Информативна сесија со Агенција за заштита на лични податоци
14.06.2021

1. Дали треба да се поднесе барање за добивање на одобрение за обработка на лични податоци за здравје од страна на работодавачот кој обработува здравствени податоци за своите вработени од аспект на безбедност и здравје при работа (пример, податоци од систематски прегледи, повреди на работа и сл.)?

Согласно членот 13 став (2) точка 8 од Законот за заштита на лични податоци, обработката на посебните категории на лични податоци (конкретно податоци што се однесуваат на здравјето) може да се врши, кога е неопходна за целите на превентивна или трудова медицина, **за проценка на работоспособноста на вработениот**, медицинска дијагноза, обезбедување на здравствена или социјална нега или третман или за целите на управување со услугите и системите за здравствена или социјална заштита, врз основа на закон или во согласност со договор со здравствениот работник во кој предмет се условите и заштитните мерки наведени во ставот (3) на членот 13.
За овој тип на податоци не е потребена согласност од Агенцијата.

2. Дали се сметаат за обработувачи на лични податоци третите страни кои вршат услуги на одржување (хигиенски услуги, хаусмајсторски услуги и сл.)? Вработените кај овие трети страни при извршувањето на своите обврски од договорот може да имаат увид во одредени податоци вклучително и лични податоци, но не е предмет на договорот обработката на личните податоци?

За ваквите вработени не се бара посебен договор бидејќи тие реално не обработуваат лични податоци, меѓутоа можат не сакајќи да дојдат (да пристапат или да имаат увид) до тие податоци. Заради тоа, доволно ќе биде овие вработени да потпишат изјава за доверливост и тајност на личните податоци.

3. Земајќи ја во предвид динамиката на економијата и со оглед на потребата компаниите да се прилагодат на новите потреби и трендови со цел да останат конкуренти на пазарите, дали во случај на заминување на вработени, компаниите се обврзани да го чуваат персоналното досие 45 години - како што е сегашната регулатива? Исто така дали со изјавата за согласност за обработка на лични податоци што ја потпишуваат при засновање на работен однос се покрива и овој сегмент (договор за работа, телефонски број, мејл адреса, М1-М2 И сл.) или е потребна дополнителна изјава?

Во однос на роковите на чување, членот 9 став (1) алинеја 5 од Законот за заштита на личните податоци (ЗЗЛП) предвидува личните податоци да се чуваат во форма која овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци (доколку не постојат законски утврдени рокови, тогаш самиот работодавец треба да го утврди рокот на чување). Оваа материја е уредена со Законот за архивско работење т.е. во Упатството за начинот и техниката на постапување со архивскиот и

документарниот материјал во канцелариското и архивското работење (Прилог 3), каде е предвидено дека работните досиеја ќе се чуваат 45 години (освен кога се работи за боледувања, решенија за годишен одмор и сл., во овие случаи рокот е 2 години). Овие рокови треба да се почитуваат.

4. Потпрашање- Дали по заминување на работникот, треба да побара компанијата од него да потпише согласност да му се чуваат неговите лични податоци?

Бидејќи компаниите имаат законска обврска да ги чуваат личните податоци, тие податоци треба да се чуваат, без разлика дали му одговара на работникот или не. Оттука, нема потреба од барање за потпишување на согласност од страна на работникот за чување на неговите лични податоци.

5. Дали резимињата кој ги добиваат компаниите за објавените работни позиции за евентуални идни вработувања, потребно е претходно да се обезбеди изјава од кандидатот дека се согласува неговото резиме да биде зачувано во базата на кандидати?

Во ЗРО е предвидено како се одвива постапката за вработување. Доколку се работи за конкретен оглас нема потреба од согласност од кандидатот затоа што кога некој се пријавил на огласот, се подразбира дека е согласен да му се обработуваат личните податоци и да приложи соодветни докази (документација) во процесот на регрутација. Работодавецот има обврска доколку тој кандидат не го избере, да му ја врати целокупната документација во рок утврден во ЗРО.

6. Дали при објавување на огласи има обрска да стои клаузула дека кандидатите со испраќање на нивното резиме, се согласуваат нивните лични податоци да бидат обработувани за целите на евентуално идно вработување?

