ВОДИЧ ЗА ИЗВЕСТУВАЊА

ЗА НАРУШУВАЊЕ НА БЕЗБЕДНОСТА НА ЛИЧНИТЕ ПОДАТОЦИ

Овој проект е финансиран од Европската Унија

ВОВЕД

Законот за заштита на личните податоци (натаму во текстот: ЗЗЛП) воведува обврска за известување на Агенцијата за заштита на личните податоци (националниот надзорен орган) за нарушувањата на безбедноста на личните податоци и, во некои случаи, обврска за информирање на физичките лица кога тие се засегнати од конкретното нарушување.

ЗЗЛП пропишува дека известувањата се задолжителни за сите контролори, освен доколку не постои веројатност дека нарушувањето на безбедноста на личните податоци ќе резултира во висок ризик по правата и слободите на физичките лица. Обработувачите имаат важна улога во оваа постапка бидејќи тие мора да го известат контролорот за сите нарушувања на безбедноста на личните податоци.

Обврската за известување носи голем број погодности. Кога ја известуваат АЗЛП, контролорите може да добијат совет дали засегнатите физички лица треба да бидат информирани. Во таков случај АЗЛП може да му нареди на контролорот да ги информира засегнатите лица за нарушувањето на безбедноста на личните податоци.

Од друга страна, информирањето на физичките лица за ваков настан им овозможува на контролорите да обезбедат информации за ризиците кои се резултат од нарушувањето на

безбедноста на личните податоци и за чекорите што засегнатите лица може да ги преземат за да се заштитат од можни последици.

Плановите за справување со нарушувања на безбедноста на личните податоци треба да се фокусираат на заштита на физичките лица и на нивните лични податоци. Следствено, известувањата за нарушување на безбедноста на личните податоци се сметаат за важна алатка која ја зајакнува усогласеноста со прописите за заштита на личните податоци. Во исто време треба да се забележи дека неподнесување известување до физичките лица или до АЗЛП повлекува изрекување на санкции за контролорот и/или обработувачот, во согласност со член 110 став (1) точки 11) и 12) од ЗЗЛП.

Затоа контролорите и обработувачите се охрабруваат да изготват планови и да воспостават постапки што ќе им овозможат навремено идентификување и прекинување на нарушувањето на безбедноста на личните податоци, да ги проценат ризиците за физичките лица и потоа да утврдат дали е потребно да се достави известување до АЗЛП и да се информираат физичките лица кои се засегнати со нарушувањето. Известувањето до АЗЛП треба да биде дел од таков план за справување со инциденти.

04

ЗЗЛП содржи одредби кои уредуваат кога и кој треба да биде известен за нарушувањето на безбедноста на личните податоци, како и видот на информации што треба да се дадат како дел од известувањето. Информациите од известувањето може да се обезбедат постепено (во фази), но во сите случаи контролорите треба навремено да реагираат на секое нарушување на безбедноста.

СОДРЖИНА

1.Известување за нарушување на безбедноста на личните податоци според ЗЗЛП

1.1.Генерални белешки за безбедноста

Еден од условите што ги пропишува ЗЗЛП се однесува на примена на соодветни технички и организациски мерки за да се обезбеди дека личните податоци се обработуваат на начин кој вклучува заштита на податоците, односно заштита од неовластена или незаконска обработка и од случајно губење, уништување или оштетување на податоците.

Следствено, ЗЗЛП налага контролорите и обработувачите да применуваат соодветни технички и организациски мерки за да обезбедат ниво на безбедност што одговара на ризикот од обработката на лични податоци.

Тие треба да ги земат предвид најновите технологии, трошокот за спроведување, како и природата, обемот, контекстот и целите на обработката, и ризиците со различна веројатност и сериозност по правата и слободите на физичките лица.

Оттука, клучен елемент на секоја политика за безбедност на личните податоци е контролорот да биде подготвен, кога тоа е можно, да го прекине нарушувањето на безбедноста на личните податоци, а кога тоа сепак ќе се случи, навремено да реагира.

Пример:

Пример за губење на личните податоци може да биде ситуација во која уредот што содржи копија од базата на клиентите на контролорот е украден или изгубен. Друг пример за губење на лични податоци може да биде ситуација во која единствената копија од личните податоци е криптирана од хакер со рансомвер (малициозен софтвер) или таа е криптирана од контролорот со клуч кој повеќе не е во негова сопственост.

Она што треба да биде јасно е дека нарушувањето е вид на безбедносен инцидент. Сепак, согласно дефиницијата од член 4, точка 12) од ЗЗЛП, одредбите од законот се применуваат само во случај на нарушување на безбедноста на личните податоци. Последиците за контролорот од такво нарушување вклучуваат неусогласеност со начелата за обработка на личните податоци, онака како се дадени во член 9 од ЗЗЛП. Тоа ја нагласува разликата меѓу безбедносен инцидент и нарушување на безбедноста на личните податоци, т.е. иако сите нарушувања се сметаат за безбедносни инциденти, не сите безбедносни инциденти задолжително вклучуваат нарушување на безбедноста на личните податоци.

1.2.Што е нарушување на безбедноста на личните податоци?

1.2.1.Дефиниција

Како дел од обидот за решавање на нарушувањето на безбедноста на личните податоци, контролорите прво треба да бидат во можност да препознаат дека станува збор за таков настан. Во член 4, точка 12), ЗЗЛП ја дава следнава дефиниција за „нарушување на безбедноста на личните податоци“:

„секое нарушување на безбедноста што доведува до случајно или незаконско уништување, губење, менување, неовластено откривање или пристапување до личните податоци кои се пренесуваат, чуваат или на друг начин се обработуваат“.

Она што се подразбира под „уништување“ на личните податоци треба да биде прилично јасно: тоа е моментот кога податоците повеќе не постојат или не постојат во формата во која ги користи контролорот“. И „менувањето“ на личните податоци е релативно очигледно: тоа е моментот кога личните податоци се изменети, корумпирани или повеќе не се сметаат за целосни. „Губењето“ на личните податоци треба да се толкува како можно постоење на податоците, но контролорот изгубил контрола врз или пристап до нив, или податоците повеќе не се во негова сопственост. На крај, „неовластена или незаконска обработка“ може да вклучи откривање на личните податоци (или давање пристап до податоците) на корисници кои не се овластени за добивање или пристап до податоците, или некоја друга форма на обработка која е спротивна на ЗЗЛП.

1.2.2. Видови на нарушувања на безбедноста на личните податоци

Нарушувањата може да се категоризираат според следниве три добропознати начела за информатичка безбедност:

- „нарушување на доверливоста“ – кога постои неовластено или случајно откривање или пристапување до личните податоци;
- „нарушување на интегритетот“ – кога постои неовластено или случајно менување на личните податоци;
- „нарушување на достапноста“ – кога постои случајно или неовластено губење на пристапот до или уништување на личните податоци.

Треба да се забележи дека, во зависност од околностите, нарушувањето на безбедноста на личните податоци може истовремено да се однесува на доверливоста, интегритетот и достапноста на личните податоци, или може да се однесува на која било комбинација од овие три ситуации.

Додека утврдувањето на фактот дали станува збор за нарушување на доверливоста или нарушување на интегритетот е релативно едноставно, утврдувањето дали постои нарушување на достапноста на личните податоци нема да биде толку очигледно. Перманентно губење или уништување на личните податоци секогаш се смета за нарушување на достапноста на личните податоци.

Примери за недостапност на личните податоци вклучуваат ситуации во кои податоците биле случајно избришани или избришани од страна на неовластено лице, или кога е изгубен клучот за декриптирање на податоците кои биле претходно криптирани од безбедносни причини. Кога контролорот не може да го поврати пристапот до податоците, на пример, од резервната копија на податоците, тоа се смета за постојана загуба на достапноста. Недостапност на личните податоци може да се појави и кога има значајно нарушување на нормалното работење на една организација, на пример, ако таа се соочува со прекин на електрична енергија или со напад за одбивање на услугата (denial of service), при што податоците стануваат недостапни.

Тука се поставува прашањето дали времена недостапност на личните податоци треба да се смета за нарушување на безбедноста и кој треба да биде известен за истото. Член 36 од ЗЗЛП се однесува на безбедноста на обработката на лични податоци и пропишува дека кога применуваат технички и организациски мерки за обезбедување соодветно ниво на безбедност што одговара на ризикот, меѓу другото, контролорите треба да покажат „способност за обезбедување континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка“ и „способност за навремено повратување на достапноста и пристапот до личните податоци во случај на физички или технички инцидент“.

Оттука може да се заклучи дека безбедносен инцидент кој резултира во недостапност на личните податоци за одреден временски период е вид на нарушување на безбедноста на личните податоци бидејќи неможност да се пристапи до податоците може да има значително влијание врз правата и слободите на физичките лица. Сепак, ситуација во која личните податоци се недостапни поради планирано одржување на системот не се смета за нарушување на безбедноста на личните податоци според дефиницијата дадена во член 4, точка 12) од ЗЗЛП.

Исто како ситуацијата со губење или уништување на личните податоци (или кој било друг вид на нарушување на безбедноста на личните податоци), нарушувањата кои подразбираат привремена недостапност на личните податоци мора да бидат документирани во согласност со член 37 став (5) од ЗЗЛП. Тоа им помага на контролорите да покажат отчетност пред АЗЛП, која може да ги побара таквите записи. Во зависност од околностите, нарушувањето на безбедноста на личните податоци може, но не мора, да наложи обврска за известување на АЗЛП и информирање на засегнатите физички лица. Контролорите треба да ја оценат веројатноста и сериозноста на влијанието од недостапноста на личните податоци врз правата и слободите на физичките лица. Според член 38 од ЗЗЛП, контролорите треба да ги информираат субјектите на лични податоци освен доколку не постои веројатност дека нарушувањето ќе резултира во ризик по нивните права и слободи. Се разбира, ваквата оценка се прави на индивидуална основа за секој случај одделно.

