

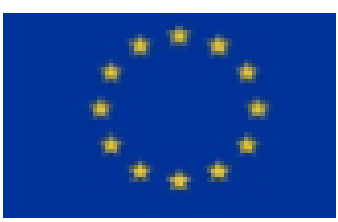
ЕУ твининг проект „Поддршка во спроведувањето на модернизираниот правна рамка за заштита на личните податоци“

ВОДИЧ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ФИНАНСИСКИОТ СЕКТОР



Овој проект е финансиран од Европската Унија





СОДРЖИНА

ВОВЕД **3**

1. МАТЕРИЈАЛНА ПРИМЕНА НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ **4**

2. ПРЕЦИЗНА И ДЕТАЛНА ДЕФИНИЦИЈА НА „ЛИЧЕН ПОДАТОК“ **4**

3. КЛУЧНИ НАЧЕЛА НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ **5**

3.1 ЗАКОНИТОСТ, ПРАВИЧНОСТ И ТРАНСПАРЕНТНОСТ **5**

3.2. ОГРАНИЧУВАЊЕ НА ЦЕЛТА **5**

3.3 МИНИМАЛЕН ОБЕМ НА ПОДАТОЦИ **5**

3.4 ТОЧНОСТ НА ПОДАТОЦИТЕ **5**

3.5 ОГРАНИЧУВАЊЕ НА РОКОТ ЗА ЧУВАЊЕ **5**

3.6 БЕЗБЕДНОСТ **6**

3.7 ОТЧЕТНОСТ **6**

4. ЗАКОНИТОСТ НА ОБРАБОТКАТА НА ЛИЧНИ ПОДАТОЦИ **6**

5. ПРАВА НА СУБЈЕКТИТЕ НА ЛИЧНИ ПОДАТОЦИ **8**

6. ТЕХНИЧКА И ИНТЕГРИРАНА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ **8**

7. ОБРАБОТУВАЧ НА ЗБИРКА НА ЛИЧНИ ПОДАТОЦИ **9**

8. ЕВИДЕНЦИЈА ЗА АКТИВНОСТИТЕ ЗА ОБРАБОТКА **10**

9. БЕЗБЕДНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ **11**

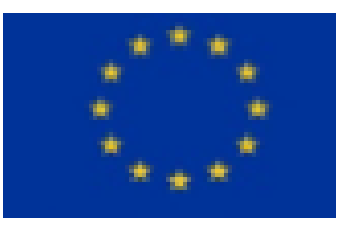
9.1 ИЗВЕСТУВАЊЕ ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ **12**

**10. ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ И
ПРЕТХОДНИ КОНСУЛТАЦИИ **13****

11. ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ **15**

**12. ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ ВОН ТЕРИТОРИЈАТА НА РЕПУБЛИКА СЕВЕРНА
МАКЕДОНИЈА **16****





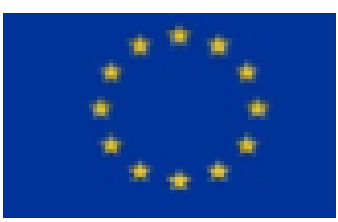
ВОВЕД:

Финансиската индустрија минува низ темелна трансформација поради брзиот технолошки развој и глобализацијата. Овие развојни моменти донесоа и нов предизвик за финансиските институции во форма на донесување нови мерки за хармонизација на националното законодавство во Република Северна Македонија во однос на обработката на личните податоци на физички лица.

Иако некои од основните начела од стариот режим за заштита на личните податоци сè уште се применуваат, новиот Закон за заштита на личните податоци вовеле и неколку нови концепти кои може да имаат значително влијание врз финансискиот сектор и да наложат промени во начинот на кој овие институции ги користат и ги обработуваат личните податоци.

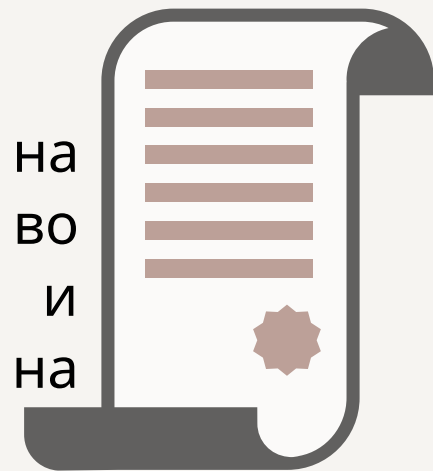
Целта на овој Водич е да обезбеди поддршка на контролорите и обработувачите од финансискиот сектор и да ја зголеми свеста за клучните елементи поврзани со обработката на лични податоци од страна на компаниите кои работат во овој сектор.





1. МАТЕРИЈАЛНА ПРИМЕНА НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Со влегувањето во сила на новиот Закон за заштита на личните податоци („Службен весник на РСМ“ бр. 42/20, натаму во текстот: ЗЗЛП) се модернизира постојниот правен режим во Република Северна Македонија за да се земат предвид новите развојни моменти и предизвици во областа на заштита на личните податоци. Освен натамошно зајакнување на постојните законски одредби, новото законодавство воведува и одредени новини.



Од аспект на територијалниот опфат од член 3, Законот за заштита на личните податоци се применува на обработката на лични податоци од страна на контролори или обработувачи основани на територијата на Република Северна Македонија, без оглед на местото каде се врши обработката. Исто така, одредбите од ЗЗЛП се применуваат и на обработка на лични податоци од страна на контролори кои не е основани во Република Северна Македонија, но се основани на место каде се применува правото на РСМ според меѓународните договори ратификувани во согласност со Уставот на Република Северна Македонија.

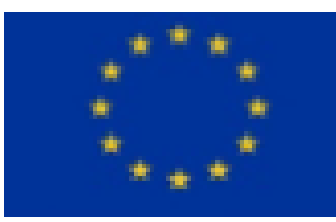
Кога личните податоци се пренесуваат од Република Северна Македонија на контролори или обработувачи во трети земји или меѓународни организации, нивото на заштита на субјектите на лични податоци што го гарантира националниот закон не смее да се потцени, при што таквиот пренос може да се изврши само доколку е целосно усогласен со ЗЗЛП.

