набавка на машина за уништување на хартиени документи -шредер (техничка мерка) и
- спроведување на соодветни работни инструкции за уништување на хартиени документи (организациска мерка).

Кога се комбинираат заедно, овие мерки нудат висока заштита со релативно мал трошок

Чекор 6: Оценете го преостанатиот ризик
Кои ризици не можат да бидат целосно елиминирани со примена на технички и организациски мерки? Колкав е степенот на сериозност и веројатност на преостанатите ризици?

Чекор 7: Консолидирајте ги мерките
Дали треба да се комбинираат различни мерки или поединечните мерки се доволни? Дали мерките се соодветни на посебните околности во вашата организација?

Чекор 8: Спроведете ги избраните мерки
Кои мерки треба прво да ги примените?. Кој ќе преземе одговорност за нивното спроведување?. Дали спроведувањето на мерките довело до посакуваниот резултат?

Овој проект е финансиран од Европската Унија

2.11. Приод што се базира на ризик

Согласно прописите, при извршување на задачите, офицерите за заштита на личните податоци треба да ги земат предвид ризиците поврзани со операциите за обработка, како и природата, обемот и целите на обработката на лични податоци. Тоа значи дека офицерот става приоритет и се фокусира на прашања кои претставуваат повисок ризик по заштитата на личните податоци. Според овој прагматичен приод, офицерите утврдуваат кои области се предмет треба да бидат предмет на внатрешна или надворешна ревизија/контрола/проверка, каква обука треба да се организира за вработените и на кои операции за обработка вработените треба да посветат поголемо внимание.

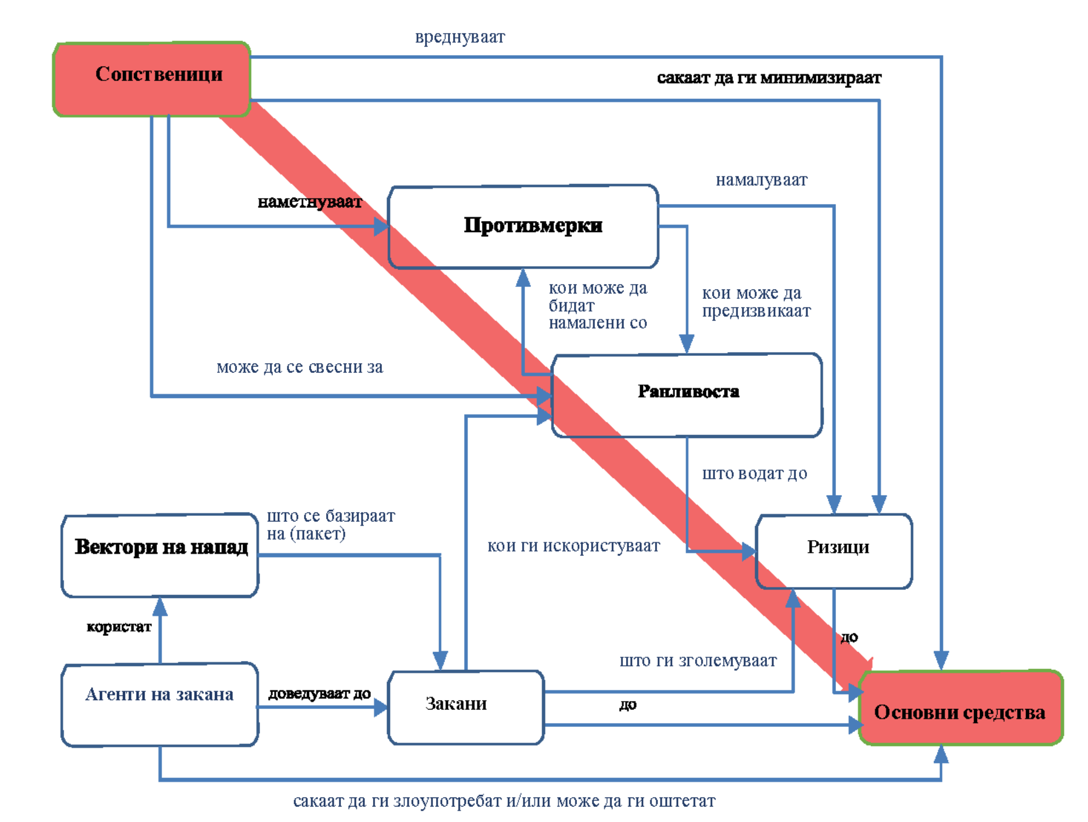
Согласно Правилникот за безбедност на обработката на лични податоци, при идентификување и оценување на ризиците (управување со ризици), контролорите ги земаат предвид ризиците кои се поврзани со обработката на лични податоци, особено од случајно или незаконско уништување, губење, менување, неовластено откривање или неовластен пристап до податоците кои се пренесени, се чуваат или на друг начин се обработуваат.