Примери:

Ако критичните медицински податоци за пациентите на една болница се недостапни, дури и привремено, тоа може да претставува ризик по правата и слободите на физичките лица, на пример, откажување на хируршка операција и ставање на нивниот живот во ризик.

Во случај на недостапност на системите на една медиумска куќа во период од неколку часа (на пример, поради прекин на електричната енергија), што ја спречува компанијата да испрати информатори до претплатниците, не постои веројатност дека тоа ќе предизвика ризик по правата и слободите на физичките лица.

Треба да се нагласи дека иако недостапноста на системите на контролорот е привремена и можеби не влијае врз физичките лица, важно е контролорот да ги разгледа сите можни последици од нарушувањето на безбедноста на личните податоци бидејќи тоа сепак може да наметне обврска за известување од други причини.

Примери:

Напад со рансомвер (малициозен софтвер што ги криптира податоците на контролорот додека да се плати откупот) може да доведе до привремена недостапност на податоци ако тие не може да се повратат од резервната копија. Во овој случај, мрежата на контролорот била пробиена и тоа налага известување доколку

инцидентот се квалификува како нарушување на доверливоста на личните податоци (т.е. напаѓачот пристапил до личните податоци) и претставува ризик по правата и слободите на физичките лица.

1.2.3. Можни последици од нарушувањето на безбедноста на личните податоци

Потенцијално, нарушувањето на безбедноста на личните податоци може да има широк спектар на негативни ефекти врз физичките лица, кои пак резултираат во физичка, материјална или нематеријална штета. Тоа може да вклучи загуба на контролата врз нивните лични податоци, ограничување на нивните права, дискриминација, кражба на идентитет или идентитетска измама, финансиска загуба, неовластено враќање во оригиналната форма на псевдономизирани податоци, нарушен углед и загуба на доверливоста на личните податоци кои се заштитени со деловна тајна. Исто така, тоа може да вклучи и други значајни економски или социјални неповолности за засегнатите физички лица.

Следствено, ЗЗЛП налага контролорот да ја извести АЗЛП за нарушувањето на безбедноста на личните податоци, освен доколку не постои веројатност дека тоа ќе резултира во негативни ефекти. Кога постои веројатност за висок ризик за појава на вакви негативни ефекти, ЗЗЛП налага контролорот да ги информира засегнатите физички лица за нарушувањето на безбедноста на личните податоци веднаш штом тоа е разумно изводливо.

Ако контролорот или обработувачот не ја извести АЗЛП или субјектите на лични податоци или пак не достави никакво известување до ниту една страна и покрај фактот дека се исполнети условите од член 37 и/ или член 38 од ЗЗЛП, тогаш АЗЛП може да размисли за изрекување соодветна прекршочна глоба во согласност со член 110. При изрекување на глобата, нејзината вредност може да се утврди во износ до 2% од вкупниот годишен приход на контролорот или обработувачот

остварен во период пократок од една година кога прекршокот е - правното лице (во апсолутен износ) остварен во деловната година што ѝ претходи на годината кога е сторен прекршокот или од вкупниот приход сторен од правното лице во првата година од започнувањето на неговата работа.

Треба да се има предвид дека, во некои случаи, неподнесувањето известување за нарушување на безбедноста на личните податоци може да упатува на отсуство на безбедносни мерки или несоодветност на безбедносните мерки што се применуваат. Неколку различни прекршоци сторени во исто време и како дел од еден случај значи дека надзорниот орган може да изрече прекршочна глоба во износ кој е ефективен, пропорционален и има одвратувачки ефект, и влегува во групата на најсериозни прекршоци. Во таков случај, АЗЛП има можност да изрече санкции за неисполнување на обврската за известување на Агенцијата и на субјектите на лични податоци за нарушување на безбедноста на личните податоци (членови 37 и 38) од една страна, и за неисполнување на обврската за примена на (соодветни) безбедносни мерки (член 36) од друга страна, бидејќи тие претставуваат посебни прекршоци.

2.Член 37: известување на АЗЛП

2.1. Кога треба да се поднесе известување

2.1.1. 1.Условите пропишани во член 37 од ЗЗЛП

Член 37 став (1) од ЗЗЛП пропишува дека:
„Во случај на нарушување на безбедноста на личните податоци, контролорот веднаш и не подоцна од 72 часа откако дознал за истото е должен да ја извести Агенцијата за нарушувањето на безбедноста на личните податоци, освен доколку не постои веројатност дека нарушувањето на безбедноста ќе резултира во ризик по правата и слободите на физичките лица. Кога известувањето до Агенцијата не е поднесено во рок од 72 часа, заедно со известувањето контролорот треба да достави и образложение за причините за доцнењето."

2.1.2. Кога контролорот „дознава" за нарушување на безбедноста на личните податоци?

Како што беше наведено претходно, ЗЗЛП пропишува обврска дека известувањето за нарушување на безбедноста на личните податоци треба да се поднесе веднаш и не подоцна од 72 часа откако контролорот дознал за истото. Тука се отвора прашањето за тоа кога се смета дека контролорот „дознал" за нарушувањето на безбедноста на личните податоци. Се смета дека контролорот „дознал" за нарушувањето на безбедноста кога постои разумно ниво на сигурност дека се случил безбедносен инцидент кој довел до компромитирање на личните податоци.

Во исто време, ЗЗЛП пропишува и обврска за контролорите и обработувачите да ги применат сите соодветни технички и организациски мерки за заштита со цел да утврдат дали се случило нарушување на безбедноста на личните податоци и веднаш да ја информираат АЗЛП и субјектите на лични податоци. Притоа, при утврдување на фактот дали известувањето било поднесено веднаш и без непотребно одлагање, предвид треба да се земе природата и сериозноста на нарушувањето на безбедноста на личните податоци, како и последиците и негативните ефекти врз субјектите на лични податоци. Оттука, контролорите/обработувачите имаат обврска да се осигурат дека се во можност навремено да „дознаат" за секое нарушување на безбедноста на личните податоци за да може да преземат соодветни дејствија.

Кога точно се смета дека контролорот „дознал" за некое нарушување на безбедноста на личните податоци ќе зависи од околностите во конкретниот случај. Во некои случаи, тоа ќе биде релативно јасно, но во други случаи потребно е одредено време да се утврди дали се компромитирани личните податоци. Сепак, акцентот се става на брза акција за истражување на инцидентот за да се утврди дали безбедноста на личните податоци е навистина нарушена, и ако е така, да се преземат корективни дејства и да се поднесе известување, кога тоа е потребно.

Примери:

1. Во случај кога некој УСБ уред со некриптирани лични податоци е изгубен честопати не може да се утврди дали неовластени лица се стекнале со пристап до податоците на уредот. Сепак, иако контролорот не може да утврди дали се случило нарушување на доверливоста на личните податоци, таквата ситуација треба да се пријави бидејќи постои разумен степен на сигурност дека настанало нарушување на достапноста на личните податоци, и се смета дека контролорот „дознал" за истото во моментот кога сфатил дека УСБ уредот е изгубен.

2. Трета страна го информира контролорот дека тие случајно добиле лични податоци за еден од неговите клиенти и обезбедува доказ за неовластено откривање на лични податоци. Бидејќи контролорот добил јасен доказ за нарушување на доверливоста на личните податоци, нема сомнеж дека тој „дознал" за нарушувањето.

3. Контролорот открива дека постои можен упад во неговата мрежа. Контролорот ги проверува своите системи за да утврди дали личните податоци кои се чуваат на тие системи се компромитирани и потврдува дека тоа е така. Повторно, бидејќи по спроведената проверка контролорот има јасен доказ за нарушувањето на безбедноста на личните податоци, нема сомнеж дека тој „дознал" за настанот.

4. Кибер-криминалец го контактира контролорот откако го хакирал неговиот систем и бара откуп за да го отклучи. Во таков случај, откако направил проверка за да потврди дека системот бил нападнат, контролорот има јасен доказ дека настанало нарушување на безбедноста на личните податоци и нема сомнеж дека тој „дознал" за истото.

Откако бил известен за потенцијално нарушување на безбедноста на личните податоци од страна на некое физичко лице, медиум или друг извор, или кога самиот открил безбедносен инцидент, на контролорот може да му треба краток временски период за да истражи дали навистина се случило нарушување на безбедноста. Оттука, додека трае истрагата не може да се смета дека контролор „дознал" за нарушувањето. Сепак, се очекува дека иницијалната истрага треба да почне колку што е можно побрзо и да утврди, со разумно ниво на сигурност, дали навистина се случило нарушување на безбедноста на личните податоци, по што може да се направи подетална истрага.

Откако дознал за нарушувањето на безбедноста на личните податоци, контролорот мора веднаш и најдоцна во рок од 72 часа да поднесе известување за нарушувањата кои подлежат на таквата обврска. Во тој период контролорот треба да ја оцени веројатноста на ризикот за физичките лица за да утврди дали се исполнети услови за поднесување известување, како и дејствијата што треба да ги преземе за се справи со нарушувањето. Контролорот можеби веќе има направено иницијална оценка на потенцијалниот ризик од нарушувањето на безбедноста на личните податоци како дел од спроведената проценка на влијанието врз заштитата на личните податоци (ПВЗЛП) пред да почне со конкретната операција за обработка на лични податоци.

Сепак, треба да се има предвид дека направената проценка на влијанието може да биде поопшта споредено со конкретните околности на нарушувањето на безбедноста на личните податоци, па затоа контролорот треба да направи дополнителна оценка и да ги земе предвид конкретните околности на настанот.

Во повеќето случаи, ваквите прелиминарни дејствија треба да бидат завршени во краток период по иницијалниот аларм (т.е. кога контролорот или обработувачот се сомневаат дека настанал безбедносен инцидент кој може да се однесува и на личните податоци), но во исклучителни случаи тоа може да трае подолго.