2. ПРЕЦИЗНА И ДЕТАЛНА ДЕФИНИЦИЈА НА „ЛИЧЕН ПОДАТОК“

За целите на новиот закон, член 4 содржи нови дефиниции кои се од суштинско значење за неговото спроведување. Меѓу другото, ЗЗЛП воведува прецизна и детална дефиниција за личен податок која треба да обезбеди колку што е можно поширока заштита за субјектите на лични податоци и која може да биде важна за тековните и идните активности на институциите од финансискиот сектор што подразбираат обработка на лични податоци.

Конкретно, личен податок е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, директно или индиректно, врз основа на идентификатори како што се: име/презиме, матичен број, податоци за локација, идентификатор преку мрежите за електронски комуникации, или преку едно или повеќе обележја специфични за физичкиот, физиолошкиот, генетскиот, менталниот, економскиот, културниот или социјалниот идентитет на лицето.





3. КЛУЧНИ НАЧЕЛА НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ



Клучните начела дадени во член 9 од ЗЗЛП претставуваат почетна точка за секоја обработка на лични податоци.

Начелата кои се однесуваат на обработка на лични податоци и се утврдени со ЗЗЛП ги вклучуваат следниве:

3.1 Законитост, правичност и транспарентност

Согласно ЗЗЛП, постојат шест правни основи за обработка на лични податоци дадени во член 10. Пред да почнат со активности кои подразбираат обработка на лични податоци, контролорите мора да одвојат време за да утврдат кој е соодветниот правен основ за предвидената обработка.

Освен законска, ЗЗЛП налага и правична обработка на лични податоци. Ова начело главно се однесува на односот меѓу контролорот и субјектите на лични податоци. Во суштина, контролорите треба да ги известат субјектите на лични податоци и општата јавност дека тие ќе обработуваат лични податоци, и мора да бидат во можност да демонстрираат усогласеност на операциите за обработка со ЗЗЛП. Операциите за обработка не смее да се одвиваат тајно и субјектите на лични податоци треба да бидат свесни за потенцијалните ризици.

Пред обработката, контролорите мора да ги информираат субјектите на лични податоци за целите на обработката и адресата на контролорот. Информациите за операциите за обработка на лични податоци мора да се обезбедат на јасен и едноставен јазик за да им се овозможи на субјектите лесно да ги разберат правилата, ризиците, безбедносните мерки, и нивните права.

3.2 Ограничување на целта

Ова начело налага секоја обработка на лични податоци да биде направена за конкретна цел која е дефинирана пред почетокот на самата обработка, при што каква било дополнителна обработка за други цели мора да биде компатибилна со оригиналната цел. Секоја нова цел за обработка на лични податоци којашто не е компатибилна со оригиналната цел треба да се заснова на засебен правен основ.

3.3 Минимален обем на податоци

Обработката на лични податоци мора да биде ограничена на она што е неопходно за исполнување на конкретната цел. Категориите на лични податоци кои се избрани за обработка мора да бидат неопходни за постигнување на севкупната цел на операциите за обработка.

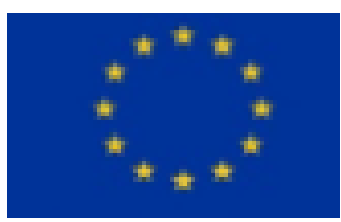
3.4 Точност на податоците

Контролорите не смеат да обработуваат лични податоци доколку не преземале разумни чекори за се осигурат дека личните податоци се точни и ажурирани.

3.5 Ограничување на рокот за чување

Личните податоци мора да се избришат или анонимизираат (при што законско чување на податоци кои повеќе не се потребни може да се постигне со нивно чување во форма која не дозволува идентификување на субјектите на лични податоци) веднаш штом тие веќе не се потребни за целите за кои биле собрани.





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

Генерално, контролорите треба да утврдат временски рокови за бришење на личните податоци и, дополнително, секој контролор треба да врши периодични контроли за да се осигури дека податоците не се чуваат подолго од она што е неопходно.

Имајќи превид дека многу активности на институциите од финансискиот сектор во својство на контролори се во согласност со Законот за заштита на личните податоци, посебните секторски прописи вклучуваат и одредби за временски рокови поврзани со обврската за чување на личните податоци. Во таа смисла, на пример, член 51 од Законот за спречување перење пари и финансирање тероризам („Службен весник“ бр. 120/2018, 275/2019 и 317/2020) пропишува дека институциите се обврзани да ги чуваат личните податоци на нивните клиенти за период од десет години.

3.6 Безбедност

Начелото за безбедност на личните податоци налага, во зависност од конкретните околности на секој случај посебно, примена на технички и организациски мерки при обработка на лични податоци со цел истите да бидат заштитени од случајно, неовластено или незаконско пристапување, користење, изменување, откривање, губење, оштетување или уништување.

Клиентите ја вреднуваат својата приватност и се загрижени за начинот на кој нивните лични податоци се заштитени во контекст на современите технологии.

3.7 Отчетност

Имајќи предвид дека и финансиските институции се предмет на споредливи обврски во рамките на различни регулаторни режими, отчетноста е ново начело што го воведува новата законска рамка и, во суштина, тоа воспоставува обврска за контролорите да применуваат мерки кои ги исполнуваат горенаведените начела.

4. ЗАКОНИТОСТ НА ОБРАБОТКАТА НА ЛИЧНИ ПОДАТОЦИ

Добро дефинирана и утврдена цел на обработката на личните податоци пред контролорот да почне со активностите за обработка е камен-темелникот на режимот за заштита на личните податоци.