Доколку контролорот има намера да воспостави збирка на кандидати за идни вработување (не се работи за оглас за конкретно работно место), во тој случај потребна е согласност од субјектот на личните податоци за да биде дел од таа збирка. Контролорот треба да утврди колку време ќе се чуваат овие податоци (на пример до 6 месеци, по истекот на овој рок, контролорот може повторно да го праша кандидатот дали се согласува неговите лични податоци да бидат и понатаму дел од оваа збирка). Исто така, кандидатот треба да биде информиран од страна на контролорот дека истиот ќе може во секое време да ја повлече неговата согласност, односно да не биде дел од збирката на кандидати за идни вработувања.

7. Во однос на видео – надзорот, Законот за заштита на лични податоци во член 94 го регулира давањето лични податоци на корисници. Како е напишана одредбата, упатува дека корисници се јавни институции („...доколку истите се потребни за извршување на работи во рамките на со закон утврдени надлежности на корисникот....“).

Корисник може да биде и физичко лице и приватна компанија. На пример одреден вработен се здобил со повреда на работното место или му е украден или оштетен негов предмет, и притоа знае дека бил под видео надзор, во тој случај има право да побара снимка од конкретен датум и час, за да го искористи на пример во судска постапка. Контролорот има право да ја даде таа снимка, односно тој сегмент од снимката за кој работникот имал основ да ја бара. Оттука не само јавниот сектор може да се јави како корисник, многу почесто во праксата приватниот сектор или физичките лица се јавуваат како корисници на личните податоци. Секако, кога ќе се поднесе вакво барање до кој било контролор, тој ќе направи проценка дали има правен основ за да ги даде податоците на користење на лицето кое ги бара.

8. Истовремено, дефиницијата за корисник го вклучува и „секое физичко лице“. Во кој случај на физичко лице би требало да се третира како корисник? Нејасна е одредбата на кого точно се однесува, кога физичко лице има право да добие лични податоци „на користење“?!

Како надоврзување на претходното прашање, ако некому за некоја постапка му е потребен некој податок (на пример при кражба или оштета), во тој случај би требало да му се даде тој податок за конкретната ситуација. Значи не цела снимка, туку само делот каде бил снимен.

9. Дали барањето за информација за статус на вакцинација на вработени се смета за профилирање и под какви услови вработените мораат да дадат таква информација?!

Тука не се работи за профилирање, туку за барање на податоци што се однесуваат на здравјето. Сепак, ќе треба да се оцени дали работодавачот има законски основ да ги добие тие податоци, на пример дали се услов за да работникот биде во работен однос, со оглед дека вакцинирањето не е задолжително, туку доброволно.

10. Дали е дозволено автокомпании кои даваат возила на пробно возење да инсталираат камери кои ќе снимаат во возилото и надвор од возилото, доколку имаат согласност од лицето кое го зема возилото за пробно возење?

Со новиот ЗЗЛП, предвидено е дека кога имаме систематско набљудување на јавно достапен простор, обемна обработка на личните податоци или на пример употреба на нови технолошки и иновативни решенија итн., ќе треба самата компанија да направи проценка на влијанието на заштитата на личните податоци, односно да оцени дали постои ризик и дали има законски основ да постави видео надзор за конкретната цел. Во однос на надворешниот простор, по правило, снимањето на јавна површина е регулирано со други прописи и јасно е предвидено кој се може да врши снимање на јавни површини. Оттука, снимањето на надворешниот простор, би било надвор од просторот што е доволен за остварување на целта за која би се поставил видео надзорот од страна на автокомпаниите. За поставување на видео надзор во возила, АЗЛП ќе подготви посебни насоки.

11. Дали збирките на лични податоци и понатаму ќе треба да се евидентираат и ажурираат во централниот регистар на Агенцијата за заштита на лични податоци?

Агенцијата е во фаза на прилагодување на централниот регистар на новините од Законот за заштита на личните податоци и истиот ќе се преименува во Евиденција на збирки на лични податоци со висок ризик. Кога ќе биде целосно подготвен за користење, сите контролори ќе бидат информирани по е-маил и преку соопштение на веб страницата на Агенцијата.

12. Во смисла на член 32 – Обработувач, од Законот за заштита на личните податоци, дали е потребно да се анексираат постоечките договори за услуги или договорите за неоткривање на доверливи информации со третите лица – обработувачи/контролори? Или тоа важи само за новите договори кои ќе се склучат по истекот на периодот на усогласување со законот?

