РАБОТНА ГРУПА 29 ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

18/EN

WP250rev.01

Водич за известување за нарушување на безбедноста на личните податоци според Регулатива 2016/679

Усвоен на 3 октомври 2017

Последна измена и усвоен на 6 февруари 2018

Оваа Работна група е создадена под член 29 од Директивата 95/46/ЕУ. Таа е независно европско советодавно тело за заштита на личните податоци и приватноста. Нејзините задачи се опишани во член 30 од Директивата 95/46/ЕУ и член 15 од Директивата 2002/58/ЕУ.

Секретаријатот е обезбеден од Директоратот Ц (Основни права и државјанство на Унијата) на Европската комисија, Генерален директорат за правда, B-1049 Brussels, Belgium, Office No MO-59 03/075.

Веб-страница: http://ec.europa.eu/justice/data-protection/index_en.htm

РАБОТНАТА ГРУПА ЗА ЗАШТИТА НА ПОЕДИНЦИТЕ ВО ОДНОС НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

поставена од Директивата 95/46/ЕУ на Европскиот парламент и на Советот на 24 октомври 1995 година,

имајќи ги предвид членовите 29 и 30 од Директивата,

имајќи го предвид нејзиниот Правилник за работа,

ГИ УСВОИ СЛЕДНИВЕ НАСОКИ:

ТАБЕЛА НА СОДРЖИНА

ВОВЕД

Општата регулатива за заштита на личните податоци (ОРЗЛП) го воведува условот нарушувањето на безбедноста на личните податоци (оттука и понатаму „нарушување на безбедноста“) да биде известено пред националниот надлежен надзорен орган[1] (или во случај на прекугранично нарушување на безбедноста, до главниот орган) а, во одредени случаи, да им се соопшти нарушувањето на безбедноста на лицата чии лични податоци биле погодени од нарушувањето на безбедноста.

Обврските да се извести во случаи на нарушување на безбедноста моментално постои за одредени организации, како што се давателите на услуги на јавно достапна електронска комуникација (како што е наведено во Директивата 2009/136/ЕУ и Регулативата (ЕУ) бр. 611/2013)[2]. Исто така, постојат некои земји-членки на ЕУ кои веќе имаат своја национална обврска за известување за нарушување на безбедноста. Ова може да вклучува обврска да се извести за нарушувања на безбедноста кои вклучуваат категории на контролори, покрај давателите на услуги на јавно достапна електронска комуникација (на пример, во Германија и Италија), или обврска да ги пријавуваат сите нарушувања на безбедноста што вклучуваат лични податоци (како на пример во Холандија). Другите земји-членки можат да имаат релевантни кодекси на практика (на пример, во Ирска[3]). Додека голем број на органи за заштита на личните податоци во ЕУ во моментов ги охрабруваат контролорите да ги известуваат нарушувањата на безбедност, Директивата за заштита на личните податоците 95/46/ЕУ[4], која што е заменета со ОРЗЛП, не содржи конкретна обврска за известување за нарушувања на безбедноста повреда и затоа таквиот услов ќе биде новина за многу организации. ОРЗЛП сега го прави известувањето задолжително за сите контролори, освен ако не е веројатно дека нарушувањето на безбедноста може да предизвика ризик за правата и слободите на поединците[5]. Обработувачите исто така имаат важна улога и тие мора да го известат секое нарушување на безбедноста на контролорот[6].

Работната група 29 (РГ29) смета дека новото барање за известување има голем број на придобивки. При известување на надзорниот орган, контролорите можат да добијат совети за тоа дали засегнатите поединци треба да бидат информирани. Всушност, надзорниот орган може да му нареди на контролорот да ги извести тие поединци за нарушувањето на безбедноста[7]. Комуникацијата за нарушувањето на безбедноста на лицата му овозможува на контролорот да обезбеди информации за ризиците што се прикажани како резултат на нарушувањето на безбедноста и чекорите што можат да ги преземат тие поединци за да се заштитат од неговите можни последици. Фокусот на секој план за одговор на нарушување на безбедноста треба да биде на заштитата на поединците и нивните лични податоци. Како резултат на тоа, известувањето за нарушувањето на безбедноста треба да се смета како алатка за подобрување на усогласеноста во однос на заштитата на личните податоци. Во исто време,

[1] Види член 4(21) од ОРЗЛП
[2] Види http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 и http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611
[3] Види https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm
[4] Види http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
[5] Правата содржани во Поглавјето за основни права на ЕУ, се достапни на http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[6] Види член 33(2). Ова е слично во концепт на член 5 од Регулативата (ЕУ) бр. 611/2013, во кој се вели дека давателот на услуги со кој се склучува договор да испорача дел од услугата за електронски комуникации (без да има директен договор со претплатниците) е должен да го извести договорниот давател на услуги во случај на нарушување на безбедноста на личните податоци.
[7] Види членови 34(4) и 58(2)(д)

треба да се забележи дека доколку не се пријави нарушување на безбедноста на поединецот или на надзорниот орган, можно е да се примени казна за контролорот според член 83.

Затоа, контролорите и обработувачите се охрабруваат да планираат однапред и да воспостават постапки за да можат да откриваат и навремено да го сопрат нарушувањето на безбедноста, да го проценат ризикот за поединците[8], а потоа да утврдат дали е потребно да се извести надлежниот надзорен орган и да се објави нарушувањето на безбедноста на засегнатите лица кога е тоа потребно. Известувањето до надзорниот орган треба да претставува дел од тој план за одговор на инциденти.

ОРЗЛП содржи одредби за тоа кога треба да се извести нарушувањето на безбедноста и на кого, како и кои информации треба да се обезбедат како дел од известувањето. Информациите потребни за известувањето можат да се дадат во фази, но во секој случај контролорите треба да постапуваат навремено за секое нарушување на безбедноста.

Во своето мислење 03/2014 за известување за нарушување на безбедноста на лични податоци[9], РГ29 обезбеди насоки за контролорите со цел да им помогне да одлучат дали да ги известат субјектите на лични податоци во случај на нарушување на безбедноста. Во мислењето се разгледуваше обврската на давателите на електронски комуникации во врска со Директивата 2002/58/ЕУ и беа дадени примери од повеќе сектори, во контекст на тогашниот нацрт ОРЗЛП и се презентираа добри практики за сите контролори.

Тековните насоки ги објаснуваат задолжителните известувања за нарушување на безбедноста и условите за комуникација од ОРЗЛП и некои од чекорите што контролорите и обработувачите можат да ги преземат за да ги исполнат овие нови обврски. Тие, исто така, даваат примери за разни видови на нарушувања на безбедноста и за тоа кој треба да бидат известен во различни ситуации.

I. Известување за нарушување на безбедноста на личните податоци според ОРЗЛП

А. Основни безбедносни разгледувања

Еден од условите на ОРЗЛП е дека, со употреба на соодветни технички и организациски мерки, личните податоци ќе бидат обработени на таков начин со кој се осигурува соодветната безбедност на личните податоци, вклучително и заштита од неовластена или незаконска обработка и од случајно губење, уништување или оштетување[10].

Во однос на тоа, ОРЗЛП ги условува контролорите и обработувачите да воспостават соодветни технички и организациски мерки за да осигурат ниво на безбедност соодветно на ризикот што се однесува на личните податоци кои се обработуваат. Тие треба да ја земат предвид најсовремената технологија, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризикот од различна веројатност и сериозност за правата и слободите на физичките лица[11]. Исто така, ОРЗЛП изискува целата соодветна технолошка заштита и организациски мерки да бидат воспоставени за веднаш да се одреди дали постои нарушување на безбедноста, што потоа утврдува дали е извршена обврската за известување[12].

---

[8] Ова може да се обезбеди под условот за надгледување и преглед на ПВЗЛП (проценка на влијанието врз заштитата на личните податоци) , која е потребна за операциите за обработка, што може да резултира во висок ризик за правата и слободите на физичките лица (член 35(1) и (11)).

[9] Види Мислење 03/2014 за известување за нарушување на безбедноста на личните податоци http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Види членови 5(1)(ѓ) и 32.

[11] Член 32; види исто образложение 83

[12] Види образложение 87

Како резултат на тоа, клучен елемент на секоја политика за безбедност на податоците е да се биде во можност, кога е возможно, да се спречи нарушување на безбедноста а, кога и покрај тоа се има случено, да се делува навремено.

Б. Што е нарушување на безбедноста на личните податоци?

1. Дефиниција

Како дел од секој обид за решавање на нарушување на безбедноста, контролорот прво треба да биде во можност да препознае такво нарушување на безбедноста. ОРЗЛП го дефинира „нарушувањето на безбедноста на личните податоци“ во член 4(12) како:

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

Она што се подразбира под „уништување“ на личните податоци треба да биде јасно: ова е кога личните податоци повеќе не постојат, или повеќе не постојат во форма што е од корист за контролорот. „Оштетување“ исто така треба да биде релативно јасно: овде личните податоци се променети, корумпирани или повеќе не се целосни. Во однос на „губење“ на личните податоци, ова треба да се толкува дека личните податоците сè уште можат да постојат, но контролорот изгубил контрола или пристап до нив, или повеќе ги нема во негова сопственост. Конечно, неовластената или незаконската обработка може да вклучува обелоденување на лични податоци до (или пристап од) примателите кои не се овластени да ги примаат (или да им пристапуваат на) личните податоци, или која било друга форма на обработка што ја нарушува ОРЗЛП.

Пример

Пример за губење на лични податоци може да биде кога уредот што содржи копија од базата на лични податоци на клиенти на контролорот е изгубена или украдена. Дополнителен пример за губење може да биде кога единствената копија на збир на лични податоци е криптирана од уценувачки софтвер (ransomware), или е криптирана од контролорот користејќи клуч кој веќе не е во негова сопственост.

Тоа што треба да биде јасно е дека нарушувањето на безбедноста е еден вид на безбедносен инцидент. Сепак, како што е наведено во член 4(12), ОРЗЛП се применува само кога има нарушување на безбедноста на *личните податоци*. Последица од ваквото нарушување на безбедноста е тоа што контролорот нема да може да обезбеди усогласеност со принципите што се однесуваат на обработката на личните податоци, како што е наведено во член 5 од ОРЗЛП. Ова ја истакнува разликата помеѓу безбедносен инцидент и нарушување на безбедноста на личните податоци - во суштина, додека сите нарушувања на безбедноста на личните податоци се безбедносни инциденти, не сите безбедносни инциденти се нужно нарушувања на безбедноста на личните податоци[13].

Потенцијалните негативни ефекти на на нарушувањето на безбедноста врз поединците се разгледуваат понатаму во текстот.

2. Видови на нарушувања на безбедноста

[13] Треба да се напомене дека безбедносен инцидент не е ограничен на модели на закана кога се врши напад врз организација од надворешен извор, туку вклучува и инциденти од внатрешна обработка кои ги нарушуваат безбедносните принципи.

Во своето мислење 03/2014 за известување за нарушување на безбедноста, РГ29 објасни дека нарушувањата за безбедност може да се категоризираат според следниве три добро познати принципи за безбедност на информации[14]:

- „Нарушување на безбедност на доверливоста“ - кога има неовластено или случајно откривање, или пристап до лични податоци.
- „Нарушување на безбедност на интегритетот“ - кога има неовластено или случајно менување на личните податоци.
- „Нарушување на безбедност на достапноста“ - кога има случајно или неовластено губење на пристап[15] до, или уништување, на личните податоци.

Исто така, треба да се напомене дека, во зависност од околностите, нарушување на безбедноста може да се однесува на доверливост, интегритет и достапност на лични податоци во исто време, како и секоја комбинација на истите.

Со оглед на тоа што утврдувањето дали има нарушување на безбедноста на доверливоста или интегритетот е релативно јасно, во случај кога има нарушување на безбедност на достапноста може да биде помалку очигледно. Нарушувањето на безбедноста секогаш ќе се смета за нарушување на безбедност на достапноста кога има постојана загуба или уништување на личните податоци.

Пример

Примери за губење на достапноста вклучуваат кога личните податоци се избришани или случајно или од неовластено лице, или, во примерот на безбедно криптирани лични податоци, клучот за декрипција е изгубен. Во случај кога контролорот не може да го врати пристапот до личните податоци, на пример, од резервна копија, тогаш ова се смета за трајно губење на достапноста.