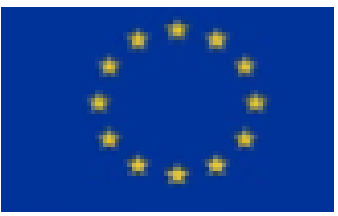
Постои широк спектар на цели за кои финансиските институции може да обработуваат податоци, од „основни“ цели кои се карактеристични за други видови на институции, како што е обработка на лични податоци за целите на работни односи/вработување, до цели кои се однесуваат на обезбедување услуги за клиенти или конкретни цели кои се во согласност со барањата што произлегуваат од националните закони.

Како што е наведено во Водичот за законска обработка на лични податоци, член 10 од ЗЗЛП пропишува шест правни основни.

Генерално, согласноста којашто финансиските институции ја користеа до влегувањето во сила на новиот закон може да биде соодветен правен основ за обработка на лични податоци само доколку се исполнети условите од член 11 од ЗЗЛП. Законот дава и дефиниција за согласност како слободно дадена, конкретна, информирана и недвосмислено изразена волја на физичкото лице преку изјава или јасно потврдено дејствие со кое се дава согласност за обработка на неговите/нејзините лични податоци.

Важно е контролорите да ги ревидираат тековните работни активности и детално да ги евидентираат за да бидат сигурни дека изјавите за согласност ги исполнуваат стандардите од новиот Закон за заштита на личните податоци.





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

Член 10, став (1), алинеја б) од ЗЗЛП пропишува дека обработката на личните податоци е законита само доколку:

- обработката е потребна за исполнување на договор каде субјектот на лични податоци е договорна страна, или
- за преземање одредени чекори на барање на субјектот на лични податоци пред пристапување кон договорот.

Кога контролорите од финансискиот сектор го користат овој правен освен за нивната обработка, за да се задоволи условот на законитост договорите мора да бидат валидни во согласност со договорното право што се применува. На пример, кога договорот се склучува со деца, тоа подразбира обезбедување усогласеност со националните закони кои се однесуваат на правниот капацитет на децата во однос на склучување договори. Освен тоа, за да обезбеди усогласеност со начелата за правичност и законитост, контролорите треба да исполнат други законски услови што се однесуваат на конкретниот договор, на пример, услови поврзани со договори со потрошувачи или, конкретно, поврзани со договори за одобрување кредити на клиенти.

Треба да се забележи дека според член 10, став (1), алинеја б) од ЗЗЛП, важен елемент на една законска обработка е концептот на „неопходност“. За таа цел, на пример, обработка на лични податоци за целите на спречување измама веројатно ќе вклучува многу повеќе податоци од она што е неопходно за извршување на договор. Сепак, ваквата обработка може да биде неопходна за финансиските институции да постигнат усогласеност со правната обврска од член 10, став (1), алинеја в) од ЗЗЛП.

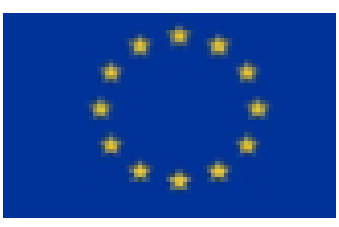
Во финансискиот сектор постојат одредени национални одредби што се однесуваат на обработката на лични податоци што ја вршат финансиските институции, и оттука таквиот вид на обработка треба да биде усогласен со правната обврска која е пропишана со закон што се применува на конкретниот контролор. Во таква ситуација, матичниот национален закон може да содржи конкретни одредби за прилагодување на примената на правилата од ЗЗЛП и општи услови кои се однесуваат на законитоста на обработката од страна на контролорот, како што се: утврдување на категориите на лични податоци кои се предмет на обработка, утврдување на засегнатите субјекти на лични податоци, утврдување на целите за кои личните податоци може да се откриваат на други страни, ограничување на целта на обработката, временски рокови за чување на податоците, итн.

Еден пример за горенаведеното е Законот за спречување на перење пари и финансирање тероризам („Службен весник на РСМ“ бр. 120/2018, 275/2019 и 317/2020) во врска со користењето податоци кои се добиени во согласност со тој закон.

Член 60

- (1) Податоците обезбедени врз основа на овој закон, вклучително и личните податоци, се користат единствено за откривање и спречување на перење пари и финансирање тероризам.
- (2) Доставувањето на податоците од став (1) на овој член до Управата за финансиско разузнавање и до соодветниот надзорен орган од член 146 од овој закон при вршење надзор согласно со овој закон не се смета за оддавање деловна тајна или откривање на класифицирани податоци и информации.
- (3) Вработените во субјектите и лицата кои управуваат со субјектите коишто имаат обврска за преземање мерки и дејствија за откривање и спречување на перење пари и финансирање тероризам согласно овој закон, не смеат да ги користат личните податоци од досиејата на клиентите за други цели освен за спроведување на мерките и дејствијата за откривање и спречување на перење пари и финансирање тероризам согласно целите предвидени со овој закон.





5. ПРАВА НА СУБЈЕКТИТЕ НА ЛИЧНИ ПОДАТОЦИ

Заштита на личните податоци не може да се обезбеди доколку не се почитуваат правата и начелата утврдени во законот. Сите права на субјектите на лични податоци и обврските на контролорите и обработувачите во однос на олеснување на остварувањето на правата на физички лица чиишто лични податоци се обработуваат ја даваат суштината на основното право за заштита на личните податоци и нивната примена мора да се смета за генерално правило.



Правата на субјектите на лични податоци се регулирани во Поглавје III од ЗЗЛП, при што акцентот е ставен на зголемување на транспарентноста кон субјектите на лични податоци и кон општата јавноста, што во крајна линија ја заканува нивната позиција.

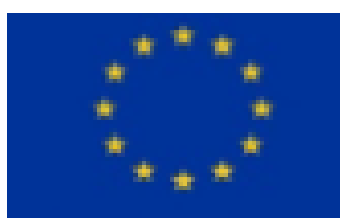
На пример, меѓу другото, субјектите на лични податоци имаат право на пристап, а не само право да добијат потврда дали нивните лични податоци се обработуваат, па така, на барање од субјектот, контролорот е обврзан да обезбеди копија од личните податоци за него/него без надомест.