Обврската од член 32 се однесува и за постоечките договори. Овој член е малку поопширен во однос на претходниот член 26 од стариот ЗЗЛП, и сега има некои нови правила кои самите контролори и обработувачи ќе треба да ги предвидат во новите договори. Исто така, ќе треба да се земе предвид и членот 28 од Правилникот за безбедност на обработката на лични податоци, каде

што се бара самите контролори да направат процедура со критериуми како ќе вршат избор на обработувачите.

13. Дали формата на изјавата за обработување на лични податоци може да биде земена и по електронски пат?

Ако има електронски потпис, согласноста за обработка на личните податоци по правило би била неспорна. Меѓутоа, без електронски потпис, контролорите можат да имаат проблем при докажувањето на согласноста, односно дали е дадена од соодветното лице. Законот за електронски документи, електронска идентификација и доверливи услуги ќе треба да го применат во конкретниот случај. Согласноста може да биде дадена во електронска форма и без електронски потпис, но треба да има доказ дека е дадена доброволно и од физичкото лице на која се однесува.

14. Согласно член 41 од Законот за заштита на лични податоци, офицерот за заштита на лични податоци се определува врз основа на неговите стручни квалификации. Ве молиме за насоки и размислувања во однос на практичната примена на оваа одредба, како Агенцијата би ги ценела конкретните стручни квалификации.

Посетени обуки, сертификати, претходно искуство - на пример доколку бил офицер во некоја компанија и работодавецот му издаде потврда дека бил на таа позиција и извршувал задачи како офицер, или пак извршувал некои проекти и активности кои биле поврзани со заштитата на личните податоци. Сè од претходно кажаното може да се докаже и Агенцијата би ги земала предвид кога ќе врши супервизија.

15. Во член 42 став 6 во Законот за заштита на лични податоци стои: „Офицерот за заштита на личните податоци може да врши и други задачи и должности. Контролорот или обработувачот е должен да обезбеди дека таквите задачи и должности не доведуваат до судир на интереси“. Дали има конфликт на интерес доколку Офицер за заштита на лични податоци биде воедно и вработен во ИТ сектор или пак да биде Одговорно лице за информациска сигурност (ОСИС)?

Офицерот за заштита на личните податоци не може да биде истото лице кое е администратор на информацискиот систем (или доколку и администраторот е истовремено ОСИС). Офицерот треба да му врши контроли на администраторот и не може истото лице да врши вакви контроли врз самиот себе. Меѓутоа, доколку работи во ИТ секторот, но на позиција различна од администратор на информацискиот систем, во тој случај би можел да биде офицер, бидејќи нема определба за профилот на офицерот - дали да биде правник, информатичар или од некоја друга област. Исто така е важно дека Офицерот не треба да обработува лични податоци. Често пати во пракса гледаме дека лицето задолжено за човечки ресурси е и офицер. Тоа лице не може да биде офицер бидејќи можно е да биде пристрасен кога ќе ја контролира сопствената збирка. Од тие причини, бараме офицерот да нема допирни точки со некои од збирките, односно со некои од операциите на обработка на личните податоци.

16. Дали пред Агенцијата за заштита на лични податоци ќе важат меѓународните сертификати за DPO (Data Protection Officer) издадени од овластени сертификациони куќи?

Да, ќе важат. Во моментот нема правило дека обуките мора да бидат испорачани од АЗЛП, туку може да бидат и од други институции/компании. Меѓутоа, Агенцијата во скоро време планира да изработи подзаконски акти за сертификација на сопствените обуки.

17. Доколку е потребно одобрение од АЗЛП иако контролорот и обработувачот ги склучиле стандардните клаузули за заштита на личните податоци кои се одобрени од страна на Европската комисија, што е потребно да се достави во прилог на барањето за добивање на одобрение за пренос на лични податоци (покрај самите стандардните клаузули)?

Правилникот за пренос на лични податоци, објавен на веб страницарта на АЗЛП и во „Службен весник на РСМ“ бр. 122/20, содржи обрасци, поместени на крајот на актот. Може да се види во образец 3, детално што сè треба да пополнат и да достават контролорите до Агенцијата за конкретниот вид на пренос на лични податоци. Доколку се потребни дополнителни информации, вработените од АЗЛП ќе ги информираат контролорите за да ги достават.