Губење на достапноста може да се појави и кога имало значително нарушување во нормалната услуга на една организација, на пример, доживување на прекин на електрична енергија или напад за одбивање на услуга, правејќи ги личните податоци недостапни.

Може да се постави прашањето дали привременото губење на достапност на личните податоци треба да се смета за нарушување на безбедноста и доколку е така, нарушување за кое треба известување. Во членот 32 од ОРЗЛП, „безбедност на обработка“, се објаснува дека при спроведување на технички и организациски мерки за да се обезбеди ниво на безбедност соодветно на ризикот, меѓу другото треба да се земе предвид „способност за обезбедување на постојана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка“ и „способност за навремено обновување на достапноста и пристапот до личните податоци во случај на физички или технички инцидент“.

Затоа, безбедносниот инцидент со кој личните податоци во одреден временски период се недостапни е исто така еден вид на нарушување на безбедноста, бидејќи недостатокот на

[14] Види мислење 03/2014

[15] Добро е утврдено дека „пристапот“ е фундаментално дел од „достапноста“. Погледнете, на пример, NIST SP800-53rev4, кој ја дефинира „достапноста“ како: „Обезбедување на навремен и сигурен пристап и употреба на информации“, достапно на http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 исто така наведува на: „Навремен, сигурен пристап до податоци и услуги за информации за овластени корисници“. Види https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 исто така, ја дефинира „достапноста“ како „Својство да се биде достапен и употреблив по барање на овластен субјект “: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

пристап до личните податоци може да има значително влијание врз правата и слободите на физичките лица. За појасно, кога личните податоци се недостапни заради извршување на планирано одржување на системот, ова не претставува „нарушување на безбедноста“, како што е дефинирано во член 4(12).

Како и со трајно губење или уништување на личните податоци (или кој било друг вид на нарушување на безбедноста), нарушувањето на безбедноста што вклучува привремено губење на достапноста треба да биде документирано во согласност со член 33(5). Ова му помага на контролорот да покаже отчетност пред надзорниот орган, кој може да побара да ги види тие записи[16]. Меѓутоа, во зависност од околностите на нарушувањето на безбедноста, може да бара или да не бара известување до надзорниот орган и комуникација до засегнатите лица. Контролорот ќе треба да ја процени веројатноста и сериозноста на влијанието врз правата и слободите на физичките лица како резултат на недостатокот на достапност на личните податоци. Во согласност со член 33, контролорот ќе треба да извести освен ако не е веројатно дека нарушувањето на безбедноста може да предизвика ризик за правата и слободите на физичките лица. Се разбира, ова ќе треба да се проценува од случај до случај.

Примери

Во контекст на болница, доколку не се достапни критични здравствени податоци за пациенти, дури и привремено, тоа може да претставува ризик за правата и слободите на физичките лица; на пример, операции може да бидат откажани и животи да бидат ставени во опасност.

Спротивно на тоа, во случај системите на едно медиумско претпријатие да бидат недостапни неколку часа (на пр. поради прекин на електрична енергија) и со тоа таа компанија е спречена да испрати билтени до своите претплатници, тогаш тоа не е веројатно дека претставува ризик за правата и слободите на физичките лица.

Треба да се напомене дека иако губењето на достапност на системите на контролорот може да биде само привремено и може да не влијае на поединците, важно е контролорот да ги земе предвид сите можни последици од нарушувањето на безбедноста, бидејќи сè уште може да бара известување за други причини.

Пример

Инфекција со уценувачки софтвер – „ransomware“ (малициозен софтвер што ги криптира податоците на контролорот сè додека не се исплати откуп) може да доведе до привремено губење на достапноста ако личните податоци можат да бидат обновени од резервна копија. Сепак, се случил мрежен упад и може да се бара известување доколку инцидентот се квалификува како нарушување на безбедност на доверливоста (т.е. напаѓачот пристапил до личните податоци) и ова претставува ризик за правата и слободите на физичките лица.

3. Можни последици од нарушување на безбедноста на личните податоци

Нарушувањето на безбедноста потенцијално може да има голем број на значителни негативни ефекти врз поединците, што може да резултира во физичка, материјална или нематеријална штета. ОРЗЛП објаснува дека ова може да вклучува губење на контролата врз нивните лични податоци, ограничување на нивните права, дискриминација, кражба на идентитет или измама, финансиска загуба, неовластено поништување на псевдонимизацијата, оштетување на угледот и губење на доверливоста на личните податоци заштитени со професионална тајна. Исто така,

[16] Види член 33(5)

може да вклучува и секоја друга значителна економска или социјална неповолност на тие лица[17].

Соодветно на тоа, ОРЗЛП изискува од контролорот да извести за нарушувањето на безбедноста на надлежниот надзорен орган, освен ако нема веројатност дека ќе резултира во ризик од делувањето на овие неповолни последици. Таму каде што постои веројатност на висок ризик од појава на овие неповолни последици, ОРЗЛП бара од контролорот да го пренесе нарушувањето на безбедноста до засегнатите лица веднаш штом е разумно изводливо[18].

Важноста да се биде во можност да се идентификува нарушување на безбедноста, да се процени ризикот за поединците, а потоа да се извести доколку е потребно, е нагласена во образложението 87 од ОРЗЛП:

„Треба да се утврди дали се спроведени сите соодветни технолошки заштитни и организациски мерки за веднаш да се утврди дали е извршено нарушување на безбедноста на личните податоци и навремено да се извести надзорниот орган и субјектот на личните податоци. Треба да се утврди фактот дека известувањето е направено без непотребно одложување, особено земајќи ја предвид природата и тежината на нарушувањет на безбедноста на личните податоци и нејзините последици и негативните ефекти за субјектот на личните податоци. Ваквото известување може да резултира во интервенција од страна на надзорниот орган во согласност со неговите задачи и овластувања утврдени со оваа регулатива."

Понатамошните насоки за проценка на ризикот од неповолни ефекти врз поединците се разгледуваат во делот IV.

Ако контролорите не го известат ниту надзорниот орган или субјектите на лични податоци за нарушување на безбедноста на личните податоци или и покрај тоа што се исполнети барањата од членовите 33 и/или 34, тогаш на надзорниот орган му се презентира избор кој мора да вклучува разгледување на сите корективни мерки што се на располагање, што вклучуваат разгледување на изрекување на соодветна административна казна[19], која или ќе придружува корективна мерка според член 58(2) или ќе биде самостојна. Кога е избрана административна казна, нејзината вредност може да биде до 10,000,000 ЕУР или до 2% ако вкупниот годишен обрт на една компанија согласно член 83(4)(а) од ОРЗЛП. Исто така, важно е да се има предвид дека во некои случаи, неуспехот да се извести за нарушување на безбедноста може да открие или отсуство на постојни безбедносни мерки или несоодветност на постојните безбедносни мерки. Насоките на РГ29 за административните казни наведуваат: „Појавување на неколку различни прекршоци извршени заедно во секој посебен случај, значи дека надзорниот орган е во состојба да ги примени административните казни на ниво кое е ефикасно, сразмерно и обесхрабрувачко во граница на најтешкото кршење на законот". Во тој случај, надлежниот надзорен орган ќе ја има можноста да изрече санкции за неизвестување или непријавување на нарушувањето на безбедноста (членовите 33 и 34) од една страна и отсуството на (соодветни) безбедносни мерки (член 32) од друга страна, бидејќи тие се две одделни прекршувања на законот.

II. Член 33 - Известување до надзорниот орган

А. Кога да се извести

[17] Види исто образложение 85 и 75
[18] Види исто образложение 86.
[19] За дополнителни детали, видете ги насоките на РГ29 за примена и утврдување на административни казни, достапни овде: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

1. Барања на член 33

Во член 33(1) се предвидува дека:

„Во случај на нарушување на безбедноста на личните податоци, контролорот е должен без непотребно одложување а, доколку е можно, не подоцна од 72 часа откако ќе се стане свесен за тоа, да го извести нарушувањето на безбедноста на личните податоци до надлежниот надзорен орган во согласност со член 55, освен ако нарушувањето на безбедноста на личните податоци веројатно нема да предизвика ризик за правата и слободите на физичките лица. Кога известувањето до надзорниот орган не е направено во рок од 72 часа, тоа ќе биде придружено со причини за одложувањето.“

Образложението 87 наведува дека[20]:

„Треба да се утврди дали се спроведени сите соодветни технолошки заштитни и организациски мерки за веднаш да се утврди дали е извршено нарушување на безбедноста на личните податоци и навремено да се извести надзорниот орган и субјектот на личните податоци. Треба да се потврди фактот дека известувањето е направено без непотребно одложување особено земајќи ја предвид природата и тежината на нарушувањето на безбедноста на личните податоци и нејзините последици и негативни ефекти за субјектот на личните податоци. Ваквото известување може да резултира во интервенција на надзорниот орган во согласност со неговите задачи и овластувања утврдени со оваа регулатива.“

2. Кога контролорот станува „свесен“?

Како што е детално наведено погоре, ОРЗЛП бара, во случај на нарушување на безбедноста, контролорот да го извести нарушувањето на безбедноста без непотребно одложување а, доколку е можно, не подоцна од 72 часа откако ќе стане свесен за тоа. Ова може да го постави прашањето кога контролорот може да се смета дека станал „свесен“ за нарушувањето на безбедноста. РГ29 смета дека контролорот треба да се смета дека станал „свесен“ кога тој контролер има разумен степен на сигурност дека се случил безбедносен инцидент кој довел до компромитирање на личните податоци.

Сепак, како што беше наведено порано, ОРЗЛП бара контролорот да ги спроведе сите соодветни технолошки заштитни и организациски мерки за веднаш да утврди дали е извршено нарушување на безбедноста и навремено да го извести надзорниот орган и субјектите на лични податоци. Исто така, наведува дека треба да се утврди фактот дека известувањето е направено без непотребно одложување, особено земајќи ја предвид природата и тежината на нарушувањето на безбедноста и нејзините последици и негативните ефекти за субјектот на личните податоци.[21]. Ова наметнува обврска врз контролорот да осигури дека тој ќе биде „свесен“ за какви било нарушувања на безбедноста, за да може навремено да преземе соодветно дејство.

Кога точно, контролорот може да се смета дека е „свесен“ за одредено нарушување на безбедноста, ќе зависи од околностите на специфичното нарушување на безбедноста. Во некои случаи, ќе биде релативно јасно од самиот почеток дека имало нарушување на безбедноста, додека во други, може да потрае некое време за да се утврди дали личните податоци биле компромитирани. Сепак, акцентот треба да се стави на навремена акција за да се испита инцидентот со кој се утврдува дали навистина е нарушена безбедноста на личните податоци, а доколку е така, да се преземат поправни мерки и да се извести доколку е потребно.

[20] Тука е исто така важно образложението 85.
[21] Види образложение 87

Примери

1. Во случај на губење на УСБ клуч со некриптирани лични податоци, честопати не е можно да се утврди дали неовластени лица добиле пристап до тие податоци. Како и да е, иако контролорот не може да утврди дали се случило нарушување на безбедност на доверливоста, таков случај треба да се извести бидејќи постои разумен степен на сигурност дека се случило нарушување на безбедност на достапноста; контролорот станува „свесен“ кога доаѓа до сознанието дека УСБ клучот е изгубен.
2. Трета страна го известува контролорот дека случајно ги добиле личните податоци на еден негов клиент и даваат докази за неовластеното откривање. Бидејќи на контролорот му биле дадени јасни докази за нарушување на безбедност на доверливоста, тогаш не може да постои сомневање дека станал „свесен“.
3. Контролорот открива дека постои можен упад во неговата мрежа. Контролорот ги проверува своите системи за да утврди дали личните податоци што се чуваат на тој систем се компромитирани и потврдува дека тоа е случајот. Уште еднаш, бидејќи контролорот сега има јасен доказ за нарушување на безбедноста, не може да постои сомневање дека станал „свесен“.
4. А компјутерски криминалец контактира со контролорот откако го хакирал неговиот систем со цел да побара откуп. Во тој случај, откако ќе го провери својот систем да потврди дека е нападнат, контролорот има јасен доказ дека се случило нарушување на безбедноста и не постои сомневање дека станал свесен.