За таа цел, кога се исполнети одредени околности, субјектите на лични податоци имаат право да ги добијат нивните лични податоци во структуриран, вообичаено користен, машински читлив формат, и имаат право да ги пренесат таквите податоци на друг контролор (преносливост на податоци).

Исто така, согласно ЗЗЛП, субјектите на лични податоци имаат право на бришење на нивните лични податоци. Се разбира, ова право не е апсолутно, а посебно не во оваа прилично регулирана област (каде што се применуваат одредби од посебни национални закони) при што финансиските институции нема да ги избришат личните податоци само по поднесено барање на субјектот поради обврската за усогласеност со правна обврска пропишана со закон.

Друг пример поврзан со бришење на лични податоци од страна на финансиски институции е случај кога тие обработуваат лични податоци на физичко пред за преземање чекори пред влегување во договор за одобрување заем. Во рамките на постапката за одобрување заем, финансиските институции ќе треба да обработуваат одредени податоци за да го оценат кредитниот ризик на апликантот, и доколку таквата оценка резултира во негативна одлука, односно заемот не е одобрен за физичкото лице, може да се каже дека во тој случај нема да се склучи договор со апликантот. Во таа смисла, апликантот не станува клиент и се смета дека целта на обработката на лични податоци е исполнета, поради што чувањето на таквите податоци не подлежи на обврските пропишани со посебните национални закони кои се однесуваат на чување лични податоци за клиентите.

За финансиските институции да бидат во можност да ги исполнат овие обврски, тие треба од самиот почеток да воведат правилни постапки (меѓу другото, и за обезбедување дека записите, односно личните податоци се точни и ажурирани) кои им овозможуваат да ги пребаруваат, да направат копија и да ги извлечат конкретните личните податоци што се однесуваат на засегнатиот субјект, или да ги избришат.



6. ТЕХНИЧКА И ИНТЕГРИРАНА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Според новата правна рамка за заштита на личните податоци, финансиските институции треба да ги проценат ризиците по правата и слободите на физичките лица од предвидената обработка на почетокот на секој нов проект кој подразбира обработка на лични податоци и при развивање на нови производи и услуги.

При спроведување на овие мерки контролорот треба да ги земе предвид најновата достапна технологија, трошокот за спроведување, природата, обемот и целите на обработката на лични податоци, како и ризиците и нивното влијание врз правата и слободите на субјектите на лични податоци.

Финансиските институции треба да спроведат соодветни технички и организациски мерки за да обезбедат дека за секоја конкретна цел, по правило, се обработуваат само оние лични податоци кои се потребни за истата.



7. ОБРАБОТУВАЧ НА ЗБИРКА НА ЛИЧНИ ПОДАТОЦИ

Концептите на контролор и обработувач имаат клучна улога во примената на ЗЗЛП бидејќи тие утврдуваат кој е одговорен за сообразноста со разните правила за заштита на личните податоци и како субјектите на лични податоци можат да ги остварат своите права во практика.

Според дефиницијата од законот, обработувач на збирка на лични податоци е физичко или правно лице, орган на државната управа, државен орган, агенција или друго тело кое врши обработка на лични податоци во име на контролор. За таа цел, постојат два основни услови за едно физичко или правно лице да се квалификува како обработувач: да биде засебен ентитет во однос на контролорот и да обработува лични податоци во име на контролорот.

Контролорот може да користи услуги само на обработувачи кои обезбедуваат доволно гаранции за примена на соодветни технички и организациски мерки со цел обработката да ги исполнува условите пропишани со ЗЗЛП. Елементите што треба да се земат предвид вклучуваат:

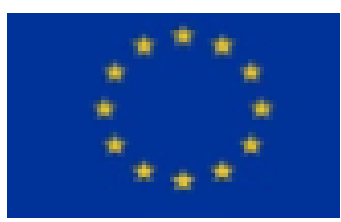
- стручно знаење на контролорот (на пр., техничка стручност во однос на безбедносни мерки и нарушување на безбедноста на личните податоци);
- веродостојност на обработувачот;
- ресурси и придржување до одобраниот кодекс за однесување или механизам за сертификација од страна на обработувачот.

Секоја обработка на лични податоци од страна на обработувачот мора да биде уредена со договор или друг правен акт во пишана и електронска форма, и со обврзувачки карактер. Контролорот и обработувачот може да изберат да преговараат за нивните меѓусебни договорни услови, вклучително и сите задолжителни елементи на таков договор, или можат да се потпрат, целосно или делумно, на стандардните договорни клаузули.

ЗЗЛП ги пропишува елементите кои треба да ги содржи договорот за обработка на лични податоци. Сепак, таквиот договор не смее само да ги препише одредбите од законот. Напротив, тој треба да вклучи специфични и конкретни информации за тоа како ќе бидат исполнети условите и кое ниво на безбедност е потребно за обработката на лични податоци што е предмет на договорот.

Обврската за користење услуги само од обработувачи кои „обезбедуваат доволно гаранции“, онака како што се дадени во член 32 од ЗЗЛП, е постојана обврска и затоа контролорот треба да ги провери гаранциите на обработувачот во соодветни интервали, вклучително и преку контроли и проверки, кога тоа е соодветно.





8. ЕВИДЕНЦИЈА ЗА АКТИВНОСТИТЕ ЗА ОБРАБОТКА

ЗЗЛП пропишува обврска за постење пишана документација и преглед на постапките за обработка на лични податоци. Записите за активностите за обработка мора да вклучат важни информации за обработката на лични податоци, вклучително и категориите на лични податоци, групата на субјекти на лични податоци, целта на обработката и корисниците на личните податоци. На барање, оваа евиденција мора да ѝ биде ставена на располагање на АЗЛП.

Согласно член 32, став (2) од ЗЗЛП, обврската за водење евиденција за активностите за обработка не се однесува само на контролорот и неговите претставници, туку и на обработувачот и неговите претставници.

