18/BG

WP250rev.01

Насоки относно уведомяването за нарушения на сигурността на личните данни съгласно Регламент (ЕС) 2016/679

Приети на 3 октомври 2017 г.

Последно преработени и приети на 6 февруари 2018 г.

Тази работна група бе създадена по силата на член 29 от Директива 95/46/ЕО. Тя е независим европейски консултативен орган за защитата на личните данни и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът се осигурява от Дирекция С („Основни права и гражданство на Съюза“) на Европейската комисия, Генерална дирекция „Правосъдие", B-1049 Brussels, Belgium, офис No MO-59 02/013.

Уебсайт: https://ec.europa.eu/info/law/law-topic/data-protection_bg

РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ,

създадена с Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ

С Общия регламент относно защитата на данните (ОРЗД) се въвеждат изискването за уведомяване при нарушение на сигурността на лични данни (наричано по-долу „нарушение“) на компетентния национален надзорен орган[1] (или в случай на трансгранично нарушение, на водещия орган) и изискването в определени случаи да се съобщава за нарушението на физическите лица, чиито лични данни са били засегнати от нарушението.

Задължения за уведомяване при случаи на нарушения съществуват понастоящем за определени организации, като доставчиците на публично достъпни електронни комуникационни услуги (както е посочено в Директива 2009/136/ЕС и Регламент (ЕС) № 611/2013)[2]. Някои държави — членки на ЕС, също имат вече свое собствено национално задължение за уведомяване при нарушение. То може да включва задължението за уведомяване за нарушения, когато освен доставчици на публично достъпни електронни комуникационни услуги са засегнати някои категории администратори на лични данни (напр. в Германия и Италия), или задължение за докладване на всички нарушения, засягащи лични данни (напр. в Нидерландия). Други държави членки може да имат съответни кодекси на практиките (напр. в Ирландия[3]). Редица органи на ЕС за защита на данните насърчават понастоящем администраторите на лични данни да съобщават за нарушения, но в Директива 95/46/ЕО[4] за защита на данните, заменена от ОРЗД, няма изрично задължение за уведомяване при нарушение, така че такова изискване ще бъде новост за много организации. Сега с ОРЗД уведомяването става задължително за всички администратори на лични данни, освен ако липсва вероятност нарушението да породи риск за правата и свободите на физическите лица[5]. Обработващите лични данни също изпълняват важна роля и са длъжни да уведомяват за всяко нарушение своя администратор на лични данни[6].

Работната група по член 29 (РГ 29) е на мнение, че новото изискване за уведомяване има ред предимства. Когато уведомяват надзорните органи, администраторите на лични данни могат да получат съвет за това дали засегнатите физически лица трябва да бъдат информирани. Всъщност надзорният орган може да нареди на администратора на лични данни да информира тези физически лица относно нарушението[7]. Уведомяването на физическите лица за нарушение дава възможност на администратора на лични данни да предостави информация относно рисковете, възникнали в резултат на нарушението, и стъпките, които тези физически лица могат да предприемат, за да се предпазят от възможните последици от него. Ударението

[1] Вж. член 4, параграф 21 от ОРЗД.

[2] Вж. https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex:32009L0136 и https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32013R0611

[3] Вж. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Вж. https://eur-lex.europa.eu/legal-content/EN-BG/TXT/?uri=CELEX:31995L0046&from=BG

[5] Правата, залегнали в Хартата на основните права на ЕС, на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:12012P/TXT

[6] Вж. член 33, параграф 2. Тази концепция е сходна с разпоредбите на член 5 от Регламент (ЕС) № 611/2013, който гласи, че доставчик, който е ангажиран с доставянето на част от електронната съобщителна услуга (без да е в преки договорни отношения с абонатите), е длъжен да уведоми доставчика, който го е ангажирал, в случай на нарушение, свързано с личните данни.

[7] Вж. член 34, параграф 4 и член 58, параграф 2, буква д).

при всеки план за реагиране при нарушение следва да бъде поставено върху защитата на физическите лица и техните лични данни. Следователно уведомяването за нарушение следва да се разглежда като инструмент за засилване на спазването на изискванията за защита на личните данни. Същевременно следва да се отбележи, че неизпълнение на задължението за съобщаване на нарушение на физическо лице или надзорен орган може да означава, че по силата на член 83 на администратора на лични данни може да бъде наложена глоба.

Администраторите и обработващите лични данни се приканват поради тази причина да планират предварително и да въвеждат процеси, които да им дават възможност да открият и бързо да ограничат нарушение, да оценят риска за физическите лица[8], след което да определят дали е необходимо да се уведоми компетентният надзорен орган и да съобщят на физическите лица за нарушението, ако трябва. Уведомяването на надзорния орган следва да бъде част от този план за реагиране при инцидент.

В ОРЗД се съдържат разпоредби относно това кога и кой трябва да бъде уведомен за дадено нарушение, както и каква информация да се предостави като част от уведомяването. Информацията, която се изисква за уведомяването, може да бъде предоставена на етапи, но във всички случаи администраторите на лични данни следва да реагират своевременно при всяко нарушение.

В своето Становище 03/2014 относно уведомяване за нарушаване на защитата на личните данни[9] РГ 29 предостави указания на администраторите на лични данни, които да им помогнат да решат дали да уведомят субектите на данни в случай на нарушение. В становището се разглежда задължението на доставчиците на електронни съобщителни услуги във връзка с Директива 2002/58/ЕО и са дадени примери от множество сектори в контекста на тогавашния проект на ОРЗД, като са представени и добри практики за всички администратори на лични данни.

В настоящите насоки се съдържат пояснения за задължителното уведомяване за нарушение и изискванията за съобщаване съгласно ОРЗД, както и някои от стъпките, които администраторите и обработващите лични данни могат да предприемат за изпълнението на тези нови задължения. В тях са дадени също така примери за различни видове нарушения и за това кой трябва да бъде уведомен при различни сценарии.

I. Уведомяване за нарушения на сигурността на личните данни съгласно ОРЗД

A. Основни съображения за сигурност

Едно от изискванията на ОРЗД е, че с помощта на подходящи технически и организационни мерки личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане[10].

[8] Това може да се направи съгласно изискването за наблюдение и проверка на оценката на въздействието върху защитата на данните, която е задължителна за операции по обработване на данни, за които има вероятност да породят висок риск за правата и свободите на физическите лица (член 35, параграфи 1 и 11).

[9] Вж. Становище 03/2014 относно уведомяване за нарушаване на защитата на личните данни http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_bg.pdf

[10] Вж. член 5, параграф 1 и член 32.

Следователно ОРЗД изисква от администраторите и обработващите лични данни да разполагат с подходящи технически и организационни мерки, чието ниво на сигурност отговаря на риска, на който са изложени обработваните лични данни. Те следва да вземат предвид достиженията на техническия прогрес, разходите по изпълнението, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица[11]. Освен това ОРЗД изисква да бъдат приложени всички подходящи мерки за технологична защита и организационни мерки, за да се определи незабавно дали е налице нарушение на лични данни, от което след това зависи дали да бъде задействано задължението за уведомяване[12].