18. Во врска со пренос на лични податоци во трети земји/организации - дали постои одлука за соодветност донесена од страна на АЗЛП? Доколку не постои одлука за соодветност, дали е потребно да се бара одобрение за преносот од АЗЛП, доколку контролорот и обработувачот ги склучиле стандардните клаузули за заштита на личните податоци кои се одобрени од страна на Европската комисија? Дополнително, доколку не е потребно во овој случај одобрение од АЗЛП, дали контролорот има друга обврска спрема АЗЛП (на пример да ја извести АЗЛП за преносот извршен врз основа на стандардните клаузули и слично)?

Во јуни 2021, Европската комисија ги усвои споменатите договорни клаузули. Агенцијата е во фаза на превод на истите и по усвојувањето, секако ќе бидат достапни до контролорите за да можат да ги користат. Контролорите ќе бидат информирани на веб страницата на АЗЛП. Новина во овој закон е што постојат различни начини на кои може да се изврши пренос на лични податоци. Не е само со одобрение на Агенцијата, туку ќе постојат и уште неколку начини на одобрување на преносот на личните податоци. Самите контролори ќе треба да оценат на кој начин и кога ќе ја известат Агенцијата.

19. При работа со клиенти од странство, документите кои ги разменуваме по мејл содржат лични податоци, вклучително и посебни категории на лични податоци. Дали за ваквата комуникација по мејл е потребно да се извести Агенцијата за заштита на лични податоци, како за пренос во трети земји? Напоменуваме дека немаме детален податок во кои се земји се наоѓаат серверите во кои се складираат / чуваат личните податоци.

Ако е-маил серверот е надвор од РС Македонија, во тој случај неспорно е дека се врши пренос на лични податоци и ќе треба да се информира АЗЛП каде се врши преносот. Меѓутоа, ваквата информација ќе мора да ја знае контролорот, бидејќи Агенцијата ги добива информациите од контролорот. Затоа е битно кога контролорите склучуваат договори или кога користат такви услуги од ИТ компаниите, да ги дознаат и овие информации, бидејќи во спротивно, би се сметало за криење на информации, односно оневозможување на супервизорот при вршење на супервизија, што претставува прекршок.

20. Дали постои друг начин или услови што треба да ги исполнат контролорот и обработувачот за пренос на лични податоци во трета земја без да постои обврска да се бара одобрение од АЗЛП за преносот?

Тоа се отстапувањата утврдени во членот 53 од ЗЗЛП. Меѓутоа, тие се користат само доколку преносот не е повторувачки и се однесува само на ограничен број на субјекти на лични податоци, а истиот е потребен за исполнување на легитимните интереси на контролорот над кои не преовладуваат интересите или правата и слободите на субјектот на лични податоци, при што контролорот ги оценил сите околности поврзани со преносот на личните податоци и врз основа на таа проценка обезбедил соодветни заштитни мерки во однос на заштитата на личните податоци. За сè друго, ќе мора да се користат некои од претходните членови за пренос.

21. Во врска со делот со Управување со Лозинка (член 38 од ПРАВИЛНИК ЗА БЕЗБЕДНОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ). Дали доколку примениме криптирање на лозинките (зип фајл со лозинка) или користиме друга алатка за енкрипција на лозинките ќе биде согласно овој дел од Правилникот? Дали мора да се користи софтвер каде ќе ги чуваме лозинките со мастер лозинка или може примената да ја направиме на начинот опишан погоре? Дали според Вашето искуство можете да ни дадете пример на софтвер или алатка која би можеле да ја користиме во овој случај?

Кога се работи за некоја конкретна обработка, АЗЛП не дава мислење како контролорите треба да се заштитат и кои технички мерки треба да ги применат. Секој контролор ќе треба да направи претходна проценка на ризик, се разбира по одредени критериуми и методологија каде што ќе утврди кои технички и организациски мерки треба да ги примени за да одговараат соодветно на ризикот кој го утврдил. Од таа проценка ќе зависи какви мерки ќе примени контролорот за конкретна обработка. Тука секако е и битно за кои процеси на обработка станува збор, кои категории на лични податоци се обработуваат, колку луѓе пристапуваат, каде се чуваат податоците, итн. Значи, има еден сет на прашања на кои треба претходно да се одговори, за да знае контролорот какви мерки треба да примени.