Секој контролор е одговорен да води евиденција за сите активности за обработка кои се одвиваат во организацијата. Овие евиденции (кои треба да бидат во пишана и електронска форма) мора да ги содржат следниве информации:



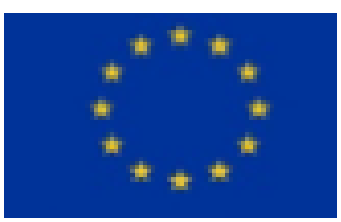
- име и контакт детали на контролорот и на офицерот за заштита на личните податоци, кога е применливо;
- цели на обработката;
- опис на категориите на субјектите на лични податоци и категориите на лични податоци;
- категории на корисници на личните податоци на кои им биле или ќе им бидат откриени личните податоци, вклучително и корисници во трети земји или меѓународни организации;
- пренос на лични податоци во трета земја или меѓународна организација, вклучително и документација за примена на соодветни безбедносни мерки;
- предвидени временски рокови за бришење на различни категории на лични податоци; и
- генерален опис на применетите технички и организациски мерки.

Исто така, секој обработувач е одговорен да води евиденција за сите категории на активности за обработка што ги врши во име на контролорот со следниве информации:

- име и контакт детали на обработувачот/обработувачите и секој контролор во чиешто име дејствува обработувачот и на офицерот за заштита на личните податоци, кога тоа е применливо;
- категории на лични податоци што се обработуваат во име на секој контролор;
- пренос на лични податоци во трета земја или меѓународна организација, вклучително и документација за примена на соодветни безбедносни мерки;
- генерален опис на применетите технички и организациски мерки.

Финансиските институции со помалку од 50 вработени се исклучени од обврската за водење евиденција, освен доколку е веројатно дека обработката што ја вршат претставува ризик по правата и слободите на субјектите на лични податоци, доколку обработуваат посебни категории на лични податоци и доколку обработката не се врши само повремено. Во практика, овој исклучок ретко може да се примени. Освен тешкотиите што се јавуваат во однос на толкувањето што се подразбира „само повремено“, во случајот на голем број финансиски институции неоспорно е дека тие редовно обработуваат лични податоци, вклучително и обработка на лични податоци за нивните веб-страници, за електронско банкарство, итн., дури и со примена на широко толкување за терминот податоци. Мора да се забележи дека обврската за документирање и, следствено на тоа, евиденцијата за активностите за обработка ќе биде во фокусот на супервизијата што ја спроведува АЗЛП.



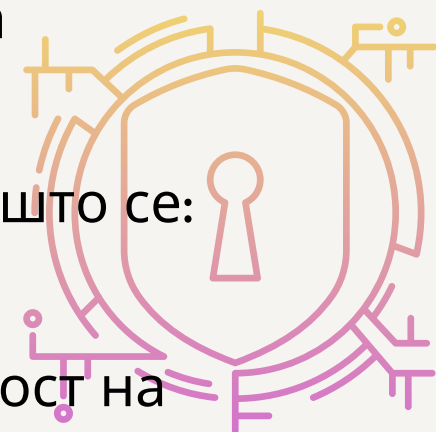


9. БЕЗБЕДНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ

Примената на соодветни технички и организациски мерки за да се обезбеди одредено ниво на безбедност наспроти ризикот има клучна улога во постигнувањето усогласеност од страна на институциите во финансискиот сектор.

Член 36 од ЗЗЛП пропишува некои од мерките што може да ги применат контролорите, како што се:

- (а) псевдонимизација и криптирање на личните податоци;
- (б) способност за обезбедување континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка;
- (в) способност за навремено, повторно воспоставување на достапноста на личните податоци и пристапот до нив во случај на физички или технички инцидент;
- (г) процесот на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки за да се гарантира безбедност на обработката.



Согласно член 66, став (6) од ЗЗЛП, АЗЛП има донесено и објавено Правилник за безбедност на обработката на лични податоци кој дава насоки за активности што контролорите треба да ги преземат во однос на спроведување технички и организациски мерки за безбедност на личните податоци.

Освен тоа, безбедноста на обработката на лични податоци е дополнително нагласена преку обврската на контролорите и обработувачите да ги пријават инцидентите (нарушувањата на безбедноста на личните податоци) до АЗЛП, а во некои случаи и до субјектите на лични податоци (член 37 и 38 од ЗЗЛП).

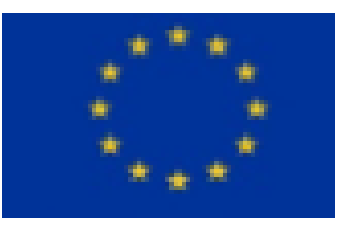
Според ЗЗЛП и согласно добропознатите начела за информатичка безбедност, нарушувањата на безбедноста на личните податоци може да се групираат во следниве категории: „нарушување на доверливоста“ – неовластено или случајно откривање или пристапување до лични податоци; „нарушување на интегритетот“ – неовластено или случајно менување на лични податоци; „нарушување на достапноста“ – случајно или неовластено губење на пристап до или уништување на личните податоци.

Може да се каже учесниците од финансискиот сектор обработуваат огромни количини на податоци кои може да се сметаат за осетливи податоци (бидејќи прекршувањето поврзано со овие податоци има сериозно влијание врз секојдневниот живот на засегнатиот субјект на лични податоци, на пример, финансиски податоци кои може да се користат за измамничко плаќање), што пак го зголемува потенцијалниот ризик.

Имајќи предвид дека основата на Законот за заштита на личните податоци претставува приод што се базира на ризик, институциите од финансиската индустрија треба да спроведуваат периодични проценки на ризикот, да развиваат внатрешни политики и постапки за ефективно следење, реагирање и ублажување на последиците од потенцијални безбедносни инциденти. Една од најважните обврски на контролорите е проценка на ризиците по правата и слободите на субјектите на лични податоци и преземање соодветни технички и организациски мерки за решавање на истите.

Обука и градење свест за прашањата поврзани со заштитата на личните податоци кај персоналот на контролорот со фокус на управување со нарушувањето на безбедноста на личните податоци се од суштинско значење за контролорите во рамките на нивните активности поврзани со мерки за обезбедување соодветно ниво на безбедност.