Откако најпрво бил информиран за потенцијално нарушување на безбедноста од страна на физичко лице, медиумска организација или друг извор, или кога самиот открил безбедносен инцидент, контролорот може да започне кратка истрага со цел да утврди дали навистина се случило нарушување на безбедноста или не. За време на овој период на истрага, контролорот не може да се смета за „свесен“. Сепак, се очекува почетната истрага да започне што е можно поскоро и да се утврди со разумен степен на сигурност дали е сторено нарушување на безбедноста; потоа може да следи подетална истрага.

Откако контролорот ќе стане свесен, нарушувањето на безбедност кое може да се пријави мора да биде известено без непотребно одложување, а кога е можно, не подоцна од 72 часа. Во овој период, контролорот треба да го процени веројатниот ризик за физичките лица со цел да утврди дали е активирано барањето за известување, како и активностите потребни за решавање на нарушување на безбедноста. Како и да е, контролорот веќе може да има првична проценка на потенцијалниот ризик што може да биде резултат на нарушување на безбедноста како дел од проценката на влијанието врз заштитата на личните податоци (ПВЗЛП)[22] направена пред да се спроведе соодветната операција за обработка. Сепак, ПВЗЛП може да биде генерализирана во споредба со специфичните околности на какво било нарушување на безбедноста, со што во секој случај треба да се направи дополнителна проценка земајќи ги предвид овие околности. За повеќе подробности за проценување на ризикот, погледнете го делот IV.

Во повеќето случаи, овие прелиминарни активности треба да бидат завршени веднаш по првичното предупредување (т.е. кога контролорот или обработувачот се сомнева дека се случил безбедносен инцидент што може да вклучува лични податоци.) – само во исклучителни случаи треба да трае подолго од ова.

Пример

Лице го известува контролорот дека добил е-пошта која лажно се претставува дека е од

[22] Види насоки на РГ29 за ПВЗЛП тука: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

контролорот, која содржи лични податоци во врска со неговата (вистинска) употреба на услугата на контролорот, сугерирајќи дека безбедноста на контролорот е загрозена. Контролорот спроведува кратка истрага и идентификува упад во нивната мрежа и докази за неовластен пристап до лични податоци. Контролорот сега ќе се смета за „свесен“ и се бара известување до надлежниот надзорен орган, освен ако е малку веројатно дека тоа претставува ризик за правата и слободите на физичките лица. Контролорот ќе треба да преземе соодветни поправни мерки да го реши нарушувањето на безбедноста.

Затоа контролорот треба да има поставено внатрешни процеси за да може да го открие и да го реши нарушувањето на безбедноста. На пример, за пронаоѓање на некои неправилности при обработка на личните податоци, контролорот или обработувачот може да користи одредени технички мерки, како што се проток на лични податоци и анализатори на најави, од кои е можно да се дефинираат настани и предупредувања преку корелација со сите податоци за најавување.[23] Важно е кога се открива повреда, да се пријавува нагоре до соодветното управно ниво, така што може да се реши и доколку е потребно, да се извести во согласност со член 33, а, доколку е потребно, член 34. Ваквите мерки и механизми за известување може да бидат подробно претставени во плановите за одговор на инциденти на контролорот и/или договорите за управување. Овие ќе му помогнат на контролорот да планира делотворно и да утврди кој има оперативна одговорност во рамките на организацијата за управување со нарушувањето на безбедноста и како или дали да го ескалира инцидентот како што е соодветно.

Контролорот исто така треба да воспостави договори со сите обработувачи што ги користи контролорот, кои самите имаат обврска да го известат контролорот во случај на нарушување на безбедноста (види подолу).

Додека одговорностите на контролорите и обработувачите се да воспостават соодветни мерки за да можат да спречат, да делуваат и да го решат нарушувањето на безбедноста, треба да постојат практични чекори што треба да се преземат во сите случаи.

- Информациите за сите настани поврзани со безбедноста треба да бидат насочени кон одговорното лице или лица кои имаат задача да се справуваат со инциденти, да утврдат постоење на нарушување на безбедноста и проценка на ризикот.
- Ризикот за физичките лица како резултат на нарушување на безбедноста треба да се процени (веројатност да нема ризик, ризик или висок ризик), при што ќе бидат информирани релевантните оддели на организацијата.
- Доколку е потребно, треба да се изврши известување до надзорниот орган и потенцијално да се комуницира за нарушувањето на безбедноста до засегнатите лица.
- Во исто време, контролорот треба да дејствува за да го запре нарушувањето на безбедноста и да се опорави.
- Документацијата за нарушувањето на безбедноста треба да се одвива за време на развојот на нарушувањето.

Соодветно на тоа, треба да биде јасно дека контролорот има обврска да постапи на секое првично предупредување и да утврди дали е направено нарушување на безбедноста или не. Овој краток период овозможува одредена истрага, а за контролорот да собере докази и други релевантни подробности. Меѓутоа, откако контролорот ќе утврди со разумен степен на сигурност дека се случило нарушување на безбедноста, доколку се исполнети условите од членот 33(1), тогаш мора да го извести надзорниот орган без непотребно одложување а, кога е

[23] Треба да се напомене дека податоците за најавување кои ја олеснуваат прегледноста на, на пр. складирање, изменување или бришење на личните податоци, исто така може да се квалификуваат како лични податоци што се однесуваат на лицето кое започнало со соодветната операција за обработка.

можно, не подоцна од 72 часа[24]. Доколку контролорот не постапи навремено и стане очигледноа дека се случило нарушување на безбедноста, тоа може да се смета како неуспех во известувањето во согласност со член 33.

Во членот 32 се појаснува дека контролорот и обработувачот треба да имаат соодветни технички и организациски мерки за да обезбедат соодветно ниво на безбедност на личните податоци: можноста за откривање, решавање и навремено известување за нарушувањето на безбедноста треба да се сметаат како суштински елементи на овие мерки.

3. Заеднички контролори

Членот 26 се однесува на заеднички контролори и прецизира дека заедничките контролори ги одредуваат нивните одговорности за усогласеност со ОРЗЛП[25]. Ова опфаќа утврдување која страна ќе има одговорност за исполнување на обврските од членовите 33 и 34. РГ29 препорачува договорните договори меѓу заеднички контролори да содржат одредби со кои се утврдува кој контролор ќе го преземе водството или е одговорен за исполнување на обврските за известување за нарушување на безбедноста на ОРЗЛП.

4. Обврски на обработувачот

Контролорот ја задржува целокупната одговорност за заштита на личните податоци, но обработувачот игра важна улога за да му овозможи на контролорот да ги исполни своите обврски; и ова вклучува известување за нарушување на безбедноста. Всушност, во членот 28(3) се утврдува дека обработката од страна на обработувачот се уредува со договор или друг правен акт. Во членот 28(3)(ѓ) се наведува дека договорот или друг правен акт пропишува дека обработувачот „му помага на контролорот во обезбедување на исполнување на обврските согласно членовите 32 до 36, земајќи ја предвид природата на обработката и информациите што му се достапни на обработувачот".

Член 33(2) појаснува дека ако обработувачот се користи од контролорот и обработувачот стане свесен за нарушување на безбедноста на личните податоци што ги обработува во име на контролорот, тој мора да го извести контролорот „без непотребно одложување". Треба да се напомене дека обработувачот нема потреба прво да ја процени веројатноста за појава на ризик од нарушување на безбедноста пред да го извести контролорот; контролорот треба да ја направи оваа проценка кога ќе стане свесен за нарушувањето на безбедноста. Обработувачот треба само да утврди дали имало нарушување на безбедноста и потоа да го извести контролорот. Контролорот го користи обработувачот за да ги постигне своите цели; затоа, во принцип, контролорот треба да се смета за „свесен" откако обработувачот ќе го извести за нарушувањето на безбедноста. Обврската на обработувачот да го извести контролорот му дозволува на контролорот да се справи со нарушувањето на безбедноста и да утврди дали е потребно да го извести надзорниот орган во согласност со член 33(1) и засегнатите лица во согласност со член 34(1). Контролорот исто така може да сака да го испита нарушувањето на безбедноста, бидејќи обработувачот може да не е во состојба да ги знае сите релевантни факти што се однесуваат на ова прашање, на пример, доколку копија или резервна копија на лични податоци што се уништени или изгубени од страна на обработувачот се сè уште во рацете на контролорот. Ова може да влијае на тоа дали контролорот тогаш има потреба да извести.

ОРЗЛП не предвидува експлицитен временски рок во кој обработувачот мора да го предупреди контролорот, освен дека тоа мора да го стори „без непотребно одложување". Затоа, РГ29

[24] Погледнете ја Регулативата бр. 1182/71 за утврдување на правилата што се применуваат за периоди, датуми и временски ограничувања, достапни на: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] Види исто образложение 79.

препорачува обработувачот веднаш да го извести контролорот, со обезбедување на дополнителни информации за нарушувањето на безбедноста во фази, како што понатаму повеќе детали стануваат достапни. Ова е од важност за да му се помогне на контролорот да ги исполни барањата за известување до надзорниот орган во рок од 72 часа.

Како што е објаснето погоре, договорот помеѓу контролорот и обработувачот треба да наведе како треба да се исполнуваат барањата изразени во член 33(2), покрај другите одредби во ОРЗЛП. Ова може да вклучува барања за рано известување од страна на обработувачот што за возврат ги поддржува обврските на контролорот да поднесе извештај до надзорниот орган во рок од 72 часа.

Кога обработувачот обезбедува услуги на повеќе контролори кои се сите погодени од истиот инцидент, обработувачот треба да ги пријави деталите за инцидентот на секој контролор.

Обработувачот може да даде известување во име на контролорот, доколку контролорот му дал соодветно овластување на обработувачот и ова е дел од договорните аранжмани помеѓу контролорот и обработувачот. Таквото известување мора да се направи во согласност со членовите 33 и 34. Сепак, важно е да се напомене дека правната одговорност за известување останува кај контролорот.

Б. Обезбедување на информации до надзорниот орган

1. Информации што треба да се обезбедат

Кога контролорот ќе го извести надзорниот орган за нарушување на безбедноста, во членот 33(3) се вели дека, најмалку, треба:

„(а) да се опише природата на нарушувањето на безбедноста на личните податоци, вклучувајќи каде е можно, категориите и приближниот број на засегнати субјекти на лични податоци и категориите и приближниот број на засегнати записи за лични податоци;

(б) да се соопшти името и деталите за контакт на офицерот за заштита на личните податоци или на друга контакт точка каде што може да се добијат повеќе информации;

(в) да се опишат најверојатните последици од нарушувањето на безбедноста на личните податоци;

(г) да се опишат преземените или предложените мерки од контролорот за да се справи со нарушувањето на безбедноста на личните податоци, вклучувајќи, доколку е соодветно, мерките за ублажување на неговите можни негативни ефекти.“

ОРЗЛП не дефинира категории на субјекти на лични податоци или записи за лични податоци. Сепак, РГ29 предложува категориите на субјекти на лични податоци да се однесуваат на различните типови на физички лица чии лични податоци биле погодени од нарушување на безбедноста: во зависност од користените идентификатори, ова може да вклучува, меѓу другите, деца и други ранливи групи, лица со посебни потреби, вработени или клиенти. Слично на тоа, категории за записи на лични податоци можат да се однесуваат на различните типови на записи што контролорот може да ги обработува, како што се здравствени податоци, образовни записи, информации за социјална помош, финансиски детали, броеви на банкарски сметки, броеви на пасоши и слично..

Образложението 85 појаснува дека една од целите на известувањето е ограничување на штетите на поединците. Според тоа, ако видовите на субјектите на лични податоци или видовите лични податоци укажуваат на ризик од одредена штета што се јавува како резултат

на нарушување на безбедноста (на пр. кражба на идентитет, измама, финансиска загуба, закана за професионална тајност), тогаш важно е известувањето да укаже на овие категории. На овој начин, тоа е поврзано со барањето за опишување на веројатните последици од нарушувањето на безбедноста.

Кога не се достапни точни информации (на пр. точен број на засегнати субјекти на лични податоци), тоа не треба да претставува пречка за навремено известување за нарушувањето на безбедноста. ОРЗЛП дозволува приближно пресметување на бројот на засегнатите лица и бројот на засегнатите записи за лични податоци. Фокусот треба да биде насочен кон решавање на негативните ефекти од нарушувањето на безбедноста наместо обезбедување на прецизни бројки.

Така, кога станува јасно дека имало нарушување на безбедноста, но колку е големо сè уште не се знае, известувањето во фази (види подолу) е безбеден начин да се исполнат обврските за известување.