22. Во делот на Псевдонимизација согласно член 29 и член 36 (став 3) од Законот за ЗЛП прашањето е во кој контекст е потребно да се изведе ваква превентивна активност на пример во една банка? Во банкарската апликација нивоата на пристап на секој вработен е точно и детално уреден и се знае кој, до кои форми има пристап а со тоа и до кои лични податоци. Пристап до банкарската апликација имаат само службениците со соодветни безбедносни контроли и ниво на пристап, што го отвара прашањето од кого би се заштитиле личните податоци, бидејќи оној кој има пристап до соодветната форма има овластување и да ги обработува таквите лични податоци кои се таму прикажани.
    Воедно во член 44 - Кодекси на однесување во став 1 треба да се наведе на кој начин (на пример во Банкарскиот сектор) да биде прецизирана примената на овој закон поточно на точка (г) псевдонимизацијата на личните податоци;
    Ве молам за објаснување со пример за модел како би се спровела псевдонимизација на лични податоци во една ваква околина (во банка) без притоа да се наруши деловното работење и покрај тоа што се применуваат сите овие безбедносни контроли, нивоа на пристап, енкрипција на податоци и сл?

Самите контролори откако ќе ја направат проценката на ризик, треба да утврдат кои мерки ќе ги применат. Доколку сметаат дека треба да направат псевдонимизација, можат да го направат тоа. Меѓутоа, кога се прави псевдоминизација, треба да се земе предвид кај контролорот дали секој овластен треба да пристапи до тие лични податоци и дали му требаат личните податоци во чист (читлив) формат. Ако на некој сектор не му се потребни податоците во ваков формат, односно може да ги добие податоците псевдонимизирани, а да ја добие информацијата која му е потребна, тогаш

треба да ја примени псевдонимизацијата како мерка. Во моментов кај нас не се изработени правила за псевдонимизација, но АЗЛП ќе подготви сет на прирачници од технички карактер, меѓу кои и за псевдонимизацијата.

23. Член 21 - Право на бришење („право да се биде заборавен“) од Законот за ЗЛП – Во банкарскиот сектор согласно регулативата на НБРСМ потребно е да се врши соодветно бекапирање на критичните системи вклучително и базите на податоци каде се наоѓаат и личните податоци на клиентите. Ваквите бекап процеси налагаат податоците да се снимаат и на лента (или друг медиум) која соодветно криптирана се чува соодветен временски период. Доколку некој клиент побара да му бидат избришани неговите лични податоци од било која од причините кои ги овозможува законот, како би се избришале податоците кои се зачувани на лента (или друг медиум) и соодветно заштитени без притоа да се наруши интегритетот на останатите податоци зачувани на тој медиум?

Контролор треба да одлучи како ќе прави синхронизација на бекапот во случај на бришење на лични податоци. Агенцијата може да му нареди на контролорот да ги избрише податоците во случај доколку дојде некоја странка и се пожали дека една компанијата или институција не ѝ ги избришала податоците, а реално немало законски основ и понатаму истите да се чуваат.

24. Дали мултилатералните мегународни договори во рамките на една компанија кои биле претходно одобрени од Дирекцијата, сега треба и агенцијата да ги одобри?

На сила е нов ЗЗЛП, со тоа и нови правила, затоа ќе треба да се направи повторно проценка на истите за да се утврди дали се усогласени или не со овие правила.

25. Дали треба да се прави проценка на влијание врз заштитата на личните податоци за постоечките збирки кои беа претходно одобрени според старата регулатива од страна на Агенцијата?

По правило, проценка треба да се направи за сè што е предвидено во листата за задолжителна проценка на влијанието на заштитата на лични податоци. Затоа предвиден е преоден период со цел контролорите да го усогласат своето работење со ЗЗЛП.

26. Дали пред имплементација на систем за контрола на пристап со биометриски податоци, пред обработка, треба ли да се информира АЗЛП и што сè треба да се достави до АЗЛП?

Агенцијата дава одобрение за обработка на биометриски податоци кои се посебни категории на лични податоци, освен ако постои законски основ. Во принцип, треба да се поднесе барање и соодветна документација со која ќе ја образложат потребата и техничките мерки кои планираат да ги применат. Образецот за одобрение за обработка на биометриски податоци е достапен на веб страницата на АЗЛП.

27. Што очекува Агенцијата за заштита на личните податоци („**АЗЛП**“) да се одвива по истекот на рокот за усогласување со новиот Закон за заштита на лични податоци („**Закон**“) во август 2021 година? Дали АЗЛП ќе се впушти во вршење инспекциски надзор кај контролорите и обработувачите на лични податоци за да ја осигура усогласеноста со Законот? Дали се

очекуваат строги контроли и казнувања или АЗЛП ќе дава препораки за отстранување на нерегуларностите во некој пропишан период?