Следователно ключов елемент от всяка политика за сигурност на данните е способността, когато това е възможно, да се предотврати дадено нарушение, а ако то все пак настъпи, да се реагира своевременно.

Б. Какво означава нарушение на сигурността на лични данни?

1. Определение

Като част от всеки опит за предотвратяване на нарушение администраторът на лични данни трябва първо да може да го разпознае. ОРЗД определя „нарушение на сигурността на лични данни“ в член 4, параграф 12 като:

> „нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.“

Следва да е съвсем ясно какво се има предвид под „унищожаване“ на лични данни: то е налице, когато данните вече ги няма или ги няма във вид, в който администраторът на лични данни да може да ги използва. Терминът „повреждане“ също следва да е относително ясен: то е налице, когато личните данни са променени, подправени или станали вече непълни. „Загубата“ на лични данни следва да се тълкува като състояние, когато те може да са все още налични, но администраторът на лични данни е загубил контрол или достъп до тях или те не са вече притежавани от него. И накрая, неразрешеното или неправомерното обработване може да включва разкриване на лични данни пред (или достъп до тях на) получатели, които не са оправомощени да ги получат (или да имат достъп до тях), или всеки друг вид обработване, което е в нарушение на ОРЗД.

Пример

Пример за загуба на лични данни е, когато устройство, съдържащо копие от база данни на клиент на администратора, е било загубено или откраднато. Друг пример за загуба е, когато единственото копие на набор от лични данни е било криптирано от софтуер за изнудване или от администратора с използване на код, който не е вече притежаван от него.

Следва да стане ясно, че нарушението е вид инцидент, свързан със сигурността. Както е посочено обаче в член 4, параграф 12, ОРЗД се прилага само когато има нарушение на сигурността на *лични данни*. Последицата от такова нарушение е, че администраторът на лични данни няма да има възможност да гарантира спазването на принципите, свързани с

[11] Член 32; вж. също така съображение 83.

[12] Вж. съображение 87.

обработването на лични данни, изложени в член 5 от ОРЗД. Оттук става ясна разликата между инцидент, свързан със сигурността, и нарушение на сигурността на лични данни — по същество, докато всички нарушения на сигурността на лични данни са инциденти, свързани със сигурността, не всички инциденти, свързани със сигурността, са непременно нарушения на сигурността на лични данни[13].

По-долу са разгледани потенциалните неблагоприятни последици от нарушенията за физическите лица.

2. Видове нарушения на сигурността на личните данни

В своето Становище 03/2014 относно уведомяване за нарушаване РГ 29 пояснява, че нарушенията могат да бъдат категоризирани по следните три, добре известни принципи на информационната сигурност[14]:

- „Нарушение на поверителността“ — когато има неразрешено или случайно разкриване или достъп до лични данни.
- „Нарушение на целостта“ — когато има неразрешена или случайна промяна на лични данни.
- „Нарушение на наличността“ — когато има неразрешена или случайна загуба на достъп[15] до или унищожаване на лични данни.

Следва да се отбележи също така, че в зависимост от обстоятелствата нарушението може да засегне поверителността, целостта и наличността на личните данни, както и каквато и да е комбинация от тях.

Да се определи дали е имало нарушение на поверителността или целостта е сравнително лесно, но не е толкова очевидно дали е имало нарушение на наличността. Нарушението се разглежда винаги като нарушение на наличността, когато има трайна загуба или трайно унищожаване на лични данни.

Пример

Сред примерите за загуба на наличността са случаи, когато данните са били заличени случайно или от неоправомощено лице, или пък ако данните са били сигурно криптирани, е бил загубен ключът за декриптиране. В случай че администраторът на лични данни не може да възстанови достъпа до тях, например от резервно копие, тогава се приема, че има трайна загуба на наличността.

[13] Следва да се отбележи, че инцидентите, свързани със сигурността, не се ограничават само до модели на опасност, при които дадена организация е атакувана от външен източник, а включват инциденти при вътрешно обработване, което нарушава принципите на сигурност.

[14] Вж. Становище 03/2014.

[15] Добре известно е, че „достъпът“ е основна част от „наличността“. Вж. например NIST SP800-53rev4, където „наличността“ е определена като: „осигуряване на своевременен и надежден достъп до и използване на информация“, достъпен на:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. В CNSSI-4009 също така е посочено, че „наличността“ е: „осигуряване на своевременен и надежден достъп до и използване на информация“, достъпен на: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. В ISO/IEC 27000:2016 „наличността“ също е определена като: „свойството на информацията да е достъпна и използваема при поискване от оправомощена единица“: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Загуба на наличността може да е налице и когато е имало значителни смущения в нормалната работа на дадена организация, като например прекъсване на електрозахранването или атака с цел отказ от обслужване, което води до спиране на наличността на личните данни.

Може да се постави въпросът дали временната загуба на наличността на лични данни следва да се разглежда като нарушение и ако е така, като такова, което подлежи на уведомяване. В член 32 от ОРЗД „Сигурност на обработването“ се пояснява, че когато се прилагат подходящи технически и организационни мерки за гарантиране на съобразено с този риск ниво на сигурност, внимание следва да се обърне, наред с други неща, на „способността за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване“ и на „способността за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент“.

Следователно инцидент, свързан със сигурността, който води до загуба на наличността на лични данни за определен период от време, също е вид нарушение, тъй като липсата на достъп до данните може да окаже значително въздействие върху правата и свободите на физическите лица. За повече яснота, когато личните данни не са налични поради извършване на планова поддръжка на системата, това не е „нарушение на сигурността на лични данни“ съгласно определението в член 4, параграф 12.

Както при трайна загуба или трайно унищожаване на лични данни (или всъщност както при всеки друг вид нарушение), нарушението, представляващо временна загуба на наличността, следва да бъде документирано в съответствие с член 33, параграф 5. Това помага на администратора на лични данни да се отчете пред надзорния орган, който може да поиска да види тази документация[16].В зависимост обаче от обстоятелствата при нарушението, то може да изисква или да не изисква уведомяване на надзорния орган и съобщаване на засегнатите физически лица. Администраторът ще трябва да прецени вероятността от и тежестта на въздействието за правата и свободите на физическите лица в резултат на липсата на наличност на личните данни. В съответствие с член 33 администраторът ще трябва да уведоми, освен ако липсва вероятност нарушението да породи риск за правата и свободите на физическите лица. Разбира се, тази оценка трябва да се направи конкретно за всеки отделен случай.

Примери

Ако в болнични условия се прекъсне, дори временно, наличността на медицински данни от решаващо значение за пациентите, това може да представлява риск за правата и свободите на физическите лица, може например да бъдат отложени операции с риск за живота на засегнатите.

От друга страна, в случай че системите на дадено медийно дружество откажат работа в течение на няколко часа (напр. поради прекъсване на електрозахранването) и ако в резултат на това на дружеството бъде попречено да изпраща бюлетини на своите абонати, няма вероятност това да представлява риск за правата и свободите на физическите лица.