Пример:

Едно лице го информира контролорот дека добил е-пошта во која некој се претставува како контролорот и која содржи лични податоци за неговото (реално) користење на услугите што ги дава контролорот, што упатува на фактот дека безбедноста на контролорот е компромитирана. Контролорот спроведува кратка истрага и утврдува упад во неговата мрежа и доказ за неовластено пристапување до личните податоци. Во тој момент се смета дека контролорот „дознал" за настанот и треба да понесе известување до надзорниот орган, освен доколку не постои веројатност дека тоа претставува ризик по правата и слободите на физичките лица. Во исто време, контролорот треба да преземе соодветни корективни мерки за да се справи со нарушувањето на безбедноста на личните податоци.

Од тие причини, контролорот треба да има воспоставено интерни постапки кои ќе му овозможат да открие и да се справи со нарушувањата на безбедноста на личните податоци. На пример, за да открие нерегуларности во обработката на личните податоци контролорот или обработувачот може да користат одредени технички мерки, како што се алатки за анализа на движењето на податоци и на записите/логовите за пристапување до податоците, кои ќе им овозможат да ги дефинираат настаните и алармите преку споредување на податоците од записите за пристапување. Кога се открива нарушување на безбедноста на личните податоци, важно е истото да се пријави до соодветното раководно ниво за да биде соодветно адресирано и за да се понесе известување, кога тоа е потребно, во согласност со член 37 и/или со член 38 од ЗЗЛП. Ваквите мерки и механизми за пријавување треба да бидат детално утврдени во плановите за справување со инциденти и/или аранжманите за управување што ги усвојува контролорот. Тие помагаат за ефективно планирање и утврдување на одговорноста во рамките на организацијата во врска со управувањето со нарушувањето на безбедноста на личните податоци, и како или дали инцидентот може да ескалира.

Контролорот треба да има утврдено аранжмани со обработувачот/обработувачите кои ги ангажирал и кои се должни да го известат во случај на нарушување на безбедноста на личните податоци. Иако контролорите и обработувачите се одговорни за примена на соодветни мерки за спречување, реагирање и справување со нарушувањата на безбедноста на личните податоци, подолу се наведени неколку практичните чекори што треба да се преземат во сите случаи:

- информациите за сите настани поврзани со безбедноста се доставуваат до одговорното лице/лица чиишто работни задачи вклучуваат справување со инциденти, утврдување на нарушување на безбедноста на личните податоци и оценување на ризикот;
- потоа се оценува ризикот за физичките лица кој е резултат од нарушувањето на безбедноста на личните податоци (веројатноста, т.е. нема ризик, ризик или висок ризик) и се информираат соодветните оддели во рамките на организацијата;

- се поднесува известување до надзорниот орган и, ако е потребно, се информираат засегнатите физички лица за нарушувањето на безбедноста на личните податоци;
- во исто време контролорот презема дејствија да го прекине и да го исправи нарушувањето на безбедноста на личните податоци;
- нарушувањето на личните податоци се документира паралелно со развојот на настаните и активностите.

Јасно е дека контролорот има обврска да постапи по сите иницијални аларми и да утврди дали навистина се случило нарушување на безбедноста на личните податоци. Овој краток период му дозволува да го истражи случајот и да собере докази и други релевантни информации за настанот. Сепак, откако контролорот утврдил, со разумно ниво на сигурност, дека се случило нарушување на безбедноста на личните податоци и доколку се исполнети условите од член 37 став (1) од ЗЗЛП, тој треба веднаш и најдоцна во рок од 72 часа да го извести надзорниот орган. Ако контролорот не го поднесе известувањето во дадениот временски рок и доколку е очигледно дека навистина се случило нарушување на безбедноста на личните податоци, тоа се смета за неусогласеност со одредбите за поднесување известување од член 37 од ЗЗЛП.

Одредбите од член 36 од ЗЗЛП јасно упатуваат на обврската на контролорите и обработувачите да применат соодветни технички и организациски мерки за да обезбедат ниво на безбедност на личните податоци што одговора на ризикот, односно мерки кои овозможуваат навремено откривање,

справување со и пријавување на нарушувањето на безбедноста на личните податоци, кои се сметаат за суштински елементи на овие мерки.

2.1.3. Заеднички контролори

Член 30 од ЗЗЛП се однесува на заеднички контролори и пропишува дека тие заеднички ги утврдуваат нивните одговорности за постигнување усогласеност со законот. Тоа подразбира и распределба на одговорноста за усогласеност со одредбите од член 37 и член 38 од ЗЗЛП. Се препорачува договорот што го склучуваат заедничките контролори да содржи одредби кои определуваат кој од контролорите ќе биде одговорен за усогласеноста со обврските за поднесување известување за нарушување на безбедноста на личните податоци.

2.1.4. Обврски на обработувачот

Контролорот ја задржува севкупната одговорност за заштита на личните податоци, но обработувачот има важна улога во овозможувањето на контролорот да ги исполни неговите обврски коишто вклучуваат и известување за нарушување на безбедноста на личните податоци. Член 32 став (3) од ЗЗЛП утврдува дека обработката од страна на обработувачот се регулира со договор или со друг правен акт. Понатаму, член 32 став (3) алинеја ѓ) пропишува дека во договорот или другиот правен акт се регулира дека обработувачот „му помага на контролорот да обезбеди усогласеност со членовите 36 до 40 од овој закон, земајќи ги предвид природата на обработка и информациите кои му се достапни на обработувачот“.

Член 37 став (2) од ЗЗЛП јасно утврдува дека откако обработувачот дознал за нарушување на безбедноста на личните податоци, тој треба „веднаш“ да го извести контролорот за истото. Треба да се нагласи дека обработувачот не треба прво да ја оцени веројатноста дали нарушувањето ќе резултира во ризик пред да го извести контролорот, туку контролорот е тој што ја прави оваа оценка откако ќе дознае за нарушувањето на безбедноста на личните податоци. Со други зборови, обработувачот треба да утврди дали се случило нарушување на безбедноста на личните податоци и да го извести контролорот. Контролорите користат обработувачи за да ги постигнат своите цели на обработка, па затоа се смета дека контролорот „дознал“ за нарушувањето на безбедноста откако бил известен за истото од страна на обработувачот. Обврската на обработувачот за известување му овозможува на контролорот да се справи со нарушувањето на безбедноста на личните податоци и да утврди дали има потреба за доставување известување до надзорниот орган во согласност со член 37 став (1) и до засегнатите физички лица во согласност со член 38 став (1) од ЗЗЛП. Контролорот може да го истражи нарушувањето бидејќи обработувачот не е во позиција да ги знае сите релевантни факти за конкретната ситуација, на пример, кога контролорот има копија или резервна копија од личните податоци кои биле уништени или загубени од страна на обработувачот. Тоа може да влијае врз одлуката на контролорот дали треба да поднесе известување. ЗЗЛП не пропишува временски рок во кој обработувачот мора да го алармира контролорот, освен тоа дека контролорот треба да биде известен „веднаш“.

Затоа, се препорачува обработувачите веднаш да ги известат контролорите и постепено да обезбедат дополнителни информации за нарушувањето на безбедноста на личните податоци, откако таквите информации ќе станат достапни.

Ова е важно и им помага на контролорите да ја исполнат обврската за поднесување известување до надзорниот орган во рок од 72 часа. Како што беше наведено погоре, договорот меѓу контролорот и обработувачот треба да го прецизира начинот на кој се исполнуваат барањата од член 37 став (2) дополнително на другите одредби од ЗЗЛП. Тоа може да вклучи барање за рано известување од страна на обработувачот во поддршка на обврската на контролорот за известување на надзорниот орган во рок од 72 часа. Кога обезбедува услуги за повеќе контролори кои се засегнати од ист инцидент, обработувачот треба да ги извести сите контролори одделно за деталите на настанот.

Обработувачот може да го поднесе известувањето во име на контролорот кога за тоа има претходно овластување и кога тоа е дел од договорот меѓу контролорот и обработувачот. Ваквото известување мора да се достави во согласност со член 37 и член 38 од ЗЗЛП. Сепак, треба да се запомни дека законската обврска за известување останува кај контролорот.

2.2.Обезбедување информации на АЗЛП

2.2.1.Информации што треба да се обезбедат

Согласно член 37 став (3) од ЗЗЛП, при поднесување на известувањето до надзорниот орган, контролорот треба, како минимум, да ги обезбеди следниве информации:
(а) опис на природата на нарушувањето на безбедноста на личните податоци, вклучително и категориите и приближниот број на засегнати субјекти на лични податоци, како и категориите и приближниот број на засегнати збирки на лични податоци;
(б) име/презиме и контакт деталите на офицерот за заштита на личните податоци или друго лице за контакт од кое може да се добијат повеќе информации;

(в) опис на можните последици од нарушувањето на безбедноста на личните податоци;
(г) опис на преземените или предложените мерки од страна на контролорот за справување со нарушување на безбедноста на личните податоци, вклучително и соодветни мерки за намалување на можните негативни ефекти.

ЗЗЛП не ги дефинира категориите на субјекти на лични податоци или категориите на записи на лични податоци. Сепак, се препорачува контролорите да ги наведат категориите на субјекти на лични податоци како упатување за разните физички лица чиишто податоци се засегнати со нарушувањето на безбедноста: во зависност од дескрипторите што се користат, меѓу другото, тие може да вклучат деца и ранливи групи, лица со попреченост, вработени или клиенти. И записите на лични податоци може да упатуваат на разни информации коишто контролорот ги обработува, како што се: податоци поврзани со здравјето, образовни записи, информации за социјална заштита, финансиски информации, банкарски сметки, број на пасош и друго.