Во членот 33(3) се вели дека контролорот треба „најмалку“ да ги достави овие информации со известување, така што контролорот може, доколку е потребно, да избере да обезбеди дополнителни детали. Различни видови на нарушувања на безбедноста (доверливост, интегритет или достапност) може да бараат дополнителни информации за целосно објаснување на околностите на секој случај.

Пример

Како дел од своето известување до надзорниот орган, контролорот може да смета дека е корисно да го именува својот обработувач ако е во основната причина за повреда, особено ако тоа довело до инцидент што влијае на евиденцијата за лични податоци на многу други контролори кои го користат истиот обработувач.

Во секој случај, надзорниот орган може да побара дополнителни детали како дел од неговата истрага за нарушувањето на безбедноста.

2. Известувањето во фази

Во зависност од природата на нарушувањето на безбедноста, понатамошна истрага од контролорот може да биде неопходна за да се утврдат сите релевантни факти поврзани со инцидентот. Според член 33(4):

„Сè додека не е можно да се обезбедат информации во исто време, информациите може да се дадат во фази без непотребно дополнително одложување.“

Ова значи дека ОРЗЛП признава дека контролорите не секогаш ги имаат сите потребни информации во врска со нарушувањето на безбедноста во рок од 72 часа откако ќе станат свесни за тоа, бидејќи целосните и сеопфатни детали за инцидентот може да не бидат секогаш достапни во овој првичен период. Во таков случај се овозможува известување во фази. Поверојатно е дека ова ќе биде случај за посложени нарушувања на безбедноста, како што се некои видови на инциденти за компјутерска безбедност каде, на пример, може да биде неопходна длабинска форензичка истрага за целосно утврдување на природата на нарушувањето на безбедноста и степенот до кој личните податоците се компромитирани. Како резултат на тоа, во многу случаи контролорот ќе мора да направи повеќе истраги и да обезбеди дополнителни информации во понатамошниот период. Ова е дозволиво, доколку контролорот дава причини за одложување, во согласност со член 33(1). РГ29 препорачува кога контролорот прво ќе го извести надзорниот орган, контролорот треба исто така да го извести надзорниот

орган ако контролорот сè уште ги нема сите потребни информации и подоцна ќе обезбеди повеќе подробности. Надзорниот орган треба да се согласи како и кога треба да се обезбедат дополнителни информации. Ова не го спречува контролорот да обезбеди дополнителни информации во која било друга фаза, доколку станува свесен за дополнителни релевантни детали за нарушувањето на безбедноста што треба да се достави до надзорниот орган.

Фокусот на барањето за известување е да ги охрабри контролорите да дејствуваат веднаш при нарушување на безбедноста, да го спречат и, доколку е можно, да ги вратат компромитираните лични податоци и да побараат релевантен совет од надзорниот орган. Известувањето за надзорниот орган во првите 72 часа може да му овозможи на контролорот да се увери дека одлуките за известување или неизвестување на поединците се правилни.

Сепак, целта на известувањето на надзорниот орган не е само да се добие насока дали да се известат засегнатите лица. Во некои случаи ќе биде очигледно дека, поради природата на нарушувањето на безбедноста и сериозноста на ризикот, контролорот треба да ги извести засегнатите лица без одложување. На пример, ако постои непосредна закана од кражба на идентитет или ако се откриваат посебни категории на лични податоци[26] преку интернет, контролорот треба да постапи без непотребно одложување за да го сопре нарушувањето на безбедноста и да им го соопшти на засегнатите лица (види дел III). Во исклучителни околности, ова може да се случи дури и пред известување на надзорниот орган. По општо, известувањето за надзорниот орган не може да послужи како оправдување за неуспехот да се пренесе нарушувањето на безбедноста до субјектот на личните податоци кога тоа се бара.

Исто така, треба да биде јасно дека откако ќе се изврши првично известување, контролорот може повторно да го извести надзорниот орган ако последователната истрага открие докази дека безбедносниот инцидент е сопрен и не се случило никакво нарушување на безбедноста. Потоа, овие информации може да се додадат на веќе дадените информации на надзорниот орган и со тоа инцидентот ќе биде евидентиран дека не е нарушување на безбедноста. Нема казна за пријавување на инцидент што на крај се востановува дека не е нарушување на безбедноста.

Пример

Контролорот го известува надзорниот орган во рок од 72 часа од откривањето на нарушувањето на безбедноста дека изгубил УСБ клуч во кој има копија на лични податоци на некои од неговите клиенти. УСБ клучот подоцна е најден дека е погрешно класифициран во просториите на контролорот и е вратен. Контролорот му ја соопштува новата состојба на надзорниот орган и бара известувањето да се измени.

Треба да се напомене дека пристапот за известување во фази е веќе начин на постапување според постојните обврски на Директивата 2002/58/ЕУ, Регулативата 611/2013 и други само пријавени инциденти.

3. Одложени известувања

Член 33(1) појаснува дека кога известување до надзорниот орган не е направено во рок од 72 часа, тоа треба да биде придружено со причини за одложувањето. Ова, заедно со концептот на известување во фази, препознава дека контролорот не може секогаш да биде во можност да извести за нарушувањето на безбедноста во тој временски период и дека може да биде дозволиво одложено известување.

[26] Види член 9. 16

Таквото сценарио може да се случи кога, на пример, контролорот искуси повеќе слични нарушувања на безбедност на доверливоста во краток временски период, влијаејќи на голем број субјекти на лични податоци на ист начин. Контролорот би можел да стане свесен за нарушување на безбедноста, но, при започнувањето на истрагата и пред известувањето, да открие дополнителни слични нарушувања на безбедноста, кои имаат различни причини. Во зависност од околностите, на контролорот можеби ќе му треба извесно време да го утврди степенот на нарушувањата на безбедност и наместо да го известува секое нарушување на безбедноста поединечно, контролорот конструира корисно известување кое застапува неколку слични нарушувања на безбедноста, со можни различни причини. Ова може да доведе до одложување на известувањето до надзорниот орган за повеќе од 72 часа откако контролорот прво ќе стане свесен за овие нарушувања на безбедноста.

Строго кажано, секое поединечно нарушување на безбедноста е инцидент што може да се пријави. Меѓутоа, за да се избегне преголема оптовареност, контролорот може да достави „пакет“ известување што ги претставува сите овие нарушувања на безбедноста, под услов тие да се однесуваат на ист вид на нарушувања на безбедноста на лични податоци, во релативно краток временски период. Ако се случат серија на нарушувања на безбедноста кои се однесуваат на различни видови на лични податоци со различни видови на нарушена безбедност, тогаш известувањето треба да продолжи на нормален начин, при што секое нарушување на безбедноста ќе биде пријавено во согласност со член 33.

Додека, ОРЗЛП дозволува одложено известување до одреден степен, ова не треба да се смета како нешто што редовно се случува. Вреди да се напомене дека пакетите известувања може да се направат и за повеќе слични нарушувања на безбедноста пријавени во рок од 72 часа.

В. Прекугранични нарушувања на безбедноста и нарушувања на безбедност на не-ЕУ институции

1. Прекугранични нарушувања на безбедноста

Кога постои прекугранична обработка[27] на личните податоци, нарушувањето на безбедноста може да влијае на субјектите на лични податоци во повеќе од една земја-членка. Членот 33(1) појаснува дека кога има нарушување на безбедноста, контролорот треба да го извести надлежниот надзорен орган во согласност со член 55 од ОРЗЛП[28]. Членот 55(1) тврди дека:

> „Секој надзорен орган е надлежен за извршување на задачите што му се доделени и за вршење на овластувањата што му се дадени во согласност со оваа регулатива на територијата на својата земја-членка.“

Сепак, во член 56(1) се наведува:

> „Без да е во спротивност со членот 55, надзорниот орган на главното место на основање или на единственото место на основање на контролорот или обработувачот е надлежен да дејствува како водечки надзорен орган за прекугранична обработка, извршена од наведениот контролор или обработувач во согласност со постапката наведена во член 60.“

Понатаму, членот 56(6) наведува:

> „ Водечкиот надзорен орган е единствениот соговорник на контролорот или обработувачот за прекугранична обработка извршена од тој контролор или обработувач.“

[27] Види член 4(23)
[28] Види исто образложение 122.

Ова значи дека секогаш кога се случи нарушување на безбедноста во контекст на прекугранична обработка и е потребно известување, контролорот треба да го извести водечкиот надзорен орган[29]. Затоа, при изготвување на планот за одговор на нарушување на безбедноста, контролорот мора да направи проценка за тоа кој надзорен орган е водечкиот надзорен орган кој ќе треба да биде известен[30]. Ова ќе му овозможи на контролорот веднаш да одговори на нарушување на безбедноста и да ги исполни своите обврски во однос на член 33. Треба да биде јасно дека во случај на нарушување на безбедноста што вклучува прекугранична обработка, мора да се изврши известување до водечкиот надзорен орган, кој не е задолжително таму каде што се наоѓаат засегнатите субјекти на лични податоци, или таму каде што навистина се случило нарушувањето на безбедноста. При известување на водечкиот орган, контролорот треба да укаже, доколку е соодветно, дали нарушувањето на безбедноста вклучува места на основање лоцирани во други земји-членки, а во кои субјектите за лични податоци на земјите-членки веројатно биле погодени од нарушувањето на безбедноста. Ако контролорот се сомнева во идентитетот на водечкиот надзорен орган, тој треба барем најмалку да го извести локалниот надзорен орган каде се случило нарушувањето на безбедноста.

2. Нарушувања на безбедност во места на основање кои не се во ЕУ

Членот 3 се однесува на територијалниот опсег на ОРЗЛП, вклучително и кога се однесува на обработка на лични податоци од контролор или обработувач што не е основан во ЕУ. Конкретно, во член 3(2) се наведува[31]:

„Оваа регулатива се применува на обработките на личните податоци на субјектите на личните податоци, кои се во Унијата, од контролор или обработувач кој не е основан во Унијата, кога активностите за обработка се поврзани со:

(а) понудата на стоки или услуги на такви субјекти на лични податоци во Унијата, без разлика дали од субјектот на личните податоци се бара да изврши плаќање, или

(б) следење на нивното однесување, доколку тоа однесување се одвива во рамките на Унијата.“

Членот 3(3) е исто така релевантен и наведува[32]:

„Оваа регулатива се применува на обработката на личните податоци од страна на контролорот кој не е основан во Унијата, но е основан на место каде што се применува правото на земја-членка во согласност со меѓународното јавно право.“

Доколку контролорот кој не е основан во ЕУ е предмет на член 3(2) или член 3(3) и доживее нарушување на безбедноста, сè уште е обврзан со задолженијата за известување според членовите 33 и 34. Членот 27 изискува контролорот (и обработувачот) да назначи претставник во ЕУ каде што се применува членот 3(2). Во вакви случаи, РГ29 препорачува да се изврши известување до надзорниот орган во земјата-членка каде што е основан претставникот на контролорот во ЕУ[33]. Слично на тоа, кога обработувачот подлежи на членот 3(2), тој ќе биде обврзан со задолженијата на обработувачите, а од особено значење овде е должноста да го извести нарушувањето на безбедноста до контролорот според член 33(2).

[29] Погледнете ги насоките на РГ29 за идентификација на водечкиот надзорен орган на контролорот или обработувачот, достапен на http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Список на детали за контакт за сите европски национални органи за заштита на личните податоци може да се најде на: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Види исто образложенија 23 и 24

[32] Види исто образложение 25

[33] Види образложение 80 и член 27

Г. Услови каде што не е потребно известување

Членот 33(1) појаснува дека нарушувањата на безбедност што „веројатно нема да предизвикаат ризик за правата и слободите на физичките лица“ не изискуваат известување до надзорниот орган. Пример може да биде кога личните податоци се веќе јавно достапни и обелоденувањето на таквите податоци не претставува веројатна опасност за поединецот. Ова е спротивно на постојните барања за известување за нарушување на безбедноста на давателите на услуги на јавно достапна електронска комуникација во Директивата 2009/136/ЕУ во кои се вели дека сите релевантни нарушувања на безбедноста треба да бидат известени до надлежниот орган.