Следва да се отбележи, че дори ако загубата на наличност на системите на администратора се окаже само временна и не доведе до въздействие за физическите лица, е важно администраторът на лични данни да разгледа всички възможни последици от нарушението, тъй като то може все пак да налага уведомяване по други причини.

Пример

[16] Вж. член 33, параграф 5.

Заразяването със софтуер за изнудване (зловреден софтуер, който криптира данните на администратора, докато не бъде платен откуп) може да доведе до временна загуба на наличност, ако има възможност данните да бъдат възстановени от резервно копие. Имало е все пак влизане в мрежата и уведомяване може да се наложи, ако инцидентът бъде окачествен като нарушение на поверителността (т.е. атакуващият е имал достъп до личните данни), а това представлява риск за правата и свободите на физическите лица.

3. Възможни последици от дадено нарушение на сигурността на лични данни

Нарушението може евентуално да предизвика редица значителни неблагоприятни последици за физическите лица, които може да породят физически, материални или нематериални вреди. В ОРЗД се пояснява, че това може да включва загуба на контрол върху личните им данни, ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизация, накърняване на репутацията и нарушаване на поверителността на лични данни, защитени от професионална тайна. Това може да включва и всякакви други значителни икономически или социални неблагоприятни последствия за тези физически лица[17].

Следователно ОРЗД задължава администратора да уведоми за нарушение компетентния надзорен орган, освен ако липсва вероятност нарушението да породи риск от настъпването на такива неблагоприятни последици. Когато има голяма вероятност и риск да настъпят тези неблагоприятни последици, ОРЗД задължава администратора да уведоми за нарушението засегнатите физически лица веднага щом това е разумно осъществимо[18].

Значението на способността да се установи нарушението, да се извърши оценка на риска за физическите лица и след това да се изпрати, ако е необходимо, уведомление е подчертано в съображение 87 от ОРЗД:

„Следва да се установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки, за да се определи незабавно дали е налице нарушение на лични данни и своевременно да се информират надзорният орган и субектът на данни. Фактът, че уведомлението е направено без ненужно забавяне следва да бъде установен, като се отчитат по-конкретно естеството и тежестта на нарушението на личните данни и последиците и неблагоприятното въздействие от него върху субекта на данни. Такова уведомление може да доведе до намесата на надзорния орган в съответствие със задачите и правомощията, които са му предоставени с настоящия регламент.“

Допълнителни насоки относно извършването на оценка на риска от неблагоприятни последици за физическите лица са представени в раздел IV.

Ако администраторите не изпълнят задължението си да уведомят надзорния орган или субектите на данни за нарушение на сигурността на данните, въпреки че са изпълнени изискванията по член 33 и/или член 34, надзорният орган е изправен пред избор, който трябва да включва разглеждането на всички корективни мерки, с които разполага, а това включва разглеждането на възможността за налагане на подходящо административно наказание „глоба“

[17] Вж. също така съображения 85 и 75.

[18] Вж. също така съображение 86.

или „имуществена санкция“ [19], в допълнение към корективна мярка по член 58, параграф 2 или самостоятелно. Когато бъде избрано административно наказание „глоба“ или „имуществена санкция“, неговият размер може да бъде до 10 000 000 EUR или до 2 % от общия годишен световен оборот на предприятието съгласно член 83, параграф 4, буква а). Важно е също така да се има предвид, че в някои случаи неизпълнението на задължението да се уведоми за нарушение може да е признак за липса на съществуващи мерки за сигурност или за недостатъчност на съществуващите мерки за сигурност. В насоките на РГ 29 относно административните наказания „глоба“ или „имуществена санкция“ се посочва: „При наличието на няколко отделни нарушения, извършени заедно в рамките на конкретен единичен случай, надзорният орган може да наложи административни наказания „глоба“ или „имуществена санкция“ на ниво, което е ефективно, пропорционално и възпиращо, като не надхвърля максималния размер за най-тежкото нарушение.“ В този случай надзорният орган ще има също възможността да налага наказания за неизпълнение на задължението за уведомяване или съобщаване на нарушение (членове 33 и 34), от една страна, и за липса на (подходящи) мерки за сигурност (член 32), от друга, тъй като става въпрос за две отделни нарушения.

II. **Член 33 — Уведомяване на надзорния орган**

A. Кога да се уведомява

1. Изисквания съгласно член 33

В член 33, параграф 1 се предвижда, че:

> „В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган, компетентен в съответствие с член 55, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.“

Съображение 87 гласи[20]:

> „Следва да се установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки, за да се определи незабавно дали е налице нарушение на лични данни и своевременно да се информират надзорният орган и субектът на данни. Фактът, че уведомлението е направено без ненужно забавяне следва да бъде установен, като се отчитат по-конкретно естеството и тежестта на нарушението на личните данни и последиците и неблагоприятното въздействие от него върху субекта на данни. Такова уведомление може да доведе до намесата на надзорния орган в съответствие със задачите и правомощията, които са му предоставени с настоящия регламент.“

2. Кога администраторът е „разбрал“ за нарушението?

[19] За допълнителни подробности можете да видите Насоки на РГ 29 прилагането и определянето на административните наказания „глоба“ или „имуществена санкция“, на следния адрес: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

[20] В случая е важно и съображение 85.

Както бе посочено с повече подробности, ОРЗД изисква в случай на нарушение администраторът да уведоми за нарушението без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него. Възниква въпросът за това кога може да се приеме, че администраторът е „разбрал“ за дадено нарушение. Според Работната група по член 29 се приема, че администраторът е „разбрал“, когато е установил с разумна степен на увереност, че е настъпил инцидент, свързан със сигурността, който е повлиял на личните данни.

ОРЗД обаче задължава администратора, както беше вече посочено, да приложи всички подходящи мерки за технологична защита и организационни мерки, за да определи незабавно дали е налице нарушение и своевременно да информира надзорния орган и субектите на данни. Според регламента следва освен това да бъде установен фактът, че уведомлението е направено без ненужно забавяне, като се отчитат по-конкретно естеството и тежестта на нарушението и последиците и неблагоприятното въздействие от него върху субекта на данни[21]. Това задължава администраторите да гарантират, че ще „разберат“ своевременно за евентуални нарушения, за да могат да вземат подходящи мерки.

Кога точно може да се приеме, че администраторът е „разбрал“ за дадено нарушение, ще зависи от обстоятелствата при конкретното нарушение. В някои случаи от самото начало става сравнително ясно, че е имало нарушение, докато в други може да отнеме известно време, за да се установи дали личните данни са били повлияни. Приоритетът обаче следва да бъде върху незабавните действия за разследване на всеки инцидент, за да се определи дали сигурността на личните данни е била наистина нарушена и ако е така, да се предприемат действия за справяне със ситуацията и да се уведоми за нея, ако се налага.

Примери

1. В случая на загуба на устройство за съхранение на данни с USB интерфейс, в което има некриптирани лични данни, често е невъзможно да се установи със сигурност дали неоправомощени лица са получили достъп до тези данни. Въпреки това, макар администраторът да не може да установи дали е имало нарушение на поверителността, за такъв случай трябва да се уведоми, тъй като има разумна степен на увереност, че е настъпило нарушение на наличността; администраторът ще „разбере“ за нарушението, когато му стане ясно, че е загубено устройството за съхранение на данни с USB интерфейс.