Недостапноста на прецизни информации (на пр., точниот број на засегнати субјекти на лични податоци) не треба да биде пречка за навремено доставување на известувањето за нарушување на безбедноста на личните податоци. ЗЗЛП дозволува давање приближни информации во однос на бројот на засегнати физички лица и бројот на записи на лични податоци. Фокусот треба да биде на справување со негативните ефекти од нарушувањето наместо на обезбедување прецизни бројки. Оттука, кога е јасно дека се случило нарушување на безбедноста на личните податоци, но сè уште не се знае опфатот на истото, за да ја исполни обврската за известување најбезбедно е контролорот да поднесе известување во фази (види подолу).

Член 37 став (3) од ЗЗЛП пропишува дека известувањето мора да обезбеди минимум информации пропишани со законот, а контролорот може да одлучи да достави дополнителни детали, кога тоа е потребно. Различни видови на известувања за нарушување на безбедноста на личните податоци (доверливост, интегритет или достапност) може да наложат доставување дополнителни информации за целосно објаснување на околностите во секој случај посебно.

Важно: Како дел од известувањето до АЗЛП, контролорот може да смета дека е корисно да го наведе името на обработувачот доколку изворот на нарушувањето на безбедноста на личните податоци е лоциран кај обработувачот, особено доколку тоа довело до инцидент кој ги засега и збирките на лични податоци на други контролори кои ги користат услугите на обработувачот.

Во секој случај, надзорниот орган може да побара повеќе детали како дел од истрагата што ја спроведува за нарушувањето на безбедноста на личните податоци.

2.2.2.Известување во фази

Во зависност од природата на нарушувањето на безбедноста на личните податоци, контролорот може да смета дека е потребно да се спроведе натамошна истрага за утврдување на сите релевантни факти кои се однесуваат на инцидентот. Конкретно, член 37 став (4) од ЗЗЛП пропишува:

„Кога и само доколку контролорот не може истовремено да ги достави сите информации, тие може да се обезбедат постепено (во фази) без понатамошно одлагање.“

Тоа значи дека ЗЗЛП признава дека контролорот нема секогаш да ги има сите потребни информации за нарушувањето на безбедноста на личните податоци во рокот од 72 часа откако дознал за истото бидејќи во иницијалниот период не се достапни целосни и сеопфатни детали за инцидентот и, од тие причини, дозволува известувањето да се достави во фази (постепено). Веројатно е дека ова ќе биде случај со посложените нарушувања на безбедноста на личните податоци, како што се видови на кибер-инциденти кои налагаат подетална форензичка истрага за целосно да се утврди природата на нарушувањето и степенот на компромитација на личните податоци. Последователно, во многу случаи контролорот ќе треба дополнително да го истражи нарушувањето и да достави дополнителни информации во подоцнежна фаза. Ваквото известување е дозволено, но само доколку контролорот ги образложи причините за доцнењето во согласност со член 37 став (1) од ЗЗЛП. Затоа се препорачува контролорот прво да го достави известувањето до АЗЛП дури и кога сè уште ги нема потребните информации и да информира дека повеќе детали ќе бидат доставени подоцна. АЗЛП треба да одреди како и кога треба да се достават дополнителните информации. Тоа не го спечува контролорот да обезбеди натамошни информации во која било друга фаза доколку дознал дополнителни детали кои се релевантни за нарушувањето на безбедноста на личните податоци и кои треба да се достават до АЗЛП.

Фокусот на обврската за известување за нарушувањето на личните податоци е да ги поттикне контролорите брзо да дејствуваат и да го прекинат нарушувањето, да ги повратат компромитираните лични податоци кога тоа е можно, и да побараат совет од АЗЛП. Известувањето на АЗЛП во првите 72 часа му овозможува на контролорот да се осигури дека одлуката дали има потреба да се известат и физичките лица е правилна.

Сепак, целта на известувањето на АЗЛП не е само да се добијат насоки за тоа дали треба да се информираат и засегнатите физички лица. Во некои случаи, поради природата на нарушувањето и сериозноста на ризикот контролорот треба веднаш да ги информира и засегнатите физички лица. На пример, доколку постои непосредна закана за кражба на идентитет или доколку посебни категории на лични податоци се откриени онлајн, контролорот треба веднаш да преземе дејствија да го прекине нарушувањето на безбедноста и да ги извести засегнатите физички лица. Во исклучителни околности, информирањето на физичките лица може да се случи пред известувањето на надзорниот орган. Генерално, известувањето до АЗЛП не смее да биде оправдување за неинформирање на субјектите на лични податоци за нарушувањето на безбедноста на личните податоци, кога тоа е потребно.

Јасно е дека по поднесувањето на првичното известување, контролорот може да достави ажурирани информации до АЗЛП доколку последователната истрага што ја спровел открила докази дека безбедносниот инцидент е прекинат и не се случило нарушување на безбедноста на личните податоци. Потоа овие информации може да ги дополнат информациите што веќе се дадени на АЗЛП и да се заведе дека инцидентот не претставувал нарушување на безбедноста на личните податоци. ЗЗЛП не пропишува санкции за пријавување на инцидент за кој на крајот е утврдено дека не претставува нарушување на безбедноста на личните податоци.

Пример:

Контролорот го известува надзорниот орган во рок од 72 часа по откривањето на нарушување на безбедноста на личните податоци поради губење на УСБ уред на кој се чуваат лични податоци на дел од клиентите. Подоцна се открива дека УСБ уредот бил одложен на погрешно место во просториите на контролорот. Контролорот го известува надзорниот орган за истото и бара измена на претходното известување.

2.2.3.Задоцнето известување

Член 37 став (1) од ЗЗЛП јасно одредува дека кога до надзорниот орган не е доставено известување во рок од 72 часа, истото треба да биде придружено со објаснување за задоцнувањето. Тоа, заедно со концептот за постепено известување (во фази), го признава фактот дека контролорите нема секогаш да бидат во можност да достават известување во дадениот временски период, и затоа се дозволува задоцнето известување.

На пример, такво сценарио може да се случи кога, во краток временски период, контролорот се соочува со повеќе слични нарушувања на доверливоста на личните податоци коишто на ист начин влијаат врз голем број субјекти на лични податоци. Контролорот може да дознае за некое нарушување и, додека ја почнува својата истрага, а пред да го поднесе известувањето, утврдува последователни слични нарушувања од различна причина. Во зависност од околностите, на контролорот може да му треба одредено време за да го утврди обемот на нарушувањата и, наместо да поднесе известување за секое нарушување одделно, контролорот организира значајно известување кое опфаќа неколку многу слични нарушувања, но од различна причина. Тоа може да доведе до одложување на известувањето до надзорниот орган за повеќе од 72 часа откако контролорот прво дознал за таквите нарушувања на безбедноста на личните податоци.

Генерално, секое посебно нарушување на безбедноста на личните податоци е инцидент што треба посебно да се пријави. Сепак, за да се избегне преголемо оптоварување, контролорите може да поднесат „споено“ известување што ги опфаќа сите нарушувања, под услов тие да се однесуваат на ист вид на нарушена безбедност на личните податоци во релативно краток временски период. Ако се случила серија на нарушувања кои се однесуваат на различни видови

на лични податоци, но нарушувањето настанало на поинаков начин, тогаш известувањето треба да се поднесе на стандардниот начин, односно секое нарушување се пријавува посебно во согласност со член 37.

Иако ЗЗЛП дозволува одложување на известувањето до одреден степен, тоа не треба да се смета за нешто што редовно се случува. Треба да се нагласи дека групирањето на известувања може да се направи и за повеќе слични нарушувања кои се пријавуваат во рок од 72 часа.

2.3.Услови кога не е потребно известување за нарушување на безбедноста на личните податоци

Член 37 став (1) од ЗЗЛП јасно наведува дека кога “не постои веројатност нарушувањето на безбедноста на личните податоци да резултира во ризик по правата и слободите на физичките лица“, тогаш нема потреба за доставување известување до АЗЛП. Пример за тоа може да биде ситуација во која личните податоци се веќе јавно достапни и откривањето на тие податоци не подразбира ризик за физичките лица.

Нарушување на доверливоста на личните податоци кои биле криптирани со најсовремена технологија сепак претставува нарушување на безбедноста на личните податоци и за истото треба да се поднесе известување. Сепак, доколку доверливоста на клучот за декриптирање не е променета, односно клучот не е компромитиран како дел од нарушувањето на безбедноста и бил генериран на начин кој не дозволува пристапување до податоците со достапни технолошки средства од страна на лице кое нема такво овластување, податоците во принцип се нечитливи. Оттука, не е веројатно дека нарушувањето на безбедноста на личните податоци ќе има негативен ефект врз физичките лица и затоа нема потреба тие да бидат информирани.

Сепак, дури и кога личните податоци се криптирани, нивното губење или менување може да има негативни последици за субјектите на лични податоци ако контролорот нема соодветна резервна копија. Во таков случај, субјектите на лични податоци треба да бидат информирани, дури и кога се применети соодветни мерки за криптирање на податоците.

Тоа ќе биде случај и кога лични податоци, како што се лозинки, не се безбедно обработени со функцијата за разбивање и солење (hashing and salting), при што хеш-вредноста е пресметана со најнова криптографска функција за клучеви, клучот што се користел за разбивањето не бил компромитиран со нарушувањето и клучот што се користел за разбивање на податоците бил генериран на начин на кој не може да биде пробиен со достапни технолошки средства од страна на лице кое нема такво овластување.

Следствено, ако личните податоци биле направени нечитливи за неовластени страни и кога податоците се копија или постои резервна копија од истите, за нарушувањето на доверливоста на соодветно криптирани лични податоци не мора да се поднесе известување до надзорниот орган. Известувањето не е потребно бидејќи не постои веројатно дека нарушувањето претставува ризик по правата и слободите на личните податоци. Секако, тоа значи дека и физичките лица не треба да бидат информирани бидејќи не постои висок ризик. Сепак, треба да се има предвид дека, иако на почетокот немало потреба за известување поради непостоење веројатност за појава на ризик по правата и слободите на физичките лица, тоа може да се смени со текот на времето и ризикот треба одново да се оцени. На пример, ако подоцна се открие дека клучот бил компромитиран или ако се открие одредена ранливост на софтверот за крипитирање, контролорот сепак може да има обврска за известување.