Во своето мислење 03/2014 за известување за нарушување на безбедноста[34], РГ29 објаснува дека нарушувањето на безбедноста на доверливоста на личните податоци кои биле шифрирани со алгоритам на најновата технологија, сè уште претставува нарушување на безбедноста на личните податоци и мора да биде известено. Меѓутоа, ако доверливоста на клучот е недопрена - т.е., клучот не бил компромитиран при какво било нарушување на безбедноста и бил создаден така што не може да се потврди со достапни технички средства од кое било лице кое не е овластено да пристапи до него - тогаш податоците во принцип се неразбирливи. Така, нарушувањето на безбедност веројатно е дека нема да влијае негативно на поединците и затоа нема да изискува комуникација со тие лица[35]. Меѓутоа, дури и кога личните податоци се шифрирани, загубата или промената може да има негативни последици за субјектите на лични податоци во случај кога контролорот нема соодветна копија. Во тој случај, ќе биде потребна комуникација до субјектите на личните податоци, дури и ако самите лични податоци подлежат на соодветни мерки за криптирање.

РГ29, исто така, објасни дека ова слично ќе биде случај ако личните податоци, како што се лозинките, биле безбедно замаскирани (хеширани) и усложнети, хешираната вредност се пресметува со врвна криптографска функција за хеширање, клучот користен за хеширање на податоците не бил загрозен во какво било нарушување на безбедноста и клучот користен за хеширање на податоците е создаден на начин што не може да се утврди со достапни технолошки средства од кое било лице кое не е овластено да пристапува до нив.

Како резултат на тоа, доколку личните податоци се направени да бидат во суштина неразбирливи за неовластените страни и кога податоците се копија или постои резервна копија, нарушување на безбедност на доверливоста кое содржи правилно шифрирани лични податоци може нема да има потреба да биде известено до надзорниот орган. Ова е затоа што такво нарушување на безбедноста не е веројатно дека ќе предизвика опасност за правата и слободите на поединците. Ова секако значи дека поединецот исто така не би требало да биде информиран, бидејќи не постои веројатност за висока опасност. Како и да е, треба да се има предвид дека иако првично може да не се бара известување доколку не постои веројатна опасност за правата и слободите на поединците, тоа може да се промени со текот на времето и опасноста ќе треба да се преиспита. На пример, ако подоцна се утврди дека клучот е загрозен или се разоткрие ранливост во софтверот за енкрипција, тогаш може сè уште да се бара известување.

Понатаму, треба да се напомене дека доколку има нарушување на безбедноста кога не постои резервна копија на криптираните лични податоци, тогаш ќе има нарушување на безбедноста на достапноста, што може да претставува опасност за физичките лица и затоа може да изискува известување. Слично на тоа, кога ќе се појави нарушување на безбедноста што вклучува губење на криптирани лични податоци, дури и ако постои резервна копија на личните

[34] РГ29, мислење 03/2014 за известување за нарушување на безбедноста, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] Види исто член 4(1) и (2) од Регулатива 611/2013.

податоци, ова сепак може да се смета за нарушување на безбедноста кое бара известување, во зависност од должината на времето потребно за враќање на личните податоци од таа резервна копија и последиците што го има врз поединците поради недостапноста. Како што наведува член 32(1)(в), важен фактор на безбедност е „можноста за навремено враќање на достапноста и пристапот до личните податоци во случај на физички или технички инцидент“.

Пример
Нарушување на безбедност кое не бара известување до надзорниот орган би било губење на безбедно криптиран мобилен уред, користен од контролорот и неговиот персонал. Доколку клучот за криптирање е безбедно во сопственост на контролорот и ова не е единствената копија на личните податоци, тогаш личните податоци би биле недостапни за напаѓачот. Ова значи дека нарушувањето на безбедноста веројатно нема да предизвика опасност за правата и слободите на субјектите на лични податоци во прашање. Ако подоцна стане очигледно дека клучот за криптирање е компромитиран или дека софтверот за криптирање или алгоритамот се ранливи, тогаш тоа значи дека опасноста за правата и слободите на физичките лица е сменета и поради тоа понатаму може да се бара известување.

Сепак, неисполнување на членот 33 е тогаш кога контролорот не го известува надзорниот орган во ситуација кога личните податоци всушност не биле безбедно криптирани. Затоа, при изборот на софтвер за криптирање контролорите треба внимателно да го проценат квалитетот и правилното спроведување на понудената криптификација, да се разбере кое ниво на заштита тоа всушност обезбедува и дали е тоа соодветно на презентираните опасности. Контролорите исто така треба да бидат запознаени со посебностите на функционирањето на нивниот производ за криптирање. На пример, уредот може да се криптира откако ќе се исклучи, но не додека е во режим на подготвеност. Некои производи што користат енкрипција имаат „основни клучеви“ кои треба да ги менува секој клиент со цел да бидат ефективни. Енкрипцијата исто така може привремено да се смета за соодветна од страна на експерти за безбедност, но за неколку години може да се смета за застарена, што значи дека е спорно дали личните податоци би биле достатно криптирани од тој производ и дека тој производ ќе обезбеди соодветно ниво на заштита.

III. Член 34 - Комуникација со субјектот на личните податоци

А. Информирање на физичките лица

Во одредени случаи, покрај известување за надзорниот орган, контролорот исто така е должен да ги извести засегнатите лица за нарушувањето на безбедноста.

Членот 34(1) наведува дека:

„Кога нарушувањето на безбедноста на личните податоци може да резултира со висок ризик за правата и слободите на физичките лица, контролорот треба да го извести субјектот на личните податоци за нарушувањето на безбедноста на личните податоци без непотребно одложување.“

Контролорите треба да потсетат дека известувањето до надзорниот орган е задолжително, освен ако не постои веројатност дека постои ризик за правата и слободите на физичките лица како резултат на нарушувањето на безбедноста. Покрај тоа, кога постои веројатност дека постои голем ризик за правата и слободите на физичките лица како резултат на нарушување на безбедноста, мора да бидат информирани и физичките лица. Затоа, прагот за комуникација на нарушување на безбедноста до физичките лица е повисок отколку за известување на надзорните органи и затоа не е задолжително сите нарушувања на безбедноста да бидат

соопштени на физичките лица, со што ќе се заштити од непотребна прекумерност во известувањето.

Во ОРЗЛП се наведува дека известувањето за нарушување на безбедноста до физичките лица треба да се изврши „без непотребно одложување“, што подразбира колку што е можно поскоро. Главната цел на известувањето на физичките лица е да се обезбедат конкретни информации за чекорите кои тие треба да ги преземат за да се заштитат[36]. Како што е наведено погоре, во зависност од природата на нарушувањето на безбедноста и ризикот што се наметнува, навремената комуникација ќе им помогне на физичките лица да преземат чекори за да се заштитат од секакви негативни последици од нарушувањето на безбедноста.

Прилог Б од овие насоки дава неисцрпна листа со примери за тоа кога нарушувањето на безбедност може да доведе до висок ризик за физички лица а, следствено, за случаи кога контролорот ќе мора да извести за нарушување на безбедноста на засегнатите лица.

Б. Информации кои треба да се обезбедат

При известувањето на физичките лица, членот 34(2) определува дека:

„ Комуникацијата до субјектот на личните податоци од ставот 1 на овој член треба да ја опише на јасен и едноставен јазик природата на нарушувањето на безбедноста на личните податоци и да ги содржи барем информациите и мерките наведени во точките (б), (в) и (г)) од член 33(3).“

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

- опис на природата на нарушувањето на безбедноста;
- името и деталите за контакт на офицерот за заштита на личните податоци или друга точка за контакт;
- опис на веројатните последици од нарушувањето на безбедноста; и
- опис на преземените мерки или предложени да бидат преземени од контролорот за решавање на нарушувањето на безбедноста, вклучително, кога е соодветно, мерки за ублажување на неговите можни негативни последици.

Како пример на преземените мерки за решавање на нарушување на повредата и за ублажување на нејзините можни неповолни ефекти, контролорот може да изјави дека, откако го известил нарушувањето на безбедноста до надлежниот надзорен орган, контролорот добил совети за управување со нарушувањето на безбедноста и намалување на нејзиното влијание. Контролорот исто така треба, доколку е соодветно, да обезбеди конкретен совет за физичките лица да се заштитат од можните неповолни последици од нарушувањето на безбедноста, како што е ресетирање на лозинки во случај кога нивните ингеренциите за пристап се компромитирани. Повторно, контролорот може да избере да обезбеди информации додатно на тоа што се бара овде.

В. Контактирање на физичките лица

Во принцип, релевантното нарушување на безбедноста треба да се пренесе директно на засегнатите субјекти на лични податоци, освен ако тоа не подразбира непропорционален напор. Во таков случај, се прави јавно известување или слична мерка со која субјектите на лични податоци ќе бидат подеднакво ефикасно информирани (член 34(3)в).

Треба да се користат наменски пораки при известување за нарушувањето на безбедноста на субјектите на лични податоци и истите не треба да се испраќаат со други информации, како

[36] Види исто образложение 86.

што се редовни ажурирања, билтени или стандардни пораки. Ова помага известувањето за нарушувањето на безбедноста да биде јасно и транспарентно.

Примерите за транспарентни методи на комуникација вклучуваат директно испраќање на пораки (на пример, е-пошта, СМС, директна порака), истакнати банери на веб-страница или известување, поштенски комуникации и истакнати реклами во печатените медиуми. Известување кое е ограничено само во рамките на соопштение за печат или корпоративниот блог не би било ефикасно средство за известување на нарушување на безбедноста на физичко лице. РГ29 препорачува контролорите да изберат средства кои ја зголемуваат можноста за правилно соопштување на информациите до сите засегнати лица. Во зависност од околностите, ова може да значи дека контролорот користи неколку начини на известување, за разлика од користењето на еден канал за контакт.

Контролорите, исто така, може ќе треба да осигураат дека комуникацијата е достапна во соодветни алтернативни формати и релевантни јазици за да се обезбеди дека физичките лица можат да ги разберат информациите што им се дадени. На пример, кога се соопштува нарушувањето на бебедноста на физичко лице, ќе биде соодветен јазикот што се користел за време на претходниот нормален тек на деловно работење со примателот. Меѓутоа, ако нарушувањето на безбедноста влијае на субјектите на лични податоци со кои контролорот претходно не комуницирал, особено тие кои што живеат во друга земја - членка или друга земја што не е членка на ЕУ од каде што е воспоставен контролорот, комуникацијата на локалниот национален јазик би можела да биде прифатлива, земајќи го предвид потребниот ресурс. Клучот е да им помогнеме на субјектите на личните податоци да ја разберат природата на нарушувањето на безбедноста и чекорите што можат да ги преземат за да се заштитат.

Контролорите се најдобро поставени за да утврдат најсоодветен канал за контакт за да комуницираат нарушување на безбедноста на физички лица, особено ако тие комуницираат со нивните клиенти на редовна основа. Како и да е, јасно е дека контролорот треба да биде претпазлив кога користи канал за контактирање кој е компромитиран од нарушување на безбедноста, бидејќи овој канал може да се користи и од напаѓачите кои лажно се претставуваат како контролорот.

Во исто време, образложението 86 објаснува дека:

> „Ваквите комуникации до субјектите на лични податоци треба да бидат остварени штом тоа е разумно изводливо и во тесна соработка со надзорниот орган, почитувајќи ги насоките дадени од него или од други релевантни органи, како што се органите за спроведување на законот. На пример, на потребата за намалување на непосреден ризик од штета, ќе се бара веднаш да се известат субјектите на лични податоци, додека потребата за спроведување на соодветни мерки против други или слични нарушување на безбедноста на личните податоци може да оправда подолг период за известување.“

Затоа, контролорите можеби сакаат да контактираат и да се консултираат со надзорниот орган, не само за да бараат совети за известување на субјектите на лични податоци за нарушување на безбедноста, во согласност со член 34, туку и за соодветните пораки што треба да се испратат до поединците и најсоодветниот начин за контакт со нив.

Поврзано со ова, е советот даден во образложението 88 дека известувањето за нарушување на безбедност треба „да ги земе предвид легитимните интереси на органите за спроведување на законот, кога раното откривање може непотребно да ја попречи истрагата за околностите на нарушувањето на безбедноста на личните податоци.”. Ова може да значи дека во одредени околности, кога тоа е оправдано, а по совет на органите за спроведување на законот, контролорот може да го одложи известувањето за нарушувањето на безбедноста на засегнатите

лица, сè додека тоа не би наштетило на ваквите истраги. Сепак, субјектите на лични податоци сепак треба да бидат навремено известени по овој рок.