Контролорите се одговорни за усогласеноста на нивото на мерки за безбедност на обработката кои ги применуваат во согласност со член 8 од Правилникот, при што треба да обезбедат соодветно ниво на безбедност на личните податоци, вклучително и заштита од неовластена или незаконска обработка на личните, како и заштита од нивно случајно губење, уништување или оштетување.

Сепак, при извршување на нивните задачи и врз основа на природата, обемот, контекстот и целите на обработката, офицерите за заштита на личните податоци треба да ги земат предвид ризиците кои се поврзани со операциите за обработка на лични податоци. Исполнувањето на овие услови налага утврдување на релевантните ризици. Тоа треба да се направи преку изготвување на инвентар на операциите за обработка на лични податоци и создавање регистер на таквите операции, како и спроведување редовна проверка на таквите операции.

Потоа, елементите на ризик и нивните односи може да бидат илустрирани во дијаграм како оној даден подолу:

Овој проект е финансиран од Европската Унија



Соодветна проценка на ризиците се спроведува во четири чекори:

1. Дефинирање на операциите за обработка и нивниот контекст.
2. Разбирање и евалуација на влијанието.
3. Дефинирање на можните закани и евалуација на нивната веројатност (можност за појава на заканата).
4. Евалуација на ризикот (комбинирање на веројатноста за појава на заканата и влијанието од истата).

ДЕЛ 3: АЛАТКИ ЗА ЗАЈАКНУВАЊЕ НА ПОЗИЦИЈАТА НА ОФИЦЕРИТЕ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

За да се зајакне и да се подобри ефикасноста на работата што ја извршуваат офицерите за заштита на личните податоци и да се интензивира соработката со АЗЛП, како и да се воспостават нови форми на соработка меѓу офицерите, потребна е изработка на пакет алатки, како што следува.

3.1. Пакет водичи

Овој Водич е изработен како дел од твининг-проектот „Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“, финансиран од Европската Унија. Тој служи како алатка за ефикасно извршување на задачите на офицерите за заштита на личните податоци и вклучува информации за новитетите кои се воведени со законодавство. Конкретно, Водичот е наменет за подобро разбирање на нивната функција и за новата позиција на контролорите, и нуди објаснувања за полесно спроведување на обврските. Пакетот корисни алатки изработени како дел од проектот вклучува поголем број водичи, информатори и слични документи на различни теми од полето на заштита на личните податоци, како што се: правата на субјектите на лични податоци; начела за заштита на личните податоци; концепт на контролор, обработувач и заеднички контролор; проценка на влијанието врз заштитат на личните податоци, пренос на податоци во трети земји и меѓународни организации, итн. достапни на веб страницата на АЗЛП.

3.2. Катче за офицери

Досега, соработката со АЗЛП е насочена кон давање совети на контролорите да ги подобрат нивните сегашни операции и да развиваат најдобри практики на конкретни теми. За интензивирање на оваа соработка, на официјалната веб-страница на АЗЛП треба да се воспостави катче за офицери како нова форма на соработка. Пристапот до овој дел од веб-страницата ќе биде ограничен само на Агенцијата и офицерите.