Изминатите 16 месеци, Агенцијата даваше препораки како контролорите да го усогласат своето работење со ЗЗЛП. Од септември 2021 ЗЗЛП ќе се применува во целост, вклучително и во делот на прекршоците. Кај редовните супервизии Агенцијата и понатаму ќе предлага мерки и рокови за целосно усогласување на контролорите, на кои доколку не постапат по мерките, при контролната супервизија ќе може да им се изрече глоба за сторен прекршок. Додека пак кај вонредните супервизии, Агенцијата има право веднаш да изрече глоба за сторен прекршок, без оглед на дадените дополнителни мерки и рокови за усогласување.

28. Во однос на сертификационите тела регулирани со член 47 од Законот, може ли да ни кажете дали вакви веќе се акредитирани од страна на Инситутот за акредитација и како ќе се одвива овој процес?

Агенцијата ќе донесе сет на акти за сертификација.

29. Дали може да се употреби техничката мерка оневозможување на пристап до лични податоци во база на податоци како мерка исполнување на правото да се биде заборавен со вклучена експлицитна контрола за администраторски пристап?

Кога зборите за право да се биде заборавен, тоа е право да се биде избришан од евиденциите на контролорот, односно право на физичкото лице да му бидат избришани личните податоци. Правото да се биде заборавен не може да се оствари со некакви мерки, односно со забрана или ограничување на пристап до неговите лични податоци.

30. Во другите земји постојат подзаконски акти за заштита на лп за регулирање на банкарскиот сектор, дали кај нас може да се очекува ваков документ подржан од Агенцијата?

Агенцијата нема обврска да изготви ваков документ. Доколку се предложи некој ваков документ, Агенцијата може да даде поддршка.

31. Дали треба да се изготви проценка на влијанието врз заштита на лп во случаите кога се даваат сметководствени, даночни, правни услуги, врз основа на договор со правно лице, согласно кој се обработуваат податоци на физички лица (на пример пресметка на плата, подготовка на даночни пријави...)

Таму каде што има законска обврска да се обработуваат некои податоци, не треба да се прави проценка на влијание, како што е и горенаведената ситуација. За сè друго, како што е утврдено во Законот за заштита на личните податоци и подзаконските акти мора да се направи проценка.

32. Ве замолувам за појаснување по однос на можноста да се ангажира надворешно лице како офицер за заштита на лични податоци. Дали може едно физичко лице да биде Офицер за заштита на лични податоци за повеќе различни контролори/обработувачи? (за појаснување: не во смисла на офицер на група на правни лица како чл 41 ст.2, туку едно физичко лице да нуди вакви услуги на повеќе различни контролори).

Може да се ангажира надворешно физичко лице, но според праксата, подобро е офицер да биде вработен кај контролорот, односно лице кое ги знае процесите и ги знае вработените. Исто така, кога ќе се избере офицер истиот треба да им биде постојано достапен на вработените, а и обратно вработените да се постојано достапни на офицерот за да имаат меѓусебна комуникација, што е отежнато во случај на ангажирање на надворешно лице. Неспорно е дека може да се ангажира надворешно лице врз основа на договор за услуги чл. 41 став (6) од ЗЗЛП, посебно ако бројот на

вработени е лимитиран кај контролорот и ниту едно лице не ги исполнува условите од чл. 41 став (5) од ЗЗЛП.

33. Дополнително, во смисла на чл 41 ст.6, на обуката на АЗЛП од 03.03.2021 беше кажано дека правен субјект-контролор може да склучи Договор за услуга за Офицер со друго правно лице, а во него да биде назначено физичко лице кое ќе ја врши таа улога. Во овој случај: Дали еден правен субјект може да нуди услуги како офицер за заштита на лични податоци на повеќе различни неповрзани контролори, иако и самиот е контролор/обработувач?

Постојат правни лица кои нудат услуга за ангажирање на надворешен офицер било од редот на неговите вработени или други ангажирани лица. Договор за услуга ќе склучи контролорот со правнотот лице кое нуди вакви услуги.