Секој пат кога не е возможно контролорот да го извести нарушувањето на безбедноста на физичко лице затоа што нема доволно собрани податоци за да се контактира со лицето, во таа конкретна околност контролорот треба да го извести физичкото лице веднаш штом тоа е разумно изводливо (на пр. кога некое физичко лице го остварува своето право според член 15 за пристап до лични податоци и му ги обезбедува на контролорот потребните дополнителни информации за контакт).

Г. Услови каде што не е потребно известување

Во членот 34(3) се наведени три услови кои, доколку се исполнети, не бараат известување за физичките лица во случај на нарушување на безбедноста. Тоа се:

- Контролорот презел соодветни технички и организациски мерки за заштита на личните податоци пред нарушувањето на безбедноста, особено мерките што ги прават личните податоци неразбирливи за секое лице кое нема дозвола за пристап до нив. Ова може, на пример, да вклучува заштита на личните податоци со најсовремена енкрипција или со означување на симболи (токени).
- Веднаш по нарушувањето на безбедноста, контролорот презел последователни мерки кои гарантираат дека веќе не постои веројатност да се материјализира високиот ризик за правата и слободите на субјектита на личните податоци. На пример, во зависност од околностите на случајот, контролорот можеби веднаш препознал и преземал дејствија против лицето кое имало пристап до лични податоци, пред тоа лице да можело да направи нешто со нив. Сепак, треба да се води сметка за можните последици од какво било нарушување на безбедноста на доверливоста, во зависност од природата на засегнатите лични податоци.
- Тоа би довело до непропорционални напори[37] за известување на физичките лица, можеби во случај кога нивните информации за контакт се изгубиле како резултат на нарушувањето на безбедноста или уште почетно не биле познати. На пример, магацинот на служба за статистика е поплавен, а документите што содржат лични податоци биле чувани само во хартиена форма. Во таков случај, контролорот прави јавно известување или се зема друга слична мерка со која субјектите на лични податоци ќе бидат подеднакво ефикасно информирани. Во случај на непропорционален напор, може да се предвидат и технички аранжмани со кои информациите за нарушувањето на безбедноста стануваат достапни на барање, што може да се покаже како корисно за оние лица кои може да бидат погодени од нарушување на безбедноста, но за кои контролорот нема начин да ги контактира.

Во согласност со принципот на одговорност, контролорите треба да бидат во можност да му покажат на надзорниот орган дека исполнуваат еден или повеќе од овие услови[38]. Треба да се има предвид дека иако првично може да не се бара известување доколку не постои ризик за правата и слободите на физичките лица, тоа може да се промени со текот на времето и ризикот ќе треба да се преиспита.

Ако контролорот одлучи да не го извести физичкото лице за нарушувањето на безбедноста, членот 34(4) објаснува дека надзорниот орган може да побара од контролорот да го стори тоа, доколку смета дека нарушувањето на безбедноста предизвикува висок ризик за физичките

[37] Погледнете ги насоките на РГ29 за транспарентност, кои ќе го разгледаат прашањето за непропорционален напор, на располагање на http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Види член 5(2)

лица. Патем речено, може да смета дека се исполнети условите од член 34(3) во кој случај не е потребно известување за физичките лица. Доколку надзорниот орган утврди дека одлуката да не се известуваат субјектите на лични податоци не е основана, може да размисли да ги искористи своите расположливи овластувања и санкции.

IV. Проценка на ризик и висок ризик

А. Ризикот како поттикнувач за известување

Иако, ОРЗЛП воведува барање за известување на нарушувањето на безбедноста, тоа не е обврска која треба да се спроведе во сите околности:

- Потребно е известување до надлежниот надзорен орган, освен ако нема веројатност дека нарушувањето на безбедноста би можело да предизвика ризик за правата и слободите на физичките лица.
- Соопштувањето на нарушувањето на безбедноста на физичкото лице се прави само кога веројатно ќе резултира во висок ризик за неговите права и слободи.

Ова значи дека веднаш откако има свесност за нарушување на безбедноста, од витално значење е контролорот не само да се обидува да го сопре инцидентот, туку треба да го процени и ризикот што може резултира од тоа. Постојат две важни причини за ова: прво, познавањето на веројатноста и потенцијалната сериозност на влијанието врз физичкото лице ќе му помогне на контролорот да преземе ефективни чекори за да може да го спречи нарушувањето на безбедноста и да се справи со него; второ, ќе му помогне да утврди дали е потребно известување до надзорниот орган а, доколку е потребно, на засегнатите лица.

Како што е објаснето погоре, потребно е известување за нарушување на безбедноста, освен доколку не е веројатно дека ќе резултира со ризик за правата и слободите на физичките лица, а клучниот поттикнувач кој предизвикува соопштување за нарушување на безбедноста на субјектите на лични податоци е таму каде што веројатно ќе резултира во *висок ризик* врз правата и слободите на физичките лица. Овој ризик постои кога нарушувањето на безбедноста може да доведе до физичка, материјална или нематеријална штета за лицата на чии лични податоци им била нарушена безбедноста. Примери за такви штети се дискриминација, кражба на идентитет или измама, финансиска загуба и штета на угледот. Кога нарушувањето на безбедноста вклучува лични податоци што откриваат расно или етничко потекло, политичко мислење, религија или филозофски убедувања, или членство во синдикатот, или вклучува генетски податоци, податоци во врска со здравјето или податоци во врска со сексуалниот живот, или кривични пресуди и криминални дела или сродни безбедносни мерки, таквата штета треба да се смета дека веројатно ќе се случи[39].

Б. Фактори што треба да се земат предвид при проценка на ризикот

Образложенијата 75 и 76 од ОРЗЛП укажуваат дека вообичаено при проценка на ризикот, треба да се земат предвид и веројатноста и сериозноста на ризикот за правата и слободите на субјектите на личните податоци. Во понатамошниот текст се наведува дека ризикот треба да се оценува врз основа на објективна проценка.

Треба да се напомене дека проценката на ризикот за правата и слободите на луѓето како резултат на нарушување на безбедноста има различен фокус од ризикот што се разгледува во Проценката на влијанието врз заштитата на личните податоци (ПВЗЛП)[40]. ПВЗЛП ги разгледува ризиците за обработката на личните податоци да се одвива како што е планирана и ризиците во случај на нарушување на безбедноста. Кога се разгледува можното нарушување на

[39] Види образложение 75 и образложение 85.
[40] Види насоки на Работната група за ПВЗЛП: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

безбедноста, таа општо гледа во веројатноста за појава на ова и на штетата што може да му настане на субјектот на личните податоци; со други зборови, тоа е проценка на хипотетички настан. Во случај на вистинско нарушување на безбедноста, настанот веќе се случил и затоа фокусот е целосно во врска со добиениот ризик од влијанието на нарушувањето на безбедноста врз физичките лица.

Пример

ПВЗЛП препорачува дека предложената употреба на одреден безбедносен софтверски производ за заштита на личните податоци е соодветна мерка за да се обезбеди ниво на безбедност соодветно на ризикот што обработката инаку би им го претставувала на физичките лица. Меѓутоа, ако ранливоста последователно стане позната, ова ќе ја промени соодветноста на софтверот да го спречи ризикот за заштитените лични податоци и би требало да се преиспита како дел од тековната ПВЗЛП. Понатаму се искористува ранливоста на производот и се појавува нарушување на безбедноста. Контролорот треба да ги процени специфичните околности на повредата, погодените лични податоци и потенцијалното ниво на влијание врз физичките лица, како и колку е веројатно овој ризик да се оствари.

Според тоа, при проценка на ризикот за физичките лица како резултат на нарушување на безбедноста, контролорот треба да ги земе предвид конкретните околности на нарушувањето на безбедноста, вклучително и сериозноста на потенцијалното влијание и веројатноста за тоа да се случи. Затоа, Работната група 29 препорачува проценката да ги земе предвид следниве критериуми[41]:

- Вид на нарушување на безбедноста

Видот на нарушувањето на безбедноста што се случил може да влијае на нивото на ризик претставен на физичките лица. На пример, нарушување на безбедноста на доверливоста со која медицинска информација им се открива на неовластени страни што може да има различно мноштво на последици за физичкото лице, до нарушување на безбедноста кога медицинските детали на физичкото лице се изгубени и повеќе не се достапни.

- Природата, чувствителноста и обемот на личните податоци

Се подразбира дека при проценка на ризикот, клучен фактор е видот и чувствителноста на личните податоци кои биле компромитирани со нарушувањето на безбедноста. Обично, колку се почуствителни личните податоци, толку е поголем ризикот од штета кај засегнатите лица, но треба да се земат предвид и другите лични податоци што може да бидат веќе достапни за субјектот на личните податоци. На пример, откривањето на името и адресата на физичкото лице во обични околности, веројатно нема да предизвика значителна штета. Меѓутоа, доколку името и адресата на родителот посвоител е откриена на биолошкиот родител, последиците може да бидат многу сериозни и за посвоителот и за детето.

Нарушувањата на безбедност кои вклучуваат здравствени податоци, лични документи или финансиски податоци, како што се детали за кредитни картички, сите самостојно можат да предизвикаат штета, но доколку се користат заедно, тие би можеле да се искористат за кражба на идентитет. Спој од лични податоци е обично почувствителен од еден единствен личен податок.

[41] Член 3.2 од Регулативата 611/2013 дава насоки за факторите што треба да се земат предвид во врска со известувањето за нарушувања на безбедноста во секторот на електронски комуникациски услуги, што може да биде корисно во контекст на известување под ОРЗЛП. Види http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Некои видови на лични податоци на почетокот може да изгледаат релативно безопасни, меѓутоа, треба внимателно да биде разгледано што тие лични податоци можат да откријат за засегнатото лице. Списокот на клиенти кои прифаќаат редовни испораки можеби не е особено чувствителен податок, но истите податоци за клиентите кои побарале да се запре нивната испорака за време на одмор, би претставувале корисни информации за криминалците.

Слично на тоа, мала количина на чувствителни лични податоци може да има големо влијание врз физичкото лице, како што и голем опсег на детали може да открие поголем опсег на информации за таа личност. Исто така, нарушување на безбедноста што влијае врз голем обем на лични податоци за многу субјекти на лични податоци, може да има последица врз соодветниот голем број на физички лица.

- Леснотијата на идентификација на физички лица

Важен фактор што треба да се разгледа е колку е лесно за странката која има пристап до компромитирани лични податоци да идентификува конкретни физички лица или да ги поврзе личните податоци со други информации за да идентификува поединци. Во зависност од околностите, идентификацијата би можела да биде возможна директно од нарушените лични податоци без да се потребни посебни истражувања за да се открие идентитетот на физичкото лице, или може да биде исклучително тешко да се совпаднат личните податоци со одредено физичко лице, иако сепак би можело да биде возможно под одредени услови. Идентификацијата може да биде директно или индиректно возможна преку нарушените лични податоци, но може да зависи и од конкретниот контекст на нарушувањето на безбедноста и од јавната достапност на засегнатите лични детали. Ова може да биде порелевантно за нарушувања на безбедност на доверливоста и достапноста.

Како што е наведено погоре, личните податоци заштитени со соодветно ниво на криптирање ќе бидат неразбирливи за неовластени лица без клучот за декрипција. Покрај тоа, соодветно спроведена псевдонимизација (дефинирана во член 4(5)) како „обработка на личните податоци на таков начин што личните податоци не можат повеќе да бидат поврзани со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки за да се обезбедни дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува“) исто така може да ја намали веројатноста за идентификација на физички лица во случај на нарушување на безбедноста. Сепак, само со користење на техниките за псевдонимизација не можат да се смета дека личните податоци се направени да бидат неразбирливи.

- Сериозност на последиците за физичките лица

Во зависност од природата на личните податоци кои се вклучени во нарушувањето на безбедноста, на пример, кога се работи за посебни категории на лични податоци, потенцијалната штета на физичките лица која би резултирала може да биде прилично сериозна, особено кога нарушувањето на безбедноста може да резултира во кражба на идентитет или измама, физичка штета, психолошка вознемиреност, понижување или оштетување на угледот. Ако нарушувањето на безбедноста се однесува на лични податоци на ранливи лица, тие може да се најдат во ситуација со поголем ризик од штета.