Овој проект е финансиран од Европската Унија

Ефикасни офицери се само оние кои се добро информирани за прописите за заштита на личните податоци и се во тек со напредокот во оваа област. Катчето ќе служи како платформа за размена на знаења и искуства и за поддршка во спроведувањето на нивните задачи. Поконкретно, офицерите ќе имаат пристап до ажурирани документи кои се фокусираат на нивната улога и задачи. Документите ќе бидат дизајнирани на начин кој дозволува јасен преглед и брзо разбирање. Истовремено, катчето ќе нуди поддршка во спроведувањето на нивните задачи, како што се формулари, обрасци и презентации кои ќе им помогнат да ја зајакнат свеста на вработените кај контролорот или обработувачот каде работи офицерот.

Дополнително, катчето за офицери ќе вклучи дел каде ќе се објавуваат тековни настани (конференции, семинари, обуки и состаноци) кои може да ги посетуваат за да ги надградат своите знаења и вештини, како и други алатки кои се потребни во нивната секојдневна работа.

3.3. Мрежа на офицери

За целите на соработка и размена на искуства меѓу офицерите за заштита на личните податоци треба да се создаде и мрежа на офицери. Со оглед на важноста на интеракцијата со колегите, а особено важноста на споделувањето најдобри практики и практични совети, мрежата е корисна алатка за подобро информирање и ефикасна работа на офицерите.

Мрежата на офицери може да биде посебен дел од катчето за офицери каде тие ќе бидат во можност да ги идентификуваат своите колеги. Таа треба да се дизајнира на начин кој овозможува лесна соработка генерално, но и на ниво на посебни сектори. Оваа мрежа може да биде корисна за давање совети и размена на ставови за вообичаени прашања и проблеми.

Пожелно е во рамките на мрежата да се формираат посебни групи на ниво на сектори за полесна соработка и размена на искуства.

3.4. е-Форуми

Се препорачува креирање веб-алатка за организирање е-форуми кои ќе овозможат комуникација меѓу офицерите преку искористување на најновите достапни технологии.

3.5. Здружение на офицери

Уште една форма на соработка и размена на знаење и искуства е формирање здружение на офицери за заштита на личните податоци, се разбира, на нивна иницијатива.

3.6. Нова програма за обуката на офицери

За да се зајакне позицијата на офицерите, потребно е да се изработи нова програма за обука и нови материјали врз основа на новиот закон кои ќе ги користат членовите на комисијата за обука во АЗЛП. Материјалите треба да бидат достапни во хартиена и електронска форма, и истите треба да вклучуваат практични чекори за исполнување на обврските од новото законодавство.

Пожелно е обуките да се организираат на ниво на сектори, што ќе ја олесни имплементацијата на новиот Закон за заштита на личните податоци.

3.7. Стратегија за комуникација

Стратегија за комуникација е вредна алатка која го поддржува спроведувањето новото законодавство. Еден дел од стратегијата за комуникација треба да се однесува на новата улога на офицерите за заштита на личните податоци. Освен тоа, овој документ треба да предвиди организирање јавни настани и кампањи за подигнување на свеста и промоција на позицијата на офицерот.

Овој проект е финансиран од Европската Унија

3.8. Денови на свест за улогата на офицерите

Се препорачува организирање денови на свест за улогата на офицерите за заштита на личните податоци како алатка за подигање на свеста и за промоција на новата улога на офицерите. На овој настан треба да се поканат раководителите на јавните органи и управителите на приватни компании за да се запознаат со профилот, позицијата и задачите на офицерите, како и условите и околностите во кои тие ги извршуваат своите задачи. Ваквите настани треба да бидат организирани на редовна основа.

Овој проект е финансиран од Европската Унија

Оваа публикација е изработена како дел од твининг-проектот „Поддршка во спроведувањето на модернизираната правна рамка за заштита на личните податоци“, финансиран од Европската Унија. Содржината на публикацијата е единствена одговорност на авторите и на проектните партнери, и не може да се смета дека ги одразува ставовите на Европската Унија.

Побарајте повеќе информации на
www.azlp.mk

SCAN ME

Овој проект е финансиран од Европската Унија