Треба да се забележи дека доколку се случи нарушување на безбедноста на личните податоци и не постои резервна копија од криптираните податоци, тогаш станува збор за нарушување на достапноста на личните податоци што може да предизвика ризици за физичките лица и потребно е тие да бидат известени. Слично, кога нарушувањето вклучува губење на криптирани лични податоци и постои резервна копија од личните податоци, тоа треба да подлежи на обврската за известување во зависност од времето кое е потребно за повратување на податоците од резервната копија и ефектот од недостапноста на личните податоци врз физичките лица. Според член 36 став (1) алинеја в) од ЗЗЛП, важен фактор за безбедноста на личните податоци е „способноста за навремено повратување на достапноста на личните податоци и пристапот до нив во случај на физички или технички инцидент".

Пример:

Нарушување на безбедноста на личните податоци што не налага известување до АЗЛП може да биде губење на безбедно криптиран мобилен уред што го користи контролорот и неговиот персонал. Под услов клучот за декриптирање да останал во безбедна сопственост на контролорот и тоа да не е единствената копија на личните податоци, напаѓачот нема да може да пристапи до нив. Тоа значи дека не постои веројатност нарушувањето да резултира во ризик по правата и слободите на засегнатите субјекти на лични податоци. Доколку подоцна стане очигледно дека клучот за декриптирање бил компромитиран или дека софтверот/ алгоритамот за криптирање е ранлив, ризикот по правата и слободите на физичките лица ќе се смени и во таква ситуација може да постои обврска за известување.

Сепак, ако контролорот не ја извести АЗЛП во ситуација кога податоците не биле безбедно криптирани, тогаш се смета дека тој не ја исполнил обврската од член 37 од ЗЗЛП. Од тие причини, кога го избираат софтверот за криптирање контролорите треба внимателно да го оценат квалитет и соодветната примена на

понуденото криптирање, да го разберат нивото на заштита што тоа го обезбедува и дали тоа ниво е соодветно на ризиците кои постојат. Контролорите треба да бидат запознаени и со спецификите на нивниот производ за криптирање. На пример, еден уред може да биде криптиран откако е исклучен, но не додека е во состојба на мирување. Некои производи за криптирање имаат „стандардни клучеви" кои треба да бидат сменети од клиентот за да бидат ефективни. Експертите за безбедност може да сметаат дека, во даденият момент, криптирањето е соодветно, но истото може да стане застарено за неколку години и го отвора прашањето дали податоците ќе бидат доволно криптирани/безбедни со даденият производ и дали тој обезбедува соодветно ниво на заштита.

3.Член 38: Информирање на субјектите на лични податоци

3.1. Информирање на физичките лица

Во одредени случаи, освен известувањето до надзорниот орган, контролорот треба да ги информира и засегнатите физички лица за нарушувањето на безбедноста на личните податоци.

Член 38, став (1) од ЗЗЛП пропишува:

„Во случај на нарушување на безбедноста на личните податоци за кое постои веројатност дека ќе предизвика висок ризик по правата и слободите на физичките лица, контролорот веднаш го известува субјектот на лични податоци за нарушувањето.“

Контролорите треба да запомнат дека известувањето на АЗЛП е задолжително освен доколку не постои веројатност дека нарушувањето на безбедноста на личните податоци ќе резултира во ризик по правата и слободите на физичките лица. Освен тоа, кога постои веројатност дека нарушувањето на безбедноста на личните податоци ќе резултира во висок ризик по правата и слободите на физичките лица, и тие треба да бидат информирани. Оттука, прагот за информирање на физичките лица е повисок од оној за известување на АЗЛП и не сите нарушувања на безбедноста на личните податоци ја активираат обврската за информирање на физичките лица, со што контролорите се заштитени од непотребно оптоварување.

ЗЗЛП пропишува дека физичките лица треба „веднаш“ да се информираат за нарушувањето на безбедноста на личните податоци, што значи „најбрзо што може“. Главната цел на информирањето на физичките лица е да се обезбедат конкретни информации за чекорите што тие треба да ги преземат за да се заштитат. Како што беше наведено погоре, во зависност од природата на нарушувањето на безбедноста на личните податоци и поврзаниот ризик, навременото информирање на физичките лица ќе им помогне да преземат чекори за да се заштитат од негативните последици што може да произлезат од нарушувањето.

3.2. Информации што треба да се обезбедат

При информирање на физичките лица, член 38 став (2) од ЗЗЛП пропишува дека:

„Во известувањето до субјектите на лични податоци од ставот (1) на овој член, на јасен и едноставен јазик се опишува природата на нарушувањето на безбедноста на личните податоци и, како минимум, се наведуваат информациите и мерките наведени во член 37 став (3) точки б), в) и г) од овој закон.“

Според оваа одредба, контролорот треба да ги обезбеди следниве информации:

- опис на природата на нарушувањето на безбедноста на личните податоци;
- име и контакт детали на офицерот за заштита на личните податоци или друго лице за контакт;
- опис на веројатните последици од нарушувањето на безбедноста на личните податоци; и
- опис на мерките што биле преземени или ќе се преземат од страна на контролорот за справување со нарушувањето, вклучително и соодветни мерки за намалување на можните негативни ефекти.

Како пример за мерки што се преземаат за справување со нарушувањето на безбедноста на личните податоци и за намалување на можните негативни ефекти кои контролорот ги наведува во известувањето може да биде тоа дека, по поднесување на известување до АЗЛП, тој добил совети за управување со нарушувањето и намалување на неговото влијание. Исто така, контролорот може да обезбеди конкретни совети за физичките лица, кога тоа е соодветно, за тие да се заштитат од можните негативни последици од нарушувањето на безбедноста на личните податоци,

на пример: промена на лозинката во случај кога се компромитирани нивните податоци за најавување. Треба да се нагласи дека контролорот може да одлучи да обезбеди и дополнителни информации од оние утврдени со оваа одредба.

3.3. Контактирање на физичките лица

Во принцип, засегнатите субјекти на лични податоци треба да бидат директно информирани за релевантното нарушување на безбедноста на личните податоци, освен доколку тоа не подразбира несразмерен напор од страна на контролорот. Во таков случај, контролорот може да објави јавно соопштение или да примени некоја друга мерка со која субјектите на лични податоци се информирани на еднакво ефективен начин (член 38 став (3) точка в) од ЗЗЛП).

При информирање на субјектите на лични податоци треба да се користат наменски пораки и тие не треба да бидат испратени заедно со други информации, како што се редовни ажурирања, информатори или стандардни пораки. На тој начин, информирањето за нарушувањето на безбедноста на личните податоци е јасно и транспарентно.

Примери за транспарентни методи на информирање вклучуваат директни пораки (на пр., е-пошта, СМС, итн.), истакнати банери или известувања на веб-страницата, комуникација преку пошта или истакнати огласи во печатените медиуми. Известување кое е дел од соопштение за јавноста или корпоративен блог не се смета за ефективно средство за информирање на физичките лица за нарушување на безбедноста на личните податоци. Се препорачува контролорите да изберат средства кои ги максимизираат шансите за соодветно пренесување на информациите до сите засегнати физички лица. Во зависност од околностите, тоа може да значи користење на неколку методи на комуникација, наместо еден канал за контакт.

Исто така, контролорите треба да се осигурат дека известувањето е достапно во соодветен алтернативен формат и на релевантните јазици за да се обезбеди дека физичките лица ги разбираат информациите што им се даваат. На пример, генерално се смета дека јазикот што се користел за време на претходните редовни деловни комуникации со физичките лица не е соодветен за информирање на лицата за нарушувањето на безбедноста на личните податоци.
Од клучно значење тука е да им се помогне на субјектите на лични податоци да ја разберат природата на нарушувањето и чекорите што може да ги преземат за да се заштитат.

Контролорите се во најдобра позиција да го утврдат најсоодветниот канал за информирање на физичките лица за нарушувањето на безбедноста на личните податоци, особено доколку тие се често во контакт со нивните клиенти. Сепак, јасно е дека контролорот треба да внимава да не ги користи каналите за комуникација кои биле компромитирани со нарушувањето на безбедноста бидејќи и тие канали може да бидат користени од страна на напаѓачите кои се претставуваат како контролорот.
Од тие причини, контролорите може да ја контактираат и да се консултираат со АЗЛП, не само за да побараат совет во врска со информирањето на субјектите на лични податоци за нарушувањето согласно член 38 од ЗЗЛП, туку и за соодветната порака што треба да се испрати и за соодветниот начин за контактирање на физичките лица.

Секогаш кога контролорот не е во можност да ги извести физичките лица за нарушувањето на безбедноста на личните податоци бидејќи нема доволно контакт информации за нив, тој треба да ги информира веднаш откако ќе се создадат услови за истото (на пр., кога едно физичко лице го остварува неговото/нејзиното право за пристап до личните податоци и притоа на контролорот му ги обезбедува потребните дополнителни информации за контакт).

Правилникот за начинот на известување за нарушување на безбедноста на личните податоци („Службен весник на Република Северна Македонија" бр. 122/20) содржи обрасци за известување за нарушување на безбедноста на личните податоци до субјектите на лични податоци и до Агенцијата, и истиот е достапен на веб-страницата на АЗЛП.

3.4. Услови кои не налагаат информирање на физичките лица

Во член 38 став (3) од ЗЗЛП се дадени три услови кои, доколку се исполнети, не ја активираат обврската за известување на физичките лица во случај на нарушување на безбедноста на личните податоци: односно:

- кога контролорот применил соодветни технички и организациски мерки за заштита и таквите мерки биле применети на личните податоци кои се засегнати од нарушувањето на безбедноста на личните податоци, особено мерки кои ги прават личните податоци неразбирливи за секое лице кое нема овластување за пристап до нив, како што е криптирање;
- кога контролорот применил дополнителни мерки кои гарантираат дека веќе не постои веројатност за појава на висок ризик по правата и слободите на субјектите на лични податоци од ставот (1) на овој член;
- кога известувањето налага несразмерен напор од страна на контролорот. Во таков случај се врши јавно известување или се применува друга слична мерка со која субјектите на личните податоци се информирани на еднакво ефикасен начин.