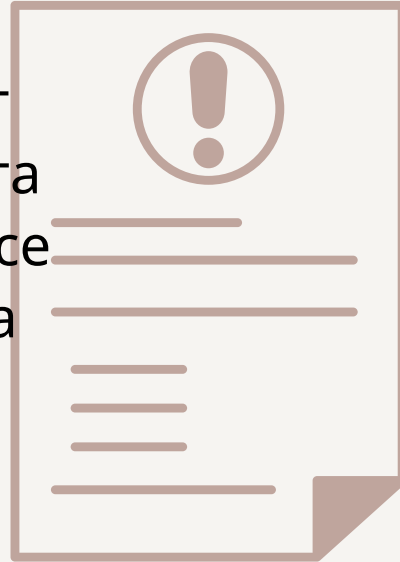


9.1. ИЗВЕСТУВАЊЕ ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

ЗЗЛП воведува обврска според која нарушувањата на безбедноста на личните податоци треба да бидат пријавени во АЗЛП (член 37) и, во некои случаи, за нарушувањата треба да се информираат лицата чишто лично податоци се засегнато со таквото нарушување (член 38).

Новата обврска за известување носи голем број придобивки. Преку известување на Агенцијата, контролорите може да добијат совети за тоа дали засегнатите субјекти на лични податоци треба да бидат информирани или пак може да добијат наредба да ги информираат лицата за нарушувањето. Информирањето на физичките лица за нарушување на безбедноста на личните податоци им дозволува на контролорите да дадат информации за ризиците кои се резултат на таквото нарушување и за чекорите што засегнатите лица може да ги преземат за да се заштитат од потенцијални последици.

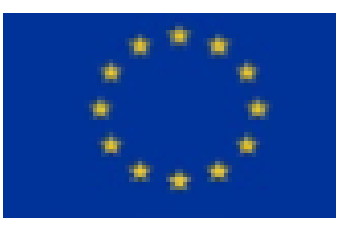
Во член 4, точка 12), законот го дефинира „нарушувањето на безбедноста на личните податоци“ како нарушување на безбедноста што доведува до случајно или незаконско уништување, менување, неовластено откривање или пристапување до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат.



Пример за губење на лични податоци вклучува губење или кражба на уред што содржи копија од базата на податоци со клиентите на контролорот

Примери за губење на достапноста на личните податоци вклучуваат случајно бришење или бришење на личните податоци од страна на неовластено лице, или пак губење на клучот за дешифрирање кога станува збор за криптирани податоци.

Законот налага и контролорите и обработувачите да применуваат соодветни технички и организациски мерки за да се обезбеди ниво на заштита кое е соодветно со ризикот по личните податоци што се обработуваат. Оттука, соодветни технички и организациски мерки треба веднаш да се пример без оглед на тоа дали се случило нарушување на безбедноста на личните податоци, што подоцна одредува дали се активира обврската за известување. Како резиме, клучен елемент на секоја политика за безбедност на личните податоци е способноста, кога тоа е можно, да се спречи нарушување и во случај на нарушување, важно е да се презема навремена реакција.



10. ПРОЦЕНКА НА ВЛИЈАНИЕТО ВРЗ ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРЕТХОДНИ КОНСУЛТАЦИИ



ЗЗЛП налага контролорите да спроведуваат соодветни мерки за да обезбедат и да бидат во можност да демонстрираат усогласеност со законот преку разгледување на, меѓу другото, ризици од различна веројатност и сериозност по правата и слободите на физичките лица (член 28, став (1) од ЗЗЛП).

Проценката на влијанието врз заштитата на личните податоци (ПВЗЛП) е процес кој е дизајниран да ја опише обработката, да ја оцени нејзината неопходност и пропорционалност, и да им помогне во управувањето со ризиците по правата и слободите на физичките лица во однос на обработката на лични податоци преку оценување и утврдување на мерки за нивно решавање.

ПВЗЛП е важна алатка од аспект на отчетноста бидејќи таа може да им помогне на контролорите не само да се усогласат со барањата од ЗЗЛП, туку и да демонстрираат дека се применети соодветни мерки.

Според приодот што се базира на ризик, спроведувањето на проценка на влијанието не е задолжителна за секоја операција за обработка што ја врши контролорот. Член 39, став (1) од ЗЗЛП пропишува дека таква проценка е потребна кога „постои веројатност дека обработка ќе резултира во висок ризик по правата и слободите на физичките лица“.

Таков вид на операции за обработка може да бидат операции кои подразбираат користење нови технологии или кои подразбираат операции за обемна обработка со цел да се обработи значителен волумен на лични податоци на регионално или на национално ниво, а кои може да влијаат врз голем број субјекти на лични податоци и за кои постои веројатност дека ќе резултираат во висок ризик, на пример, кога личните податоци се обработуваат за донесување одлуки за конкретни физички лица по некаков вид на систематска и екстензивна евалуација на личните особености на лицата во однос на исполнување на критериумите за кредитоспособност или условите што ги нуди кредиторот.

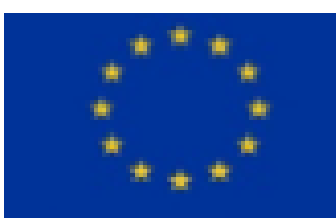
ЗЗЛП пропишува дека ПВЗЛП мора да се спроведе во следниве случаи:

(а) систематска и сеопфатна оценка на личните аспекти кои се поврзани со физички лица, којашто се заснова на автоматска обработка, вклучително и профилирање, а врз основа на која се донесуваат одлуки што произведуваат правно дејство во врска со физичкото лице или значително влијаат на физичкото лице;

(б) обемна обработка на посебните категории на лични податоци од член 13, став (1) од ЗЗЛП, или лични податоци поврзани со кривични осуди и кривични дела од член 14 од ЗЗЛП; или

(в) систематско набљудување на јавно достапни простори од голем размер.