2. Трета страна уведомява администратора, че е получила случайно личните данни на един от своите клиенти и представя доказателство за неразрешеното разкриване. Тъй като на администратора е било представено ясно доказателство за нарушение на поверителността, извън съмнение е, че той е „разбрал“ за него.

3. Администратор открива, че е имало възможно проникване в неговата мрежа. Той проверява своите системи, за да установи дали лични данни, съхранявани в тази система, са били повлияни и потвърждава, че случаят е такъв. Отново, тъй като администраторът има сега ясно доказателство за нарушение, не може да има съмнение, че той е „разбрал“ за него.

4. Киберпрестъпник установява контакт с администратора, след като е хакнал системата му с цел да поиска откуп. В този случай, след като провери системата си, за да потвърди, че е била атакувана, администраторът има ясно доказателство, че е настъпило нарушение и е извън съмнение, че той е „разбрал“ за него.

[21] Вж. съображение 87.

След като е бил първо уведомен за възможно нарушение от физическо лице, медийна организация или друг източник, или когато сам е открил инцидент, свързан със сигурността, администраторът може да проведе кратко разследване, за да установи дали наистина е станало нарушение. През този период на разследване не може да се приеме, че администраторът е „разбрал“. Очаква се обаче първоначалното разследване да започне във възможно най-кратък срок и да установи с разумна степен на увереност дали е имало нарушение; след това може да се направи по-задълбочено разследване.

Щом администраторът разбере за него, за всяко подлежащо на уведомяване нарушение трябва да се уведоми без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа. През този период администраторът следва да извърши оценка на вероятния риск за физическите лица с цел да се определи, дали е задействано изискването за уведомяване, както и какво действие (какви действия) са необходими за справяне с нарушението. Възможно е обаче администраторът да разполага вече с първоначална оценка на потенциалния риск в резултат на нарушение като част от оценка на въздействието върху защитата на данните[22], направена преди извършване на съответната операция по обработване на данни. Оценката на въздействието върху защитата на данните може обаче да се окаже по-обобщена в сравнение с конкретните обстоятелства на дадено действително нарушение, така че във всички случаи ще трябва да се направи допълнителна оценка, отчитаща тези обстоятелства. За допълнителни подробности относно оценки на риска вж. раздел IV.

В повечето случаи тези предварителни действия следва да се извършат скоро след първия предупредителен сигнал (т.е. когато у администратора или обработващия лични данни възникне подозрение, че е имало инцидент, свързан със сигурността, който може да е засегнал лични данни) — по-дълго време би отнело само в изключителни случаи.

Пример

Дадено физическо лице уведомява администратора, че е получило електронно писмо от името на администратора, съдържащо лични данни във връзка с (действително) използване от самия него на услугата му, което е признак, че сигурността на администратора е изложена на риск. Администраторът провежда кратко разследване и установява проникване в своята мрежа и доказателство за неразрешен достъп до лични данни. Приема се, че сега вече администраторът е „разбрал“ за нарушението и се налага уведомяване на надзорния орган, освен ако липсва вероятност нарушението да доведе до риск за правата и свободите на физическите лица. Администраторът ще трябва да предприеме подходящи коригиращи действия за справяне с нарушението.

За тази цел администраторът следва да разполага с вътрешни процеси, даващи възможност за откриване и справяне с нарушението. Така например за откриване на някои нередности при обработването на данни администраторът или обработващия данните може да използва определени технически средства, като анализатори на потоци от данни или на данни от дневници, които дават възможност за установяване на събития и предупредителни сигнали чрез установяване на взаимовръзките между данни от дневници[23]. Важно е, когато се открие нарушение, то да бъде докладвано нагоре по веригата до подходящото управленско ниво за

[22] Вж Насоките на РГ 29 относно оценката на въздействието върху защитата на данните тук: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[23] Следва да се отбележи, че данните от дневници, спомагащи за одитируемостта напр. на съхранение, изменения или заличаване на данни, може да се определят и като лични данни, отнасящи се до лицето, започнало съответната операция по обработване.

справяне с него и, ако трябва, да се изпрати уведомление в съответствие с член 33, а при необходимост и в съответствие с член 34. Подробности за такива мерки и механизми за докладване може да бъдат включени в плановете на администратора за реагиране при инцидент и/или в мерките за управление. Те ще помогнат на администратора да планира ефективно дейността си и да определи кой в организацията отговаря оперативно за управлението на нарушенията и как и в какви случаи да се признае значимостта на даден инцидент.

Администраторът трябва също така да има установени договорености с всички обработващи лични данни, които той използва и които, от своя страна, са длъжни да уведомят администратора в случай на нарушение (вж. по-долу).

Администраторите и обработващите лични данни отговарят за въвеждането на подходящи мерки за предотвратяване, реагиране и справяне с нарушение, но има някои практически стъпки, които следва да се предприемат във всички случаи.

- Информацията относно всички събития, свързани със сигурността, трябва да се насочва към отговорно лице или отговорни лица, чиято задача е справянето с инциденти, установяването на наличие на нарушение и оценката на риска.
- Рискът за физическите лица в резултат на нарушение трябва след това да бъде оценен (вероятност за липса на риск, както и за наличие на риск или на висок риск), за което да бъдат информирани съответните отдели на организацията.
- Трябва, ако е необходимо, да се уведоми надзорният орган и евентуално да се съобщи за нарушението на засегнатите физически лица.
- Същевременно администраторът трябва да предприеме действия за ограничаване на нарушението и възстановяване на първоначалното състояние.
- Нарушението следва да се документира в процеса на неговото развитие.

Трябва следователно да е ясно, че администраторът има задължение да действа по всеки първоначален сигнал за нередност и да установи дали наистина е имало нарушение. Този кратък период дава възможност за разследване и администраторът може да събере доказателства и други важни подробности. След като обаче администраторът е установил с разумна степен на увереност, че е настъпило нарушение, ако са изпълнени условията по член 33, параграф 1, той трябва да уведоми надзорния орган без ненужно забавяне и, когато това е осъществимо — не по-късно от 72 часа[24]. Ако администраторът не изпълни задължението си да действа своевременно и стане очевидно, че е настъпило нарушение, това може да се разглежда като неизпълнение на задължението за уведомяване в съответствие с член 33.

В член 32 е ясно определено, че администраторът и обработващият лични данни трябва да разполагат с подходящи технически и организационни мерки за гарантиране на съобразено с този риск ниво на сигурност на личните данни: способностите за своевременно откриване, справяне със и докладване за нарушение трябва да се разглеждат като важни елементи от тези мерки.

3. Съвместни администратори

Член 26 се отнася до съвместните администратори и в него се уточнява, че съвместните администратори определят съответните си отговорности за спазване на ОРЗД[25]. Това включва

[24] Вж. Регламент (ЕИО, Евратом) № 1182/71 за определяне на правилата, приложими за срокове, дати и крайни срокове, достъпен на: https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:31971R1182&from=BG

[25] Вж. също така съображение 79.