Согласно начелото за отчетност, контролорот треба да биде во можност да ѝ покаже на АЗЛП дека исполнува еден или повеќе од овие услови. Треба да се нагласи дека, иако иницијално можеби нема потреба за какво известување бидејќи не постои ризик по правата и слободите на физичките лица, таквата ситуација може да се смени со

текот на времето и затоа треба да се направи повторна оценка на ризикот.

Доколку контролорот одлучи да не ги информира физичките лица за нарушувањето на безбедноста на личните податоци, член 38 став (4) од ЗЗЛП пропишува дека АЗЛП може да го побара истото кога смета дека постои веројатност нарушувањето да резултира со висок ризик за субјектите на лични податоци. Алтернативно, АЗЛП може да утврди дека се исполнети условите од член 38, став (3) и дека нема потреба за известување на физичките лица. Доколку надзорниот орган утврди дека одлуката на контролорот да не ги информира субјектите на лични податоци е неоснована, тој може да размисли за примена на своите овластувања и за изрекување санкции.

4.Оценување на ризик и висок ризик

4.1. Ризикот како активатор на обврската за известување

Иако ЗЗЛП воведува обврска за известување за нарушување на безбедноста на личните податоци, тоа не е задолжително во сите околности:

- известување до надзорниот орган треба да се поднесе, освен во случај кога не е веројатно дека нарушувањето ќе резултира во ризик по правата и слободите на физичките лица;
- информирање на физичките лица за нарушувањето е потребно само кога постои веројатност дека тоа ќе резултира во висок ризик по нивните права и слободи.

Тоа значи дека веднаш откако дознал за нарушувањето на безбедноста на личните податоци, од клучно знаење е контролорот не само да се обиде да го прекине инцидентот, туку и да го оцени ризикот што може да произлезе од таквиот инцидент. Постојат две важни причини за тоа: прво, знаењето за веројатноста и потенцијалната сериозност на влијанието врз физичките лица може да му помогне на контролорот да преземе ефективни чекори за да го прекине и да се справи со нарушувањето, и второ, тоа ќе му помогне да утврди дали треба да поднесе известување до надзорниот орган и, ако е потребно, до засегнатите физички лица.

Како што беше наведено претходно, известување за нарушување на безбедноста на личните податоци е потребно освен доколку не е веројатно тоа да резултира во ризик по правата и слободите на физичките лица, при што клучен фактор за информирање на субјектите на лични податоци е веројатноста дека нарушувањето на безбедноста на личните податоци ќе резултира во висок ризик по правата и слободите на физичките лица. Ваков ризик постои кога нарушувањето може да доведе до физичка, материјална или нематеријална штета за физичките лица чиишто лични податоци се засегнати со нарушувањето на безбедноста.

Примери за таква штета се дискриминација, кражба на идентитет или идентитетска измама, финансиска загуба или нарушување на угледот.

Кога нарушувањето вклучува лични податоци кои откриваат расно или етничко потекло, политички ставови, верски или религиозни убедувања, или членство во синдикати, или кога вклучува генетски податоци, податоци поврзани со здравјето или со сексуалниот живот, или со кривични дела и кривични осуди, или податоци поврзани со безбедносни мерки, таквата штета треба да се смета за веројатна.

4.2. Фактори што треба да се земат предвид при оценување на ризикот

Треба да се има превид дека оценувањето на ризикот по правата и слободите на физичките лица кој е резултат од нарушување на безбедноста на личните податоци има различен фокус од ризикот што се разгледува како дел од проценката на влијанието врз заштитата на личните податоци (ПВЗЛП). Проценката на влијанието предвид ги зема и ризиците од планираната обработка на личните податоци и ризиците кои се јавуваат во случај на нарушување на безбедноста. При разгледувањето на потенцијално нарушување на безбедноста на личните податоци, проценката на влијанието ги разгледува ризиците погенерално и во однос на нивната веројатност, како и во однос на штетата што може да настане за субјектите на лични податоци. Со други зборови, тоа е проценка на хипотетички настан. Кога станува збор за реално нарушување на безбедноста на личните податоци, настанот веќе се случил и затоа фокусот е целосно ставен на резултатниот ризик што го произведува нарушувањето врз физичките лица.

Пример:
ПВЗЛП сугерира дека предложеното користење на конкретен безбедносен софтверски производ за заштита на личните податоци претставува соодветна мерка која обезбедува ниво на безбедност што одговора на ризикот по физичките лица од самата обработка. Сепак, доколку подоцна се открие ранливост на таквиот производ,

тоа ја менува соодветноста на софтверот за ограничување на ризикот по заштитените лични податоци и затоа истиот треба повторно да се оцени како дел од тековна (нова) проценка на влијанието врз заштитата на личните податоци. Подоцна, ваквата ранливост на производот е искористена и настанува нарушување на безбедноста на личните податоци. Контролорот треба да ги оцени конкретните околности на нарушувањето, засегнатите податоци, и потенцијалното ниво на влијание врз физичките лица, како и веројатноста таквиот ризик да се материјализира.

Се препорачува оценката да ги земе превид следниве елементи:

- **Видот на нарушување на безбедноста на личните податоци**

Видот на нарушувањето на безбедноста на личните податоци што се случило може да влијание врз нивото на ризикот по физичките лица. На пример, нарушување на доверливоста при што медицински информации се откриени на неовластени страни може да има различни последици за некое физичко лице отколку нарушување на безбедноста што подразбира губење или недостапност на медицинското досие на лицето.

- **Природата, осетливоста и обемот на личните податоци**

Се разбира дека видот и осетливоста на личните податоци кои се компромитирани со нарушувањето на безбедноста се клучен фактор во оценката на ризикот. Колку е поголема осетливоста на податоци, толку е повисок ризикот за нанесување штета на лицата кои се засегнати, но предвид треба да се земат и другите лични податоци на субјектот кои можеби се веќе достапни. На пример, мала е веројатноста дека откривањето на името и адресата на некое лица во нормални околности ќе предизвика значителна штета. Сепак, ако името и адресата на родителот-посвоител се откријат на биолошкиот родител, последиците може да биде многу сериозни и за посвоителот и за детето.

Нарушувањата кои вклучуваат податоци за здравјето, документи за лична идентификација, или финансиски податоци, на пример број на кредитна картичка, сами по себе може да предизвикаат штета, но кога се користат заедно може да доведат и до кражба на идентитет. Обично, комбинација на лични податоци е поосетлива од единечен личен податок.

На прв поглед, некои видови на лични информации може да се чинат релативно безбедни, но сепак внимателно треба да се размисли за она што податоците може да откријат за засегнатото лице. Список на клиенти кои добиваат редовна испорака можеби нема да се смета за посебно осетлив податок, но истите податоци за клиентите кои побарале испораката да биде стопирана додека се на одмор може да биде корисна информација за криминалци.

Слично на тоа, мал обем на високо осетливи лични податоци може да има големо влијание врз некое лице, и голем обем на детали може да открие широк спектар на информации за тоа лице. Исто така, нарушување на безбедноста кое се однесува на голем обем на лични податоци за голем број субјекти на лични податоци може да влијае врз соодветно голем број на физички лица.

- **Лесна идентификација на физички лица**

Важен фактор што треба да се разгледа е леснотијата со која некоја страна што има пристап до компромитираните лични податоци може да идентификува одредени лица или да ги комбинира податоците со други информации за идентификација на некое лице. Во зависност од околностите, идентификација е можна директно од личните податоци чијашто безбедност е нарушена без посебно истражување за откривање на идентитетот на лицето, или пак може да биде исклучително тешко личните податоци да се поврзат со конкретно лице, но сепак можно во одредени услови. Можна е директна или

индиректна идентификација од личните податоци чијашто безбедност е нарушена, но тоа може да зависи од конкретниот контекст на нарушувањето и јавната достапност на поврзани лични детали.

Оваа ситуација е порелевантна во случај нарушување на доверливоста и достапноста на личните податоци.

Како што беше наведено претходно, личните податоци кои се заштитени со соодветно ниво на криптирање ќе бидат нечитливи за неовластени лица кои немаат клуч за декриптирање. Освен тоа, соодветно спроведена псевдонимизација (дефинирана во член 4, точка 5) од ЗЗЛП како „обработка на лични податоци на таков начин што тие не можат повеќе да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да се предмет на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува“) може да ја намали веројатноста за идентификација на физичките лица во случај на нарушување на безбедноста на личните податоци. Сепак, исклучива примена на техники за псевдонимизација не може да се смета за претворање на личните податоци во нечитливи информации.

Сериозноста на последиците за физичките лица
Во зависност од природата на личните податоци кои се засегнати со нарушувањето на безбедноста, потенцијалната штета за физичките лица што е резултат од таквото нарушување може да биде прилично серозна, особено во случај кога нарушувањето може да резултира со кражба на идентитет или идентитетска измама, физичка повреда, психолошки стрес, понижување или нарушен углед. Ако

нарушувањето се однесува на лични податоци на ранливи лица, тие би биле ставени во поголем ризик од штета.

Свеста на контролорот за тоа дали личните податоци се во рацете на луѓе чиишто намери се непознати или можеби малициозни може да влијае врз нивото на потенцијалниот ризик. Може да станува збор за нарушување на доверливоста на личните податоци, при што тие по грешка се откриени на трета страна, онака како што е дефинирана во член 4, точка 10) од ЗЗЛП, или на друг корисник. Ова може да се случи, на пример, кога личните податоци случајно се испраќаат до погрешното одделение во рамките на една организација, или до добавувач кој обично се користи. Контролорот може да побара од корисникот да ги врати или безбедно да ги уништи податоците што му биле откриени. Во обата случаи, корисникот може да се смета за ентитет „од доверба“ со оглед на тоа дека контролорот има тековен однос со таа организација или може да биде запознаен со постапките, историјатот и други релевантни детали за корисникот.