Дополнително, треба да се забележи дека АЗЛП има донесено и објавено неколку документи во оваа област, односно:

Правилник за процесот на проценка на влијанието врз заштитата на личните податоци.

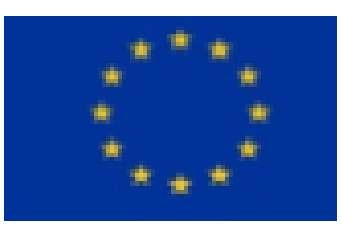
Листа на видови операции за обработка кои не налагаат проценка на влијанието врз заштитата на личните податоци.

Листа на видови операции за обработка кои налагаат проценка на влијанието врз заштитата на личните податоци.

Доколку контролорот, како дел од својата проценка, заклучил дека ризиците треба да се сметаат за доволно намалени, согласно одредбите од член 40, став (1) од ЗЗЛП, обработката може да продолжи без консултации со АЗЛП. Во случаите кога идентификуваните ризици не можат да бидат доволно ублажени од страна на контролорот и кога контролорот не може да најде доволно мерки за намалување на ризиците до прифатливо ниво, тогаш мора да се организираат консултации со АЗЛП.

Согласно одредбите од член 39, став (1) од ЗЗЛП, контролорот е тој кој спроведува проценка на влијанието врз заштитата на личните податоци. Сепак, офицерот за заштита на личните податоци може да има многу важна и корисна улога преку давање помош на контролорот. За таа цел, член 39, став (2) конкретно налага контролорот да побара совет од офицерот за заштита на личните податоци при спроведувањето на проценка на влијанието врз заштитата на личните податоци. Понатаму, член 43, став (1), алинеја в) од ЗЗЛП пропишува дека задачите на офицерот за заштита на личните податоци вклучува давање совети за проценка на влијанието и следење на спроведувањето на таквата проценка според член 39 од ЗЗЛП.





II. ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Според одредбите од член 41, став (1) од ЗЗЛП, одредени контролори и обработувачи се должни да определат офицер за заштита на личните податоци. Поконкретно, законот налага определување таков офицер во три конкретни случаи:

- а) обработката ја врши орган на државната управа, освен за судовите кога постапуваат во рамките на нивните надлежности, а кои определуваат офицер за друга обработка на личните податоци во согласност со законот;
- б) основните активности на контролорот или обработувачот се состојат од операции за обработка кои, поради својата природа, опсег и/или цели, во голема мера налагаат редовно и систематско следење на субјекти на лични податоци; или
- в) основните активности на контролорот или обработувачот се состојат од обемна обработка на посебни категории на лични податоци или лични податоци поврзани со кривични осуди и кривични дела од член 14 од ЗЗЛП.

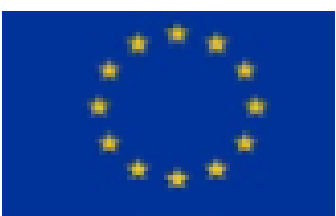
Во однос на финансиските институции, горенаведениот член 41, став (1), точка б) од ЗЗЛП упатува на основни активности на контролорот или обработувачот. Концептот „основни активности“ не треба да се толкува дека исклучува активности каде обработката на лични податоци е неразделив дел од дејноста на контролорот или на обработувачот. На пример, според член 2, точка (4) од Законот за банките („Службен весник на РМ“ бр. 67/2007, 90/2009, 67/2010, 26/2013, 15/2015, 153/2015, 190/2016, 7/2019, 101/2019 и 122/2021), „банкарски активности“ се прибирање на депозити и одобрување на кредити во свое име и за своја сметка; а според член 4, став (1), точки (1) и (2) од Законот за финансиските друштва („Службен весник на РМ“ бр. 158/2010, 169/2010, 53/2011, 112/2014, 153/2015 и 23/2016), едно финансиско друштво може да врши една или повеќе од следниве активности: одобрување кредити, и издавање и администрирање кредитни картички.

Имајќи предвид дека една банка или финансиска институција не може да ги извршува своите активности без обработка на личните податоци на клиентите, обработката на овие податоци треба да се смета како една од основните активности на банката или финансиската институција.

Понатаму, цитираните законски одредби налагаат обемна обработка на лични податоци, но не дефинираат што претставува „обемна обработка“. Иако не може да се даде прецизен број во однос на обемот на обработените податоци или број на лица кои се засегнати од конкретната ситуација, не се исклучува можноста за развивање стандардна практика со цел поточно да се одговори на прашањето за тоа што претставува „обемна обработка“ во однос на одредени видови на активности за обработка.

За таа цел, предвид треба д се земат следниве фактори: бројот на засегнати субјекти на лични податоци, обемот на податоци кои се обработуваат, времетраење на активноста за обработка, географскиот опфат на активноста за обработка. Оттука, на пример, обработката на податоците на клиентите како редовна деловна активност на една банка може да се смета за „обемна“ обработка.





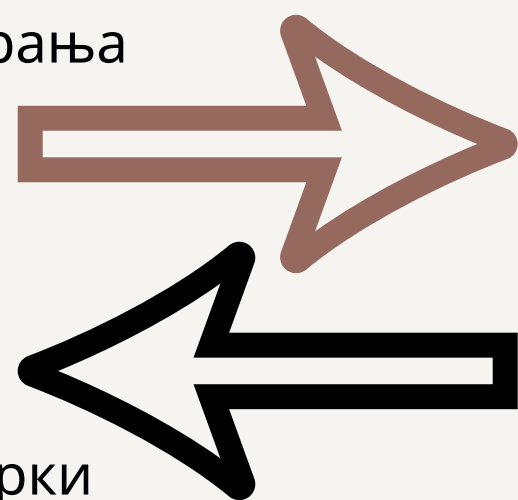
Кога станува збор за позицијата на офицерот за заштита на личните податоци, член 42 од ЗЗЛП пропишува дека контролорот и обработувачот обезбедуваат вклученост на офицерот, на соодветен и навремен начин, во сите прашања кои се однесуваат заштита на личните податоци преку обезбедување поддршка за извршување на неговите задачи од член 43 од ЗЗЛП. За таа цел, член 42, став (6) од ЗЗЛП пропишува дека офицерот за заштита на личните податоци може да врши и други задачи и должност надвор од оние специфицирани со овој закон, но контролорот или обработувачот е должен да обезбеди дека такви задачи и должности нема да доведат до судир на интереси, што е поврзано со барањето офицерот да дејствува независно. Со други зборови, офицерот не може да извршува позиција во рамките на организација која подразбира утврдување на целите и средствата за обработка на лични податоци. Такви позиции во рамките на организацијата може да бидат: главен финансиски директор, раководител на одделение за човечки ресурси или раководител на одделение за информатичка технологија.