определяне на това коя страна е отговорна за спазване на задълженията по членове 33 и 34. РГ 29 препоръчва в договорните споразумения между съвместните администратори да се включват разпоредби, определящи кой администратор ще ръководи или ще отговаря за спазването на задълженията за уведомяване за нарушение съгласно ОРЗД.

4. Задължения на обработващия лични данни

Администраторът запазва общата отговорност за защитата на личните данни, но обработващият лични данни има важната роля да осигури на администратора възможността да спази своите задължения; към тях спада и уведомяването за нарушение. И наистина, в член 28, параграф 3 се уточнява, че обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт. Член 28, параграф 3, буква е) гласи, че в договора или в другия правен акт се предвижда, че обработващият лични данни „подпомага администратора да гарантира изпълнението на задълженията съгласно членове 32—36, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни“.

От член 33, параграф 2 става ясно, че ако обработващият лични данни е използван от администратор и обработващият данните „разбере“ за нарушение във връзка с личните данни, които обработва от името на администратора, той е длъжен да уведоми администратора „без ненужно забавяне“. Следва да се отбележи, че не е необходимо обработващият лични данни да извърши първо оценка на вероятността за риск, породен от нарушение, преди да уведоми администратора; именно администраторът трябва да извърши тази оценка, след като е „разбрал“ за нарушението. Обработващият лични данни е длъжен само да установи дали е настъпило нарушение и след това да уведоми администратора. Администраторът използва обработващия лични данни за постигане на своите цели; следователно за администратора следва по-принцип да се счита, че е „разбрал“ за нарушението, след като обработващият лични данни го е уведомил за него. Задължението на обработващия лични данни да уведоми администратора дава възможност на администратора да се справи с нарушението и да определи дали е длъжен да уведоми надзорния орган в съответствие с член 33, параграф 1 и засегнатите физически лица в съответствие с член 34, параграф 1. Администраторът може освен това да пожелае да разследва нарушението, тъй като обработващият лични данни може да не е в състояние да знае всички важни факти по въпроса, например дали администраторът на данни има все още резервно копие от личните данни, унищожени или загубени от обработващия ги. От това може да зависи дали тогава администраторът ще трябва да уведомява.

В ОРЗД не се определя изричен срок, в който обработващият лични данни трябва да предупреди администратора, освен че той трябва да направи това „без ненужно забавяне“. Поради това РГ 29 препоръчва обработващият лични данни да уведоми веднага администратора, а допълнителната информация относно нарушението да се предоставя поетапно при постепенното появяване на допълнителни подробности. Това е важно, за да се помогне на администратора да изпълни изискването за уведомяване на надзорния орган в срок от 72 часа.

Както е обяснено по-горе, в договора между администратора и обработващия лични данни трябва да се уточни как изискванията по член 33, параграф 2 трябва да бъдат изпълнени в допълнение на други разпоредби на ОРЗД. Това може да включва изисквания за ранно уведомяване от страна на обработващия лични данни, които, от своя страна, са в подкрепа на задълженията на администратора да докладва на надзорния орган в срок от 72 часа.

Когато обработващият лични данни предоставя услуги на няколко администратори, засегнати от един и същ инцидент, обработващият е длъжен да докладва подробности за инцидента на всеки един от администраторите.

Обработващият лични данни може да извърши уведомяването от името на администратора, ако последният е оправомощил обработващия за това и то е част от договорните споразумения между администратора и обработващия лични данни. Такова уведомяване трябва да се направи в съответствие с членове 33 и 34. Важно е обаче да се отбележи, че законовото задължение за уведомяване е на администратора.

Б. Информиране на надзорния орган

1. Изисквана информация

Когато администраторът уведомява за нарушение надзорния орган, съгласно член 33, параграф 3 в уведомлението следва да се съдържа най-малко следното:

> „а) описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителният брой на засегнатите записи на лични данни;
>
> б) посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
>
> в) описание на евентуалните последици от нарушението на сигурността на личните данни;
>
> г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.“

В ОРЗД няма определение за категории на субектите на данни или на записите на лични данни. Работната група по член 29 предлага обаче категориите на субектите на данни да са съгласно различните видове физически лица, чиито лични данни са били засегнати от нарушението: в зависимост от използваните дескриптори това може да включва, наред с други, деца и други уязвими групи, хора с увреждания, работници и служители или клиенти. Аналогично категориите на записи на лични данни могат да се отнасят за различни видове записи, които администраторът може да обработва, като данни, свързани със здравето и образованието, информация за социалните грижи, финансови данни, номера на банкови сметки, номера на паспорти и пр.

В съображение 85 се пояснява, че една от целите на уведомяването е ограничаването на вредите за физическите лица. Следователно ако видовете субекти на данни или видовете записи на лични данни указват риск от конкретна вреда, настъпваща в резултат на нарушение (напр. кражба на самоличност, измама с фалшива самоличност, финансова загуба, заплаха за професионална тайна), важно е в уведомлението да бъдат посочени тези категории. По този начин то се свързва с изискването за описание на вероятните последици от нарушението.

Когато липсва точна информация (напр. точен брой на засегнатите субекти на данни), това не следва да бъде пречка за своевременно уведомяване относно нарушението. ОРЗД предоставя възможност за приблизителна оценка на броя на засегнатите физически лица и на съответните записи на лични данни. Ударението следва да се постави по-скоро върху справянето с неблагоприятните последици от нарушението, отколкото върху предоставянето на точни числени данни. По този начин, когато стане ясно, че е имало нарушение, но мащабите му не са още известни, поетапното уведомяване (вж. по-долу) е сигурен начин за изпълнение на задълженията за уведомяване.

В член 33, параграф 3 се определя, че администраторът предоставя в уведомлението „най-малко“ тази информация, така че той може, ако е необходимо, да предпочете да предостави допълнителни подробности. Различни видове нарушения (на поверителността, целостта или

наличността) може да изискват предоставянето на допълнителна информация за цялостно обяснение на обстоятелствата във всеки отделен случай.

Пример

Като част от уведомлението си до надзорния орган администраторът може да сметне за полезно да даде името на своя обработващ лични данни, ако при него е основната причина за настъпило нарушение, по-специално ако това е довело до инцидент, засегнал записите на личните данни на много други администратори, които използват същия обработващ на данни.

Във всички случаи надзорният орган може да поиска допълнителни подробности като част от своето разследване на дадено нарушение.