Со други зборови, контролорот може да смета на одредено ниво на сигурност дека корисникот нема да ги чита или нема да пристапи до податоците кои биле испратени по грешка и дека ќе ги почитува инструкциите дадени од контролорот за враќање на податоците. Дури и кога корисникот пристапил до личните податоци, контролорот може да му верува дека нема да преземе друго дејство, веднаш ќе ги врати на контролорот и ќе соработува во насока на повратување на податоците. Во таков случај, фактот дека корисникот е ентитет од доверба може да се земе предвид во оценката на ризикот што ја спроведува контролорот по настанување на нарушувањето, што ја намалува сериозноста на последиците од

нарушувањето, но не значи дека не се случило нарушување на безбедноста на личните податоци. За возврат, тоа може да ја отстрани веројатноста за ризик по физичките лица, со што повеќе нема потреба за поднесување известување до надзорниот орган или до засегнатите физички лица. Треба да се нагласи, дека тоа ќе зависи од околностите во конкретниот случај. И покрај тоа, контролорот мора да ги чува информациите за нарушувањето како дел од општата должност за водење евиденција за нарушувањата на безбедноста на личните податоци.

Предвид треба да се земе и трајноста на последиците за физички лица, бидејќи влијанието може да се смета за поголемо ако ефектите од нарушувањето се долготрајни.

- **Посебни карактеристики на физичките лица**

Едно нарушување на безбедноста може да влијае на личните податоци на деца или други ранливи групи кои може да бидат изложени на поголем ризик од опасност како резултат на истото. Постојат и други фактори за физичките лица кои може да влијаат на нивото на ризик на кое се изложени поради нарушувањето на безбедноста на личните податоци.

- **Посебни карактеристики на контролорот**

Природата и улогата на контролорот и неговите активности може да влијае врз нивото на ризик за физичките лица кој е резултат на нарушување на безбедноста на личните податоци. На пример, медицинските установи обработуваат посебни категории на лични податоци, што значи дека постои поголема закана за физичките лица доколку е нарушена безбедноста на нивните лични податоци, за разлика од ситуација која вклучува мејлинг листа на некоја новинска организација.

- **Бројот на засегнати физички лица**

Нарушувањето на безбедноста на личните податоци може да влијае врз едно, неколку или врз неколку илјади физички лица, па и повеќе. Генерално, колку е повисок бројот на засегнатите физички лица толку е поголемо влијанието што може да го предизвика нарушувањето. Сепак, едно нарушување може да има сериозно влијание дури и врз само едно физичко лице во зависност од природата на личните податоци и контекстот во кој тие се компромитирани. Треба да се нагласи дека од клучно значење во овие случаи е да се утврди веројатноста и сериозноста на влијанието врз лицата кои се засегнати.

- **Општи поенти**

Од овие причини, при оценување на ризикот кој веројатно ќе произлезе од нарушувањето на безбедноста на личните податоци контролорот треба да ја земе предвид комбинацијата од сериозноста на потенцијалното влијание по правата и слободите на физичките лица и веројатноста тоа да се оствари. Јасно е дека кога последиците од нарушувањето се посериозни, ризикот е поголем. Слично, кога веројатноста за остварување на влијанието е поголема, постои поголем ризик. Кога не се сигурни, контролорите секогаш треба да постапат од страната на внимателност и да поднесат известување за нарушување на безбедноста на личните податоци

5.Отчетност и водење евиденција

5.1. Документирање на нарушувањата на безбедноста на личните податоци

Без оглед на тоа дали нарушувањето на безбедноста на личните податоци треба да биде пријавено до надзорниот орган, контролорот мора да води евиденција за сите нарушувања на безбедноста на личните податоци, што е пропишано во член 37 став (5) од ЗЗЛП:

„Контролорот ги документира сите нарушувања на безбедноста на личните податоци, вклучително и фактите поврзани со нарушувањето на безбедноста на личните податоци, нивните последици и преземените активности за справување со нарушувањето, а со цел да ѝ овозможи на Агенцијата да ја провери усогласеноста со овој член.“

Ова е поврзано со начелото за отчетност од законот, кое е дадено во член 9 став (2). Целта на водењето евиденција за нарушувањата кои не се пријавуваат, како и за нарушувањата кои мора да се пријават, е поврзана со обврските на контролорот дадени во член 28 од ЗЗЛП, при што надзорниот орган може да побара увид во таквата евиденција. Од таа причина, се советува контролорите да воспостават интерен регистар на нарушувања на безбедноста на личните податоци без оглед на тоа дали тие ја активираат обврската за известување или не.

Иако контролорот сам одлучува за методот и структурата на евиденцијата за документирање на нарушувања на безбедноста на личните податоци, кога станува збор за информациите кои треба да се заведат постојат неколку клучни елементи што треба да бидат вклучени во сите записи. Согласно член 37 став (5) од ЗЗЛП, контролорот треба да ги документира деталите поврзани со нарушувањето на безбедноста на личните податоци, што вклучува причина, време кога се случило нарушувањето и кои се засегнатите лични податоци. Исто така, евиденцијата треба да ги вклучи и ефектите и последиците од нарушувањето, заедно со корективните мерки што ги преземал контролорот.

ЗЗЛП не го прецизира рокот за чување на оваа документација. Кога ваквите записи содржат лични податоци, од контролорот се очекува да утврди соодветен рок за чување во согласност со начелата кои се однесуваат на обработка на личните податоци и треба да постои правен основ за обработката. Документацијата од член 37 став (5) од ЗЗЛП треба да се чува бидејќи АЗЛП може да побара од контролорот да достави докази за усогласеност со одредбите од тој член или генерално за усогласеноста со начелото за отчетност. Се разбира дека начелото за ограничување на рокот за чување не се применува доколку записите не содржат лични податоци.

Дополнително на овие детали, се препорачува контролорите да го документираат и сопственото резонирање за одлуките што ги донеле како одговор на нарушувањето на безбедноста на личните податоци. Конкретно, ако не се поднесе известување за нарушување, треба да се документира и оправдувањето за таквата одлука. Тоа треба да ги вклучи причините зошто контролорот смета дека не постои веројатност нарушувањето да резултира во ризик по правата и слободите на физичките лица. Алтернативно, ако контролорот смета дека се исполнети некои од условите дадени во член 38 став (3) од ЗЗЛП, тој треба да биде во можност да обезбеди соодветни докази за таквата одлука.

Кога контролорот поднесува известување за нарушувањето на безбедноста на личните податоци до АЗЛП, но истото е задоцнето, тој мора да биде во можност да ги наведе причините за доцнењето, односно треба да обезбеди документи кои покажуваат дека доцнењето на известувањето е оправдано и не е прекумерно.

Кога контролорот ги информира засегнатите физички лица за нарушувањето на безбедноста на личните податоци, тој треба да биде транспарентен за нарушувањето, при што таквата

комуникација треба да биде ефективна и навремена. Исто така, чувањето доказ од таквата комуникација му помага на контролорот во покажувањето отчетност и усогласеност.

За целите на усогласеност со член 37 и член 38, корисно е контролорите и обработувачите да имаат воспоставено документирана постапка за известување, односно да имаат утврдено процес кој ќе го следат по откривање на нарушувањето на безбедноста на личните податоци, што вклучува и постапки за изолирање, управување и решавање на инцидентот, како и за проценка на ризикот, и поднесување на известувањето. Во таа смисла, за да покажат усогласеност со законот, корисно е контролорите да бидат во можност да демонстрираат дека вработените се запознаени со таквите постапки и механизми и знаат како да реагираат при нарушување на безбедноста на личните податоци.

Треба да се нагласи дека неподнесување соодветен документ за нарушување на безбедноста на личните податоци може да доведе до активирање на овластувањата на АЗЛП согласно член 66 од ЗЗЛП и изрекување прекршочна глоба согласно член 110.

5.2. Улогата на офицерот за заштита на личните податоци

Контролорите и обработувачите може да имаат определено офицер за заштита на личните податоци согласно барањата од член 41 од ЗЗЛП или на доброволна основа, односно како добра практика. Член 43 од ЗЗЛП пропишува серија на задолжителни задачи за офицерите за заштита на личните податоци, но не ги ограничува контролорите да им доделат и други работни задачи, ако тоа е соодветно.

Во однос на известувањата за нарушување на безбедноста на личните податоци, задолжителните задачи на офицерите, меѓу

другото, вклучуваат давање совети и информации на контролорот или обработувачот, следење на усогласеноста со ЗЗЛП, и давање совети во врска со проценката на влијанието врз заштитата на личните податоци. Офицерите за заштита на личните податоци мора да соработуваат со АЗЛП и да дејствуваат како контакт точка за Агенцијата и за субјектите на лични податоци. Треба да се забележи дека, при поднесување известување за нарушување на безбедноста на личните податоци до надзорниот орган (АЗЛП), член 37 став (3) точка б) од ЗЗЛП налага контролорите да го наведат името и контакт деталите на нивниот офицер за заштита на личните податоци или друго лице кое е определено како контакт точка.

Од аспект на документирање на нарушувањата на безбедноста на личните податоци, контролорите или обработувачите може да побараат мислење од нивниот офицер во врска со структурата, организацијата и администрирањето на оваа документација. Офицерот за заштита на личните податоци може да има дополнителна задача поврзана со чувањето на ваквата евиденција.