Дали контролорот е свесен дека личните податоци се во рацете на луѓе чии намери се непознати или евентуално злонамерни, може да има влијание врз нивото на потенцијалниот ризик. Може да има нарушување на безбедноста на доверливоста, при што по грешка личните податоци се објавени на трето лице, како што е дефинирано во член 4(10), или на друг примател. Ова може да се случи, на пример, кога личните податоци случајно се испраќаат на

погрешно одделение од една организација или на често користена организација на набавувачи. Контролорот може да побара од примателот или да ги врати или безбедно да ги уништи примените лични податоци. И во двата случаи, со оглед дека контролорот има постојан однос со нив и може да има сознание за нивните процедури, историја и други релевантни детали, примателот може да се смета за „доверлив“. Со други зборови, контролорот може да има ниво на убеденост во сигурноста на примателот, така што може разумно да очекува дека таа странка не чита или пристапува до личните податоци што се испратени по грешка и дека ги почитува сопствените упатства за да ги врати. Дури и ако пристапиле до личните податоци, контролорот сè уште може да му верува на примателот дека не презема дополнителни активности со нив и дека веднаш ќе му ги врати личните податоци на контролорот и ќе соработува за нивно обновување. Во вакви случаи, ова може да се земе предвид во проценката на ризикот што контролорот ја спроведува по нарушувањето на безбедноста - фактот дека на примателот му се верува може да ја поништи сериозноста на последиците од нарушувањето на безбедноста, но тоа не значи дека не се случило нарушување на безбедноста. Сепак, ова може да ја отстрани веројатноста за ризик кај физичките лица, со тоа што веќе не се бара известување до надзорниот орган или засегнатите лица. Повторно, ова ќе се проценува од случај до случај. Како и да е, контролорот сепак треба да чува информации во врска со нарушувањето на безбедноста како дел од општата должност да води евиденција за нарушувањата на безбедноста (види дел V, подолу).

Треба да се разгледа и трајноста на последиците за физичките лица, кога влијанието може да се смета за поголемо доколку ефектите се долгорочни.

- Посебни карактеристики на физичкото лице

Нарушувањето на безбедноста може да влијае на личните податоци што се однесуваат на деца или други ранливи лица, кои како резултат на тоа можат да бидат подложени на поголем ризик. Може да има и други фактори за физичкото лице кои можат да делуваат на нивото на влијанието на нарушувањето на безбедноста врз нив.

- Посебни карактеристики на контролорот на личните податоци

Природата и улогата на контролорот и неговите активности може да влијаат врз нивото на ризик за физичките лица како резултат на нарушување на безбедноста. На пример, медицинска организација ќе обработува посебни категории на лични податоци, што значи дека постои поголема закана за физичките лица доколку се наруши безбедноста на нивните лични податоци, во споредба со списокот со адреси за достава на весник.

- Бројот на засегнати лица

Нарушувањето на безбедноста може да влијае на само едно или неколку лица или неколку илјади, ако не и повеќе. Општо гледано, колку е поголем бројот на засегнати лица, толку е поголемо влијанието на нарушувањето на безбедноста. Сепак, нарушувањето на безбедноста може да има сериозно влијание дури и врз една личност, во зависност од природата на личните податоци и контекстот во кој е компромитирана таа личност. Повторно, клучно е да се разгледа веројатноста и сериозноста на влијанието врз тие што се засегнати.

- Општи точки

Затоа, при проценка на ризикот што може да биде резултат на нарушување на безбедноста, контролорот треба да размисли за комбинација на сериозноста на потенцијалното влијание врз правата и слободите на физичките лица и веројатноста за нивна појава. Јасно е дека, кога последиците од нарушување на безбедноста се посериозни, ризикот е поголем и на сличен начин кога веројатноста за нивна појава е поголема, ризикот исто така се зголемува. Доколку

има двоумење, контролорот треба да се одлучи на претпазливост и да извести. Прилогот Б дава неколку корисни примери на различни видови на нарушувања на безбедноста кои вклучуваат ризик или висок ризик за физичките лица.

Европската агенција за мрежна и информациска безбедност (ЕНИСА) донесе препораки за методологија за проценка на сериозноста на нарушувањето на безбедноста, кои контролорите и обработувачите може да сметаат дека се корисни при создавање на нивниот план за одговор при управување со нарушување на безбедноста[42].

V. **Одговорност и водење на евиденција**

А. Документирање на нарушувањата на безбедност

Без оглед дали нарушувањето на безбедноста треба да биде известено до надзорниот орган, контролорот мора да води документација за сите нарушувања на безбедноста, како што објаснува член 33(5):

„Контролорот ги документира сите нарушувања на безбедноста на личните податоци, вклучувајќи ги фактите поврзани со нарушувањето на безбедноста на личните податоци, нивните последици и преземените активности за справување со нарушувањето. Оваа документација му овозможува на надзорниот орган да ја провери усогласеноста со овој член.“

Ова е поврзано со принципот на одговорност на ОРЗЛП, содржан во член 5(2). Целта на евидентирање на нарушувања на безбедноста што не се известуваат, како и за нарушувања што се известуваат, исто така се однесува на обврските на контролорот според член 24, а надзорниот орган може да побара да ги види овие записи. Затоа, контролорите се охрабруваат да воспостават внатрешен регистар на нарушувањата на безбедност, без оглед дали се бара да известат или не[43].

Додека контролорот е тој кој треба да утврди каков метод и структура да се користи при документирање на нарушување на безбедноста, во однос на информацијата што може да се евидентира има клучни елементи што треба да бидат вклучени во сите случаи. Како што се бара во член 33(5), контролорот треба да запише детали во врска со нарушувањето на безбедноста, што треба да ги вклучи нејзините причини, што се случило и засегнатите лични податоци. Исто така, треба да ги вклучи ефектите и последиците од нарушувањето на безбедноста, заедно со поправните мерки преземени од контролорот.

ОРЗЛП не определува период на задржување на таквата документација. Кога таквите записи содржат лични податоци, на контролорот му е должност да го одреди соодветниот период на задржување во согласност со принципите во однос на обработката на личните податоци[44] и да исполни законска основа за обработка[45]. Треба да се зачува документацијата во согласност со член 33(5) доколку има можност да биде повикан да му обезбеди доказ за усогласеност со тој член или поопшто со принципот на одговорност, на надзорниот орган. Јасно е дека ако самите

[42] ЕНИСА, Препораки за методологија за проценка на сериозноста на нарушувањата на безбедност на личните податоци, https://www.enisa.europa.eu/publications/dbn-severity

[43] Контролорот може да избере да ги документира нарушувањата како дел од записите за активности за обработка кои се одржуваат во согласност со член 30. Не е потребен посебен регистар, доколку информациите што се релевантни на нарушувањето на безбедноста се јасно идентификуваат како такви и можат да бидат извлечени на барање.

[44] Види член 5

[45] Види член 6 и член 9.

записи не содржат лични податоци, тогаш не се применува принципот на ограничување на складирање[46] на ОРЗЛП.

Покрај овие детали, РГ29 препорачува контролорот да го документира и своето расудување за донесените решенија како одговор на нарушувањето на безбедноста. Особено, во случај ако не се извести нарушувањето на безбедност, треба да се документира оправданоста за таа одлука. Ова треба да вклучува причини зошто контролорот смета дека нарушувањето на безбедноста веројатно нема да резултира во ризик за правата и слободите на физичките лица.[47]. Во друга ситуација, ако контролорот смета дека се исполнети некои од условите од член 34(3), тогаш треба да биде во можност да обезбеди соодветни докази дека тоа е случајот.

Кога контролорот ќе извести за нарушување на безбедноста до надзорниот орган, но известувањето е одложено, контролорот мора да биде во можност да обезбеди причини за тоа одложување; документацијата во врска со ова може да помогне да се докаже дека доцнењето во известувањето е оправдано и не е претерано.

Кога контролорот им соопштува нарушување на безбедноста на засегнатите лица, треба да биде транспарентен за нарушувањето и да соопшти на ефективен и навремен начин. Согласно на тоа, ќе му биде од помош на контролорот да демонстрира одговорност и усогласеност преку чување на доказите од тоа соопштување.

За да се помогне во усогласување со членовите 33 и 34, поволно би било за контролорите и обработувачите да имаат воспоставено документирана постапка за известување, со одредување на процесот што треба да следи откако ќе се открие нарушување на безбедноста, вклучително и како да се спречи, да се управува и опорави од инцидентот, како и проценка на ризикот и известување за нарушувањето на безбедноста. Во овој поглед, за да се покаже усогласеност со ОРЗЛП, исто така може да биде корисно да се докаже дека вработените се информирани за постоењето на вакви постапки и механизми и дека тие знаат како да реагираат на нарушувања на безбедноста.

Треба да се напомене дека непостоењето на правилно документирање на нарушувањето на безбедноста може да доведе до тоа надзорниот орган да ги изврши своите овластувања според член 58 и или да одреди административна казна во согласност со член 83.

Б. Улога на офицерот за заштита на личните податоци

Контролорот или обработувачот може да има офицер за заштита на личните податоци (ОЗЛП)[48], или како што се бара во член 37, или доброволно како прашање на добра практика. Членот 39 од ОРЗЛП поставува голем број на задолжителни задачи за ОЗЛП, но не спречува да му бидат доделени понатамошни задачи од контролорот, доколку е тоа пригодно.

Од особено значење за известувањето за нарушување на безбедноста е дека задолжителните задачи на ОЗЛП вклучуваат, меѓу другите должности, давање совети и информации за заштита на личните податоци на контролорот или обработувачот, следење на усогласеноста со ОРЗЛП и давање совети во врска со ПВЗЛП. ОЗЛП исто така мора да соработува со надзорниот орган и да дејствува како точка за контакт за надзорниот орган и за субјектите на личните податоци. Исто така, треба да се напомене дека при известување за нарушување на безбедноста до надзорниот орган, членот 33(3)(б) наложува контролорот да ги наведе името и деталите за контакт на неговиот ОЗЛП, или на друга точка за контакт.

[46] Види член 5(1)(д).

[47] Види образложение 85

[48] Види насоки на РГ за ОЗЛП овде: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Во однос на документирање на нарушувања на безбедноста, контролорот или обработувачот може да посака да добие мислење од својот ОЗЛП за структурата, поставувањето и администрацијата на оваа документација. ОЗЛПто може да има и дополнителна задача да одржува вакви записи.

Овие фактори значат дека ОЗЛП треба да игра клучна улога во помагањето во спречување или подготовка за нарушување на безбедноста со давање совети и следење на усогласеноста, како и при нарушување на безбедноста (т.е. при известување на надзорниот орган), како и за време на секоја последователна истрага од страна на надзорниот орган. Во оваа смисла, РГ29 препорачува ОЗЛП да е веднаш информиран за постоење на нарушување на безбедноста и вклучен во целиот процес на управување и известување за нарушувањето.

VI. Обврски за известување според други правни инструменти

Додатно и одвоено од, известувањето и соопштувањето на нарушувањата на безбедност според ОРЗЛП, контролорите треба да бидат свесни за сите услови за известување на безбедносни инциденти според други придружни законодавства што може да важат за нив и дали тоа може да бара од нив да го известат надзорниот орган за нарушување на безбедноста на лични податоци во исто време. Ваквите барања може да варираат помеѓу земјите-членки, но примери на барања за известување во други правни инструменти и како овие меѓусебно се поврзани со ОРЗЛП, го вклучуваат следното:

- Регулатива (ЕУ) 910/2014 за електронска идентификација и доверливи услуги за електронски трансакции во внатрешниот пазар (регулатива еИДАС)[49].

Членот 19(2) од регулативата еИДАС бара од давателите на доверливи услуги да го известат надзорниот орган за нарушување на безбедноста или загубата на интегритетот што има значително влијание врз услугата за доверба или на личните податоци што се чуваат во нив. Таму каде што е применливо, т.е., кога таквото нарушување на безбедноста или загуба е исто така нарушување на безбедноста на личните податоци според ОРЗЛП - давателот на доверливата услуга исто така треба да го извести надзорниот орган.

- Директива (ЕУ) 2016/1148 во врска со мерките за обезбедување високо заедничко ниво на безбедност на мрежи и информациски системи ширум Унијата (НИС Директива)[50].