2. Поетапно уведомяване

В зависимост от естеството на нарушението може да се наложи допълнително разследване от страна на администратора, за да се установят всички важни факти във връзка с инцидента. Член 33, параграф 4 гласи:

„Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.“

С това в ОРЗД се потвърждава, че администраторите невинаги имат цялата необходима информация относно дадено нарушение в срок от 72 часа, след като са разбрали за него, тъй като невинаги има пълни и всеобхватни подробности за инцидента през този първоначален период. Това обстоятелство дава възможност за поетапно уведомяване. По-вероятно е случаят да е такъв при по-сложни нарушения, като за някои видове инциденти, свързани с киберсигурността, при които може например да се наложи задълбочено криминално разследване за пълно изясняване на естеството на нарушението и степента, в която са били засегнати личните данни. Ето защо в много случаи администраторът трябва да проведе повече разследвания и да предприеме последващи действия с допълнителна информация на по-късен етап. Това е допустимо, при условие че администраторът посочи причините за забавянето в съответствие с член 33, параграф 1. Работната група по член 29 препоръчва, когато администраторът уведоми за първи път надзорния орган, да информира този орган, дори ако не разполага все още с цялата необходима информация, и да предостави подробности по-късно. Надзорният орган следва да даде съгласие за това как и кога да му бъде предоставена допълнителна информация. Това не е пречка за администратора да предостави допълнителна информация на всеки друг етап, ако узнае допълнителни важни подробности за нарушението, които трябва да бъдат съобщени на надзорния орган.

Основната цел на изискването за уведомяване е да се насърчат администраторите да действат веднага при нарушение, да го ограничат и, ако е възможно, да възстановят засегнатите лични данни и да потърсят компетентен съвет от надзорния орган. Уведомяването на надзорния орган в рамките на първите 72 часа може да даде възможност на администратора да се убеди, че решенията за това дали да бъдат уведомени физическите лица или не са правилни.

Целта на уведомяването на надзорния орган обаче не се свежда единствено до получаване на указания дали да бъдат информирани засегнатите физически лица. В някои случаи е очевидно, че поради естеството на нарушението и сериозността на риска администраторът ще трябва да уведоми незабавно засегнатите лица. Ако има например непосредствена заплаха за кражба на самоличност или ако специални категории лични данни[26] са разкрити онлайн,

[26] Вж. член 9.

администраторът трябва да действа без ненужно забавяне, за да ограничи нарушението и да съобщи за него на засегнатите физически лица (вж. раздел III). При изключителни обстоятелства това може да стане дори преди да бъде уведомен надзорният орган. По-общо казано, уведомяването на надзорния орган не може да служи като оправдание за неизпълнение на задължението за съобщаване на нарушението на субекта на данни, когато то е задължително.

Следва освен това да стане ясно, че след като направи първоначалното уведомяване, администраторът може да уведоми отново надзорния орган, ако при последвало разследване открие доказателство, че инцидентът, свързан със сигурността, е бил ограничен и всъщност не е имало нарушение. Тази информация може тогава да се добави към вече предоставената на надзорния орган и инцидентът да бъде съответно регистриран като несвързан с нарушение. Не се предвижда санкция за докладване на инцидент, за който накрая става ясно, че не е бил нарушение.

Пример

Администратор уведомява надзорния орган в срок от 72 часа след откриване на нарушение, че е загубил устройство за съхранение на данни с USB интерфейс, съдържащо копие на личните данни на някои от неговите клиенти. Устройството за съхранение на данни с USB интерфейс е намерено по-късно на друго място в помещенията на администратора и е възстановено. Администраторът актуализира информацията за надзорния орган и иска да внесе изменение в уведомлението.

Следва да се отбележи, че поетапен подход към уведомяването е вече приложим съгласно съществуващите задължения по Директива 2002/58/ЕО, Регламент (ЕС) № 611/2013 и при други инциденти, докладвани от потърпевшите.

3. Забавени уведомления

В член 33, параграф 1 е посочено ясно, че уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа. Това изискване, заедно с концепцията за поетапно уведомяване, потвърждава, че администраторът невинаги е в състояние да уведоми за нарушение в указания срок и че забавянето на уведомление може да е допустимо.

Такъв сценарий може да има, когато например администраторът установи няколко сходни нарушения на поверителността за кратък период от време, които засягат по един и същ начин голям брой субекти на данни. Администраторът може да разбере за нарушение и, започвайки разследването и преди да е уведомил, да открие допълнителни сходни нарушения, които имат различни причини. В зависимост от обстоятелствата администраторът може да има нужда от известно време, за да установи мащабите на нарушенията и вместо да уведомява за всяко нарушение поотделно, да подготви съдържателно уведомление за няколко много сходни помежду си нарушения с възможни различни причини. Това може да доведе до забавяне на уведомяването на надзорния орган с повече от 72 часа, след като администраторът е разбрал за първи път за тези нарушения.

Стриктно погледнато, всяко отделно нарушение е инцидент, който подлежи на докладване. За да избегне обаче прекомерното обременяване, администраторът може да подаде „обединено“ уведомление за всички тези нарушения, при условие че става въпрос за един и същ вид данни, нарушени по един и същ начин за сравнително кратък период от време. Ако има редица нарушения, засягащи различни видове лични данни, нарушени по различни начини, уведомяването следва да се извърши по обичайния ред, като за всяко нарушение се докладва в съответствие с член 33.

ОРЗД дава до известна степен възможност за забавени уведомления, но това не бива да се разглежда като редовна практика. Струва си да се отбележи, че обединени уведомления могат да се направят и за няколко сходни нарушения, докладвани в рамките на 72 часа.

B. Трансгранични нарушения и нарушения в места на установяване извън ЕС

1. Трансгранични нарушения

При трансгранично обработване[27] на лични данни нарушението може да засегне субекти на данни в повече от една държава членка. В член 33, параграф 1 се посочва ясно, че когато стане нарушение, администраторът следва да уведоми надзорния орган, компетентен в съответствие с член 55 от ОРЗД[28]. В член 55, параграф 1 се предвижда, че:

> „Всеки надзорен орган е компетентен да изпълнява задачите и да упражнява правомощията, възложени му в съответствие с настоящия регламент, на територията на своята собствена държава членка."

Член 56, параграф 1 обаче гласи следното:

> „Без да се засяга член 55, надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да действа като водещ надзорен орган за трансграничното обработване, извършвано от посочения администратор или обработващ лични данни в съответствие с процедурата по член 60."

Освен това, член 56, параграф 6 гласи следното:

> „За трансграничното обработване, което извършва, администраторът или обработващият лични данни комуникира единствено с водещия надзорен орган."

Това означава, че когато стане нарушение при трансгранично обработване и се изисква уведомяване, администраторът ще трябва да уведоми водещия надзорен орган[29]. Следователно когато изготвя своя план за реагиране при нарушение, администраторът трябва да прецени кой надзорен орган е водещият надзорен орган, който трябва да уведоми[30]. Това ще даде възможност на администратора да реагира веднага на нарушение и да изпълни задълженията си съгласно член 33. Трябва да е ясно, че в случай на нарушение при трансгранично обработване трябва да бъде уведомен водещият надзорен орган, който невинаги е там, където се намират засегнатите субекти на данни или всъщност където е извършено нарушението. При уведомяване на водещия орган администраторът следва да посочи, когато е целесъобразно, дали нарушението обхваща места на установяване, намиращи се в други държави членки, и в кои държави членки е вероятно субектите на данни да са били засегнати от нарушението. Ако

---

[27] Вж. член 4, параграф 23.

[28] Вж. също така съображение 122.