Овие фактори упатуваат на тоа дека офицерот за заштита на личните податоци треба да има клучна улога преку давање помош за спречување или подготвеност за справување со нарушување на безбедноста на личните податоци преку совети или следење на усогласеноста, како и за време на нарушувањето (кога се известува АЗЛП) и за време на последователната истрага од страна на АЗЛП. Во таа насока, се препорачува офицерот за заштита на личните податоци веднаш да биде информиран за постоењето на нарушување на безбедноста на личните податоци и да биде вклучен во целата постапка за управување со нарушувањето и поднесување на известувањето за нарушување на безбедноста на личните податоци.

6. Примери за нарушување на безбедноста на личните податоци и кој треба да биде известен

Подолу е дадена неисцрпна листа со примери која ќе им помогне на контролорите да утврдат дали треба да поднесат известување во различни сценарија со нарушување на безбедноста на личните податоци. Овие примери може да помогнат во разграничување на тоа што е ризик, а што е висок ризик по правата и слободите на физичките лица.

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
1. Контролорот користи УСБ уред за чување на безбедносна копија од архивата на лични податоци кои се криптирани. УСБ уредот е украден при провала во просториите на контролорот.	Не	Не	Доколку личните податоци се криптирани со алгоритам според најновата технологија, постои резервна копија од личните податоци и единствениот клуч за декриптирање не е компромитиран, податоците може да се повратат за краток временски период и оваа ситуација не мора да се пријави како нарушување на безбедноста на личните податоци. Сепак, доколку подоцна тие станат компромитирани, тогаш контролорот мора да поднесе известување.

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
2. Контролорот нуди онлајн услуги, при што личните податоци на физичките лица (клиентите) се извлечени како резултат од кибер-напад на онлајн услугите.	Да, се поднесува известување до АЗЛП кога е веројатно дека ќе има последици за физичките лица.	Да, се поднесува известување до физичките лица во зависност од личните податоци кои се засегнати со овој напад и од степенот на веројатност за сериозни последици за физичките лица.	
3. Краток прекин на електрична енергија во времетраење од неколку минути во центарот за грижа за корисници на контролорот подразбира дека клиентите не се во можност да се јават на службите и да добијат пристап до нивните записи	Не	Не	Ова не претставува нарушување на безбедноста што треба да се пријави, но треба да биде документирано како инцидент во согласност со член 37 став (5) од ЗЗЛП. Контролорот треба да води соодветна евиденција за истото.

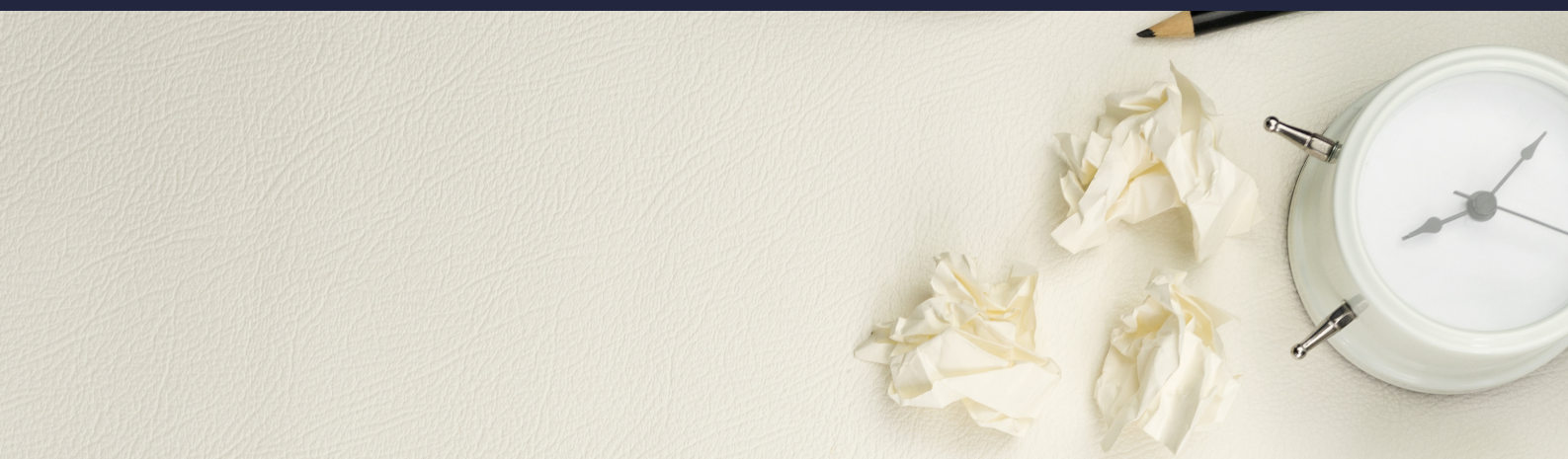
Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
4. Контролорот е нападнат со рансомвер што резултира во криптирање на сите податоци. Не постои резервна копија и податоците не може да се повратат. При истражување на настанот станува јасно дека единствената функција на нападот била криптирање на податоците, но во системот не постои друг малициозен софтвер.	Да, треба да се поднесе известување до АЗЛП доколку постои веројатност за последици по физичките лица бидејќи станува збор за загуба на достапноста на личните податоци.	Да, треба да се поднесе известување до физичките лица во зависност од природата на засегнатите лични податоци и можниот ефект од недостапноста на личните податоци, како и веројатноста за појава на други последици.	Доколку постои резервна копија од личните податоци и тие може да се повратат во догледно време, тогаш нема потреба за известување на АЗЛП и физичките лица бидејќи нема постојана загуба на достапноста или доверливоста на личните податоци. Сепак, доколку АЗЛП на друг начин е информирана за овој инцидент, таа може да размисли за истражување на случајот за да се оцени усогласеноста со мерките за безбедност на личните податоци согласно член 36 од ЗЗЛП.
5. Едно лице се јавува во центарот за информации на банката за да пријави нарушување на безбедноста на личните податоци. Лицето добило месечен извештај од банкарската сметка на некој друг.	Да	Се известуваат само засегнатите физички лица доколку постои висок ризик и јасно е утврдено дека другите не се засегнати.	Доколку по истрагата се утврди дека се засегнати повеќе лица, до АЗЛП мора да се испрати ажурирано известување и контролорот треба да преземе дополнителни чекори за известување на другите физички

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
Контролорот спроведува кратка истрага (која е завршена во период од 24 часа) и утврдува со разумна сигурност дека се случило нарушување на безбедноста на личните податоци и дека станува збор за системски недостаток кој може да значи дека и други лица се или може да бидат засегнати со истото.			лица кога постои висок ризик за нив
6. Контролорот има онлајн продавница и голем број клиенти. Онлајн продавницата е цел на кибер-напад при што напаѓачот на интернет ги објавува корисничките имиња, лозинките и историјатот на купени производи на клиентите на контролорот.	Да, се поднесува известување до АЗЛП	Да, се поднесува известување до субјектите на лични податоци бидејќи тоа може да доведе до висок ризик за нив.	Контролорот треба да преземе дејствија за намалување на ризикот, на пример, преку присилна промена на лозинките на засегнатите кориснички сметки, и други чекори. Контролорот треба да ги земе предвид и другите обврски за известување.

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
7. Компанија која обезбедува хостирање на ве-страници и дејствува како обработувач идентификувала грешка во кодот за контрола на овластувањата на корисниците. Ефектот од таквата грешка значи дека секој корисник може да пристапи до деталите за сметките на другите корисници.	Како обработувач, компанијата за хостирање на веб-страници мора веднаш и без одлагање да ги извести засегнатите клиенти (контролорите). Под претпоставка дека компанијата спровела сопствена истрага, засегнатите контролори треба да бидат разумно сигурни дали секој од нив претрпел нарушување на безбедноста на личните податоци и веројатно е дека секој од нив „дознал“ за истото откако бил известен од компанијата за хостирање на веб-страници (обработувачот). Потоа, контролорот мора да достави известување до АЗЛП.	Доколку не постои веројатност за висок ризик по физичките лица, тие не мора да бидат известени.	Компанијата за хостирање на веб-страници (обработувачот) мора да ги земе предвид и другите обврски за известување. Доколку нема докази дека оваа ранливост е искористена во однос на некој од контролорите што ги опслужува компанијата, може да се смета дека не се случило нарушување на безбедноста на личните податоци кое налага известување, но веројатно е дека треба да се документира или подразбира неусогласеност со член 36 од ЗЗЛП.

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
8. Поради кибер-напад, медицинските досиеја на една болница се недостапни во период од 30 часа.	Да, болницата е обврзана да поднесе известување бидејќи може да се јави висок ризик по добросостојбата и приватноста на пациентите.	Да, се известуваат засегнатите физички лица.	
9. По грешка, личните податоци на голем број студенти се испратени на погрешна мејлинг листа со повеќе од 1000 примателиа.	Да, се поднесува известување до надзорниот орган.	Да, се поднесува известување до физичките лица во зависност од обемот и видот на лични податоци кои се засегнати и сериозноста на можните последици.	
10. Директен маркетиншки е-мејл е испратен до примателиа во полето за видливи адреси наместо во полето за скриени адреси, со што сите можат да ги видат електронските адреси на другите примателиа.	Да, известување на надзорниот орган може да биде задолжително доколку се засегнати голем број физички лица, доколку се откриваат осетливи податоци	Да, физичките лица се известуваат во зависност од обемот и видот на засегнатите лични податоци и сериозноста на можните последици.	Известување можеби нема да биде потребно доколку не се откриени осетливи податоци или доколку се откриени само мал број на електронски адреси.

Пример	Известување на АЗЛП?	Известување на субјектите на лични податоци?	Белешки/ препораки
	(на пр., мејлинг листа на психотерапевт) или доколку други фактори претставуваат висок ризик (на пр., е-мејлот ја содржи иницијалната лозинка).		



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.

SCAN ME

+389 2 3230 635

info@privacy.mk

бул. „Гоце Делчев“ бр 18
Скопје

www.azlp.mk

Овој проект е финансиран од Европската Унија