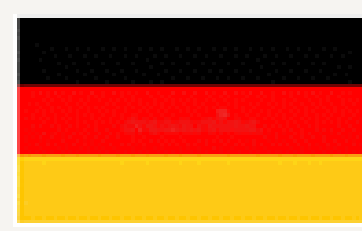
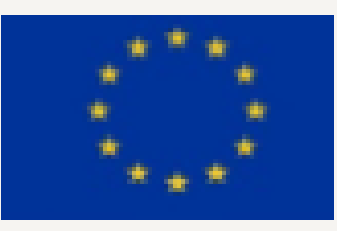
НА КРАЈ, ТРЕБА ДА СЕ НАГЛАСИ ДЕКА ОФИЦЕРИТЕ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ НЕ СЕ ЛИЧНО ОДГОВОРНИ ВО СЛУЧАЈ НА НЕУСОГЛАСЕНОСТ СО ЗЗЛП. ЗЗЛП ЈАСНО УПАТУВА НА ТОА ДЕКА КОНТРОЛОРОТ И ОБРАБОТУВАЧОТ СЕ ТИЕ КОИ ТРЕБА ДА ОБЕЗБЕДАТ И ДА БИДАТ ВО МОЖНОСТ ДА ДЕМОСТРИРААТ ДЕКА ОБРАБОТКАТА СЕ ВРШИ ВО СОГЛАСНО СО ОДРЕДБИТЕ ОД ЧЛЕН 28, СТАВ (1). ОТТУКА, УСОГЛАСЕНОСТА СО ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ Е ОДГОВОРНОСТ НА КОНТРОЛОРОТ ИЛИ ОБРАБОТУВАЧОТ.

12. ПРЕНОС НА ЛИЧНИ ПОДАТОЦИ ВОН ТЕРИТОРИЈАТА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Правната рамка за заштита на личните податоци во Република Северна Македонија ја признава важноста на зголемениот ризик по личните податоци во врска со пренос на податоците во трети земји или меѓународни организации и затоа содржи конкретни барања кои имаат за цел да понудат исто ниво на заштита и за податоците кои се пренесуваат надвор од територијата на Република Северна Македонија.

Дополнително на усогласеноста со условите пропишани во другите одредби од законот, субјектите што вршат пренос на лични податоци во трети земји или меѓународни организации мора да се осигурат, врз основа од-случај-до-случај, дека предвидените мерки за пренос на лични податоци во трети земји се јасно применливи и на инструментот за пренос.





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

Генерално, при примената на одредбите за пренос на лични податоци, контролорите и обработувачите треба да применат повеќеслоен приод, односно:

- прво, тие треба да разгледаат дали третата земја обезбедува соодветно ниво на заштита, односно дали Агенцијата за заштита на личните податоци (АЗЛП) има донесено одлука во согласност со одредбите од член 49 од ЗЗЛП дека конкретната трета земја или меѓународна организација обезбедува соодветно ниво на заштита;
- второ, доколку не постои одлука за соодветно ниво на заштита во конкретниот случај, субјектот што врши пренос на лични податоци треба да размисли за примена на соодветни безбедносни мерки и преносот да го врами во еден од механизмите дадени во член 50 од ЗЗЛП;
- само во отсуство на инструментите образложени во претходните ставки, контролорот или обработувачот може да се потпре на отстапувања дадени во член 53 од ЗЗЛП.

Кога зборуваме за видовите на отстапувања, треба да се забележи дека тие мора да се толкуваат внимателно, ограничено и само врз основа од-случај-до-случај. На пример, правниот основ „важен јавен интерес“ подразбира интерес кој е идентификуван како таков во националното законодавство што се однесува на контролорите воспоставени во Република Северна Македонија.

Во однос на финансиските услуги, одредени мерки им овозможуваат на контролорите да одат подалеку од нивните конкретни законски обврски при спроведувањето на законите за борба против незаконски активности, како што се перење пари или откривање измами. Доколку се смета дека тоа е важен јавен интерес според националните закони кои се применуваат за контролорот, тогаш ова отстапување може да се примени на преносот на лични податоци до надлежни органи во трети земји кога тоа е неопходно за вршење супервизија или, на пример, во случај на матична компанија или подружница лоцирана на нивната територија. Сепак, јавен интерес не може да се користи за оправдување на повторливи, преобемни или структурни преноси кои се однесуваат на предложен голем пренос на лични податоци до трети земји за целите на спречување перење пари.

Доколку ниту едно од отстапувањата не е применливо, тогаш субјектот што врши пренос на лични податоци мора да примени соодветни безбедносни мерки за да обезбеди дека субјектите на тие податоци се соодветно заштитени преку применлив и законски обврзувачки инструмент. Во случај на приватни субјекти, тоа обично има форма на пишан договор во кој се вградени стандардните договорни клаузули, задолжителни корпоративни правила или друг вид на ад-хок договор меѓу субјектот што врши пренос и субјектот што ги прима податоците во трета земја. За подетални информации во врска со преносот на лични податоци надвор од територијата на Република Северна Македонија и можните инструменти за пренос видете го Водичот за пренос на лични податоци во трети земји и меѓународни организации објавен на веб-страницата на АЗЛП.





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

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