[29] Вж. Насоки на РГ 29за определяне на водещ надзорен орган на администратор или обработващ лични данни на следния адрес: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

[30] Списък с координати за връзка с всички европейски национални органи за защита на данните може да се намери на адрес: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

администраторът има някакви съмнения относно това кой точно е водещият надзорен орган, той следва да уведоми най-малко местния надзорен орган, където е извършено нарушението.

2. Нарушения в места на установяване извън ЕС

Член 3 се отнася до териториалния обхват на ОРЗД, включително когато се прилага към обработването на лични данни от администратор или обработващ лични данни, който не е установен в ЕС. По-конкретно член 3, параграф 2 гласи[31]:

„Настоящият регламент се прилага за обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза, когато дейностите по обработване на данни са свързани със:

а) предлагането на стоки или услуги на такива субекти на данни в Съюза, независимо дали от субекта на данни се изисква плащане; или

б) наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Съюза.“

От значение в случая е и член 3, параграф 3, който гласи[32]:

„Настоящият регламент се прилага за обработването на лични данни от администратор, който не е установен в Съюза, но е установен на място, където се прилага правото на държава членка по силата на международното право.“

Когато администратор, който не е установен в ЕС, подлежи на разпоредбите на член 3, параграф 2 или 3 и претърпява нарушение, той следователно е все още обвързан със задълженията за уведомяване съгласно членове 33 и 34. Член 27 задължава администратора (и обработващия лични данни) да определи свой представител в ЕС, когато се прилага член 3, параграф 2. В такива случаи РГ 29 препоръчва уведомление да се отправи до надзорния орган в държавата членка, където е установен представителят на администратора в ЕС[33]. Аналогично, когато обработващият лични данни подлежи на разпоредбите на член 3, параграф 2, той е обвързан от задълженията на обработващите лични данни, и по-специално в този случай от задължението да уведоми за нарушение администратора съгласно член 33, параграф 2.

Г. Условия, при които не се изисква уведомяване

В член 33, параграф 1 се пояснява, че нарушения, за които „не съществува вероятност... да породят риск за правата и свободите на физическите лица“, не изискват уведомяване на надзорния орган. Пример за това е, когато личните данни са вече публично достъпни, така че не съществува вероятност разкриването на такива данни да породи риск за физическото лице. Не е такъв случаят със съществуващите изисквания за уведомяване за нарушение към доставчиците на публично достъпни електронни комуникационни услуги в Директива 2009/136/ЕО, съгласно която за всички важни нарушения трябва да се уведомява компетентният орган.

[31] Вж. също така съображения 23 и 24.

[32] Вж. също така съображение 25.

[33] Вж. съображение 80 и член 27.

В своето Становище 03/2014 относно уведомяване за нарушаване [34] РГ 29 пояснява, че нарушението на поверителността на лични данни, криптирани със съвременен алгоритъм, си остава нарушение на сигурността на лични данни и подлежи на уведомяване. Ако обаче поверителността на ключа не е нарушена, т.е. ключът не е бил засегнат от никакво нарушение на сигурността и е бил генериран по такъв начин, че не може да бъде установен с наличните технически средства от никое лице, което не е оправомощено за достъп до него, то данните са по принцип неразбираеми. Ето защо няма вероятност нарушението да засегне неблагоприятно физическите лица, така че то не изисква уведомяване на тези физически лица[35]. При все това, дори когато данните са криптирани, тяхната загуба или промяна може да има отрицателни последици за субектите на данни, когато администраторът не разполага с адекватни резервни копия. В този случай се налага субектите на данни да бъдат уведомени, дори ако данните са били адекватно криптирани.

РГ 29 пояснява също така, че такъв ще бъде по аналогия и случаят, ако лични данни, като пароли, са били сигурно хеширани и „посолени“, хешираната стойност е била изчислена със съвременна кодирана криптографска функция за хеширане, ключът, използван за хеширане на данните не е бил засегнат от нарушение и е генериран по такъв начин, че не може да бъде установен с наличните технически средства от никое лице, което не е оправомощено за достъп до него.

Следователно ако личните данни са станали по същество неразбираеми за неоправомощени страни или когато данните са копирани, или има резервно копие за тях, може да не се наложи надзорният орган да бъде уведомяван за нарушение на поверителността на надлежно криптирани лични данни. Това е така, защото няма вероятност такова нарушение да изложи на риск правата и свободите на физическите лица. Оттук естествено следва, че не е необходимо да бъде уведомено и физическото лице, тъй като няма вероятност за висок риск. Следва обаче да се има предвид, че макар първоначално да не се налага уведомяване, ако няма вероятност от риск за правата и свободите на физическите лица, това може да се промени след време и да се наложи повторна оценка на риска. Ако например бъде по-късно установено, че ключът е бил засегнат или се открие уязвима страна в софтуера за криптиране, възможно е уведомяване все пак да се наложи.

Следва също така да се отбележи, че ако е налице нарушение, при което няма резервни копия на криптираните лични данни, тогава значи е имало нарушение на наличността, което може да изложи на риск физическите лица, така че уведомяването може да стане задължително. Аналогично, когато е станало нарушение, водещо до загуба на криптирани данни, дори да има резервно копие на личните данни, нарушението може все пак да налага уведомяване в зависимост от това колко време е необходимо за възстановяване на данните от резервното копие и последиците за физическите лица, породени от липсата на наличност. Както е посочено в член 32, параграф 1, буква в), важен фактор за сигурността са „способността за своевременно възстановяване на наличността и достъпът до личните данни в случай на физически или технически инцидент“.

Пример

Нарушение, за което не е задължително да бъде уведомен надзорният орган, е например загубата на сигурно криптирано мобилно устройство, използвано от администратора и неговия персонал. При условие че криптографският ключ остава в сигурно притежание на

[34] Становище 03/2014 на Работната група по член 29 относно уведомяване за нарушаване, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_bg.pdf

[35] Вж. също член 4, параграфи 1 и 2 от Регламент (ЕС) № 611/2013.

администратора и копието на личните данни не е единствено, последните ще бъдат недостъпни за атакуващия. Това означава, че няма вероятност нарушението да породи риск за правата и свободите на въпросните субекти на данни. Ако по-късно стане ясно, че криптографският ключ е засегнат или че софтуерът или алгоритъмът за криптиране е уязвим, тогава рискът за правата и свободите на физическите лица ще се промени, така че уведомяването може да стане вече задължително.

Неизпълнение на задължението за спазване на изискванията на член 33 ще има, когато администраторът не уведоми надзорния орган в ситуация, при която данните всъщност не са били сигурно криптирани. Затова при избора на софтуерен продукт за криптиране администраторите трябва внимателно да преценят качеството и правилното изпълнение на предлаганото криптиране, да разберат какво всъщност ниво на защита предоставя то и дали съответства на съществуващите рискове. Администраторите следва също така да познават добре характерните особености на функционирането на своя криптографски продукт. Дадено устройство може например да бъде криптирано, след като се изключи, но не и докато е в режим на готовност. Някои продукти, които използват криптиране, имат „ключове по подразбиране“, които трябва да бъдат сменени от всеки клиент, за да са ефективни. Освен това криптирането може да се разглежда към настоящия момент като адекватно от експертите по сигурността, но то може да остарее морално за няколко години, което поставя под въпрос адекватното криптиране на данните от този продукт и достатъчната степен на защита.