Членовите 14 и 16 од НИС Директивата бараат од операторите на основните услуги и давателите на дигитални услуги да ги известат безбедносните инциденти до нивниот надлежен орган. Како што е препознаено со образложението 63 од НИС[51], безбедносните инциденти честопати вклучуваат компромитирање на лични податоци. Додека НИС бара надлежните органи и надзорните органи да соработуваат и разменуваат информации за тој контекст, останува случајот кога такви инциденти се или стануваат нарушувања на безбедноста на личните податоци според ОРЗЛП, од тие оператори и/или давателите на услуги се бара да го известат надзорниот орган одделно од барањата за известување на инцидентот на НИС.

[49] Види http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[51] Образложение 63: *„Личните податоци во многу случаи се компромитирани како резултат на инциденти. Во овој контекст, надлежните органи и органите за заштита на личните податоци треба да соработуваат и да разменуваат информации за сите релевантни работи за да се решат сите нарушувања на безбедноста на личните податоци како резултат на инцидентите.“*

Пример

Давателот на услуги на облак кој известува за нарушување на безбедноста според Директивата НИС, исто така, можеби ќе треба да го извести контролорот, доколку ова вклучува нарушување на безбедноста на личните податоци. Слично на тоа, давателот на доверливата услуга што известува под еИДАС, исто така, може да биде потребно да го извести надлежниот орган за заштита на личните податоци во случај на нарушување на безбедноста.

- Директива 2009/136/ЕУ (Директива за правата на граѓаните) и Регулатива 611/2013 (Регулатива за известување на нарушување на безбедноста).

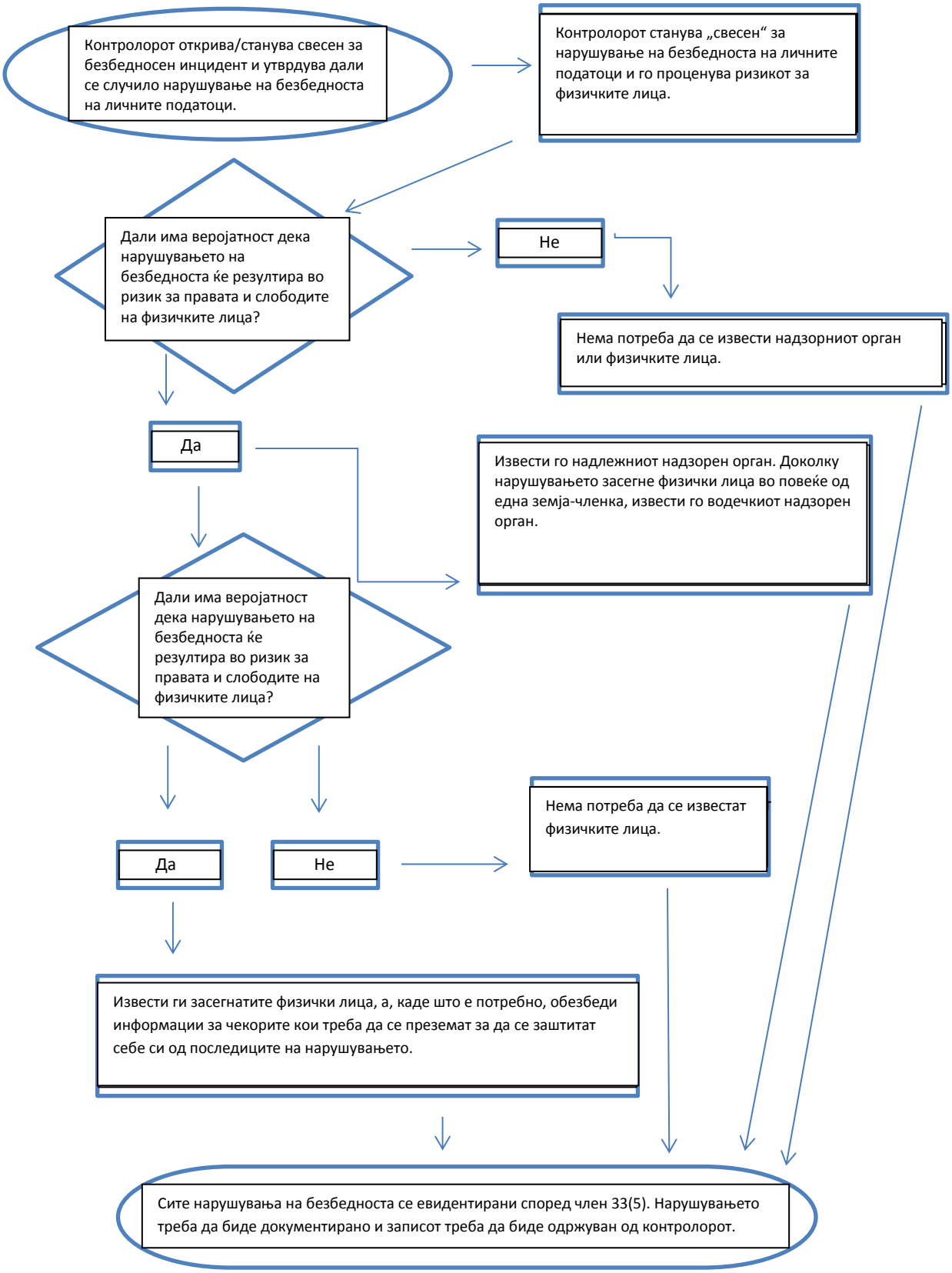
Давателите на услуги за јавно достапна електронска комуникација во контекст на Директивата 2002/58/ЕУ[52] мора да ги известат нарушувањата на безбедност на надлежните национални органи.

Контролорите исто така треба да бидат свесни за сите дополнителни правни, медицински или професионални должности за известување според други применливи режими.

[52] На 10 јануари 2017 година, Европската комисија предложи Регулатива за приватност и електронски комуникации што ќе ја замени Директивата 2009/136/ЕУ и ќе ги отстрани барањата за известување. Сепак, сè додека овој предлог не биде одобрен од страна на Европскиот парламент, постојното барање за известување останува во сила, види https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. **Прилог**

А. Дијаграм за прикажување на барањата за известување



Б. Примери за нарушувања на безбедноста на личните податоци и кој да биде известен

Следниов нецелосен список на примери ќе им помогне на контролорите да утврдат дали треба да известат во различни случаи за нарушување на безбедноста на личните податоци. Овие примери може да помогнат да се направи разлика помеѓу ризикот и високиот ризик за правата и слободите на физичките лица.

Пример	**Да се извести надзорниот орган?**	**Да се извести субјектот на личните податоци?**	**Забелешки/препораки**
i. Контролорот зачувал резервна копија на архива со лични податоци шифрирана на УСБ клуч. Клучот е украден за време на кражба.	Не.	Не.	Сè додека личните податоци се криптирани со алгоритам на најсовремената технологија, резервните копии на личните податоци постојат, единствениот клуч не е компромитиран, а податоците можат да бидат обновени со време, ова може да не е нарушување на безбедноста што треба да се пријави. Меѓутоа, ако подоцна биде компромитиран, потребно е известување.
ii. Контролорот одржува услуга на интернет. Како резултат на кибер напад врз таа услуга, личните податоци на физичките лица се извадени. Контролорот има корисници во една земја-членка.	Да, пријавете до надлежниот надзорен орган ако има веројатност за последици врз физички лица.	Да, пријавете им на физичките лица во зависност од природата на засегнатите лични податоци и дали сериозноста на веројатните последици врз лицата е голема.	

iii. Краток прекин на напојувањето трае неколку минути во центар за повици на контролорот што значи дека корисниците не можат да го повикаат контролорот и да пристапат до нивните записи.	Не.	Не.	Ова нарушување на безбедноста не се известува, но сепак инцидентот може да се документира според член 33(5). Контролорот треба да ги одржува соодветните записи.
iv. Контролорот страда од напад на уценувачки софтвер, што резултира во криптирање на сите лични податоци. Нема достапни резервни копии и личните податоци не можат да бидат обновени. При истрагата, станува јасно дека единствената функција на уценувачкиот софтвер била да ги криптира личните податоци и дека нема присуство на друг штетен софтвер во системот.	Да, пријави до надзорниот орган, доколку има веројатност за последици врз физичките лица бидејќи ова е оневозможување на достапноста.	Да, пријавете им на физичките лица, во зависност од природата на засегнатите лични податоци и можниот ефект од недостигот на достапност на личните податоци, како и од другите можни последици.	Доколку има достапна резервна копија и личните податоци може да бидат вратени со време, нема потреба ова да се пријавува до надзорниот орган или на физичките лица бидејќи нема да има трајно губење на достапноста или доверливоста. Меѓутоа, доколку надзорниот орган се запознал со инцидентот преку други средства, може да размисли за истрага за проценка на усогласеноста со пошироките безбедносни барања од член 32.
v. Лице телефонира во телефонскиот центар на банката за да пријави нарушување на безбедноста на личните податоци. Лицето добило месечен извод за некој друг. Контролорот презема кратка истрага (т.е. завршена во рок од 24 часа) и утврдува со разумна доверба дека се случило нарушување на безбедноста на личните податоци и дали има системска	Да.	Само засегнатите лица се известени доколку постои висок ризик и е јасно дека други лица не биле засегнати.	Доколку, по понатамошно испитување, се утврди дека се засегнати повеќе лица, мора да се извести надзорниот орган и контролорот презема дополнителен чекор за известување на други лица доколку за нив постои висок ризик.

маана што може да значи дека други лица се или може да бидат засегнати.			
vi. Контролорот работи на интернет пазар и има клиенти во повеќе земји-членки. Пазарот страда од кибер напад и корисничките имиња, лозинките и историјата на купувањето се објавуваат на интернет од напаѓачот.	Да, пријави до водечкиот надзорен орган ако вклучува прекугранична обработка.	Да, затоа што може да доведе до висок ризик.	Контролорот треба да преземе акција, на пр. со принудување на ресетирање на лозинките на погодените сметки, како и други чекори за ублажување на ризикот. Контролорот треба да земе предвид и други обврски за известување, на пр. според Директивата НИС (NIS) како давател на дигитални услуги.
vii. Компанија за хостирање на веб-страница што дејствува како обработувач на лични податоци наоѓа грешка во кодот што го контролира овластувањето на корисникот. Ефектот на маната значи дека секој корисник може да пристапи до деталите за сметката на кој било друг корисник.	Како обработувач, компанијата за хостирање на веб-страници мора да ги извести засегнатите клиенти (контролорите) без непотребно одложување. Под претпоставка дека компанијата за хостирање на веб-страницата спровела своја истрага, погодените контролори треба да бидат разумно сигурни во однос на тоа дали секој претрпел нарушување на безбедноста и затоа веројатно ќе се смета дека „станале свесни“ откако ќе бидат известени од страна на хостинг компанија (обработувачот). Контролорот тогаш мора да го извести	Доколку постои веројатност дека нема висок ризик за физички лица, тие не треба да бидат известени.	Компанијата за хостирање на веб-страница (обработувач) мора да ги земе предвид сите други обврски за известување (на пр. според НИС Директивата како давател на дигитални услуги). Доколку нема докази дека оваа ранливост е експлоатирана кај било кој од нејзините контролори, можно е да не се случило нарушување на безбедноста што треба да се извести, но веројатно треба да се документира или може да се смета за непочитување според член 32.

	надзорниот орган.		
viii. Медицинските записи во болница се недостапни за период од 30 часа, како резултат на кибер напад.	Да, болницата е должна да извести дека може да се појави висок ризик за благосостојбата на пациентот и неговата приватност.	Да, пријавете на засегнатите лица.	
ix. Личните податоци на голем број студенти погрешно се испратени на погрешен поштенски список за испраќање со 1000+ примачи.	Да, пријави до надзорниот орган.	Да, пријавете на физичките лица во зависност од обемот и видот на вклучените лични податоци и сериозноста на можните последици.	
x. Е-пошта за директен маркетинг се испраќа до примателите во полињата „до:“ или „ЦЦ:“, со што му се овозможува на секој примател да ја види адресата за е-пошта на другите примателi.	Да, известувањето за надзорниот орган може да биде задолжително ако се засегнати голем број на лица, доколку се откриени чувствителни податоци (на пр. поштенски список на психотерапевт) или ако други фактори претставуваат високи ризици (на пр. поштата ги содржи почетните лозинки).	Да, пријавете на физичките лица во зависност од обемот и видот на вклучените лични податоци и сериозноста на можните последици.	Известувањето може да не е потребно ако не се откриваат чувствителни податоци и ако се открие само мал број на адреси за е-пошта.