34. Дали при обработката на личните податоци за директен маркетинг потребно е да се обезбеди претходна изречена согласност од субјектот на личните податоци за секој вид на директен маркетинг, без оглед дали вклучува и профилирање кое е поврзано со директниот маркетинг?

За обработка на лични податоци, многу е јасно уредено во ЗЗЛП, дека кога нема законски основ за обработка на личните податоци потребна е согласност од субјектот на личните податоци - согласноста е задолжителна кога се работи за директен маркетинг. Одговорот на ова прашање можат да се најде во член 11, а во врска со член 96 од ЗЗЛП. Доколку личните податоци се обработуваат за повеќе цели, меѓу кои и онаа за директен маркетинг, во тој случај согласноста за директен маркетинг треба да е издвоена како посебна согласност. Во секој случај, за кој било вид на обработка на лични податоци кои се обработуваат врз основа на согласност, треба да постои можност субјектот во секое време, да ја повлечи согласноста за обработка на личните податоци.

35. Во однос на соодветноста на техничките и организациските мерки кои би се применувале за заштита на личните податоци од страна на контролорите и обработувачите, дали Агенцијата е отворена за поддршка на контролорите и обработувачите за насоки во однос на подобрување или поставување соодветни технички и организациски мерки?

Ова прашање е општо и не може да се даде конкретен одговор бидејќи секој компанија е различна и различни мерки може да применуваат кои би биле најсоодветни за таа компанија, во дадената ситуација. Всушност, дали мерките се соодветни Агенцијата може да ги процени при вршење на супервизија. Агенцијата ќе подготви водич за технички и организациски мерки.

36. Дали АЗЛП има намера да објави насоки и совети за контролорите и обработувачите кои обработуваат лични податоци на вработени?

Веќе има водичи објавени од страна на Агенцијата што ги покриваат овие прашања. Агенцијата ќе објави нови/ажурирани правила, обрасци, алатки,... кои ќе им помогнат на контролорите за тоа како полесно да се усогласат со Законот за ЗЛП.

37. Доколку обврската за траснфер на податоци е барање согласно законски прописи, дали е потребно за тоа да се бара одобрување од Агенцијата?

Зависи дали станува збор за пренос во ЕУ или ЕЕП, или пак треба да се врши пренос во земја која не е дел од ЕУ или ЕЕП. Доколку е за ЕУ или ЕЕП, тогаш треба да се извести АЗЛП за преносот. Во другите ситуации треба да се постапи согласно глава V од ЗЗЛП.

- Дали по барање да се биде заборавен, постои рок за реализација на бришењето (1 година , 6 месеци ..)?

Рокот е 30 дена, доколку е потребно овој рок може да биде продолжен за уште два месеци земајќи ги предвид сложеноста и бројот на барањата. Контролорот го информира субјектот на личните податоци за секое продолжување во рок од еден месец од денот на приемот на барањето, заедно со причината за одложувањето (чл. 16 став (3) од ЗЗЛП).

- Доколку не може технички бришењето да се реализира за 30 дена, дали може да се продолжи за уште некое разумно времетраење?

Доколку е потребно овој рок може да биде продолжен за уште два месеци земајќи ги предвид сложеноста и бројот на барањата. Контролорот го информира субјектот на личните податоци за секое продолжување во рок од еден месец од денот на приемот на барањето, заедно со причината за одложувањето (чл. 16 став (3) од ЗЗЛП).

- Дали користење на cloud сервиси на сервери во ЕУ потребно е да се бара одобрение од Агенцијата за да се користат cloud сервиси како пренос на лични податоци? Пример Microsoft 365, Amazon...

Во принцип, Microsoft 365 и Amazon имаат сервери во ЕУ, така што доколку можат да докажат дека податоците за Македонија се на сервери во ЕУ или ЕЕП, во тој случај ќе треба само да ја информираат Агенцијата. Доколку се наоѓаат во која било земја надвор од ЕУ/ЕЕП, ќе треба да бараат одобрение од Агенцијата.

- Во кои случаи се користи легитимен интерес за законска основа за обработка?

Кога контролорот има законски основ за обработка на личните податоци, тогаш не треба да се повикува на легитимен интерес. Кога контролорот нема законски основ за обработка на личните податоци, а податоците му се неопходни, во тој случај најверојатно постои легитимен интерес за обработка на личните податоци. Кај легитимниот интерес е потребно да се направи LIA тест (тест за балансирање) од страна на контролорот.