III. **Член 34 — Съобщаване на субекта на данните за нарушение**

A. Уведомяване на физическите лица

В определени случаи, освен да уведоми надзорния орган, администраторът е длъжен също така да съобщи за нарушение на засегнатите физически лица.

Член 34, параграф 1 гласи:

„Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.“

Администраторите следва да помнят, че уведомяването на надзорния орган е задължително, освен ако липсва вероятност от риск за правата и свободите на физическите лица в резултат на нарушението. Освен това, когато има вероятност от висок риск за правата и свободите на физическите лица в резултат на нарушението, последните също трябва да бъдат уведомени. Прагът за съобщаване относно нарушение на физическите лица е следователно по-висок, отколкото за уведомяване на надзорните органи, така че не за всички нарушения е задължително да се съобщава на физическите лица, което ги предпазва от ненужно натоварване със съобщения.

В ОРЗД се определя, че на физическите лица следва да се съобщи за нарушение „без ненужно забавяне“, т.е. във възможно най-кратък срок. Основната цел на уведомяването на физическите лица е да им се предостави конкретна информация относно стъпки, които те следва да предприемат за своя собствена защита[36]. Както е отбелязано по-горе, в зависимост от естеството на нарушението и създадения риск, своевременното съобщаване ще помогне на

[36] Вж. също така съображение 86.

физическите лица да предприемат стъпки, за да се предпазят от евентуални отрицателни последици от нарушението.

В приложение Б към настоящите Насоки е даден неизчерпателен списък от примери, когато за дадено нарушение е възможно да има вероятност да породи висок риск за физическите лица, и съответно на случаи, в които администраторът е длъжен да съобщи за нарушението на засегнатите.

Б. Изисквана информация

При съобщаване на физическите лица в член 34, параграф 2 се определя, че:

> „В съобщението до субекта на данните, посочено в параграф 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в член 33, параграф 3, букви б), в) и г).“

В съответствие с тази разпоредба администраторът следва да предостави най-малко следната информация:

- описание на естеството на нарушението;
- името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт;
- описание на евентуалните последици от нарушението; и
- описание на предприетите или предложените от администратора мерки за справяне с нарушението, включително, когато е целесъобразно, мерки за намаляване на евентуалните неблагоприятни последици.

Като пример на мерките, предприети за справяне с нарушението и намаляване на евентуалните неблагоприятни последици от него, администраторът може да заяви, че след като е уведомил за нарушението съответния надзорния орган, администраторът е получил съвет за справяне с нарушението и намаляване на неговото въздействие. Администраторът трябва освен това да предоставя по целесъобразност конкретни съвети на физическите лица за това как да се предпазят от евентуални неблагоприятни последици от нарушение, като например смяна на пароли при засягане на атрибутите им за достъп. Администраторът може също така да предостави по свой избор информация в допълнение на изискваната в случая.

В. Установяване на контакт с физическите лица

По принцип съответното нарушение следва да се съобщи директно на засегнатите субекти на данни, освен ако това не е свързано с непропорционално големи усилия. В такъв случай се прави публично съобщение или се предприема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани (член 34, параграф 3, буква в)).

При уведомяване на субектите на данни за нарушение следва да се използват специализирани съобщения, които не трябва да се изпращат съвместно с друга информация, като редовни актуализации, бюлетини или стандартни съобщения. Това помага съобщението за нарушение да бъде ясно и прозрачно.

Сред примерите за начини за прозрачно съобщаване са непосредствено свързване (като електронно писмо, SMS, пряко съобщение), характерни уебсайт флагчета или уведомления, съобщения по пощата и налагащи се на вниманието обяви в печатните медии. Уведомление единствено в рамките на съобщение за медиите или в корпоративен блог не е ефективно средство да се съобщи на дадено физическо лице за нарушение. РГ 29 препоръчва администраторите да избират начин, който увеличава максимално вероятността за адекватно

съобщаване на информацията до всички засегнати физически лица. В зависимост от обстоятелствата това може да означава, че администраторът ще използва няколко начина за съобщаване, вместо един-единствен канал за връзка.

На администраторите може освен това да им се наложи да осигурят достъп на уведомлението в подходящи алтернативни формати и на съответните езици, за да се гарантира, че физическите лица могат да разберат предоставената им информация. Когато например се съобщава за нарушение на засегнатото физическо лице, езикът, използван обикновено при предходните делови контакти с получателя, е в общия случай подходящ. Ако обаче нарушението засяга субекти на данни, с които администраторът не е имал дотогава връзка, или по-специално такива, които пребивават в различни държави членки или в друга държава извън ЕС, различна от онази, в която е разположено установяването на администратора, уведомяване на местния национален език може да се окаже подходящо с оглед на необходимия ресурс. От ключово значение е да се помогне на субектите на данни да разберат естеството на нарушението и стъпките, които могат да предприемат, за да се предпазят.

Администраторите са в най-добра позиция да определят най-подходящия канал за връзка, по който да съобщят за нарушение на физическите лица, особено ако са често във връзка със своите клиенти. Ясно е обаче, че администраторът следва да бъде предпазлив при използване на канал за връзка, засегнат от нарушението, тъй като този канал може да се използва и от атакуващите, които се представят за администратора.

Същевременно в съображение 86 е пояснено, че:

> „Такива уведомления до субектите на данни следва да бъдат правени веднага щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват насоките, предоставени от него или от други съответни органи, като правоприлагащите органи. Така например необходимостта да се ограничи непосредственият риск от вреди би наложила незабавното уведомяване на субектите на данните, докато необходимостта от предприемането на целесъобразни мерки срещу продължаването на нарушения на сигурността на личните данни или срещу подобни нарушения би оправдала по-дълги срокове за уведомлението.“

Администраторите може следователно да поискат да се обърнат към надзорния орган за съвет не само относно уведомяването на субектите на данни за нарушение в съответствие с член 34, но и за това какви подходящи съобщения да се изпратят на физическите лица и кой е оптималният канал за контакт с тях.

В тази връзка е съветът, даден в съображение 88, че при уведомяване за нарушение „следва да се отчитат законните интереси на правоприлагащите органи, когато ранното разкриване може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността на личните данни“. Това може да означава, че при определени обстоятелства, когато това е обосновано и по съвет на правоприлагащите органи, администраторът може да забави уведомяването на засегнатите физически лица за нарушението дотолкова, че то да не попречи на такива разследвания. След изтичането на този период от време обаче субектите на данни трябва все пак да бъдат уведомени незабавно.

Когато администраторът няма възможност да съобщи на съответното физическо лице за нарушение, тъй като не са съхранени достатъчно данни за връзка с него, при тези специфични обстоятелства администраторът трябва да уведоми физическото лице веднага щом това е разумно осъществимо (напр. когато физическото лице упражни правото си по член 15 за достъп до личните данни и предостави на администратора допълнителната информация, необходима за връзка с него).

Г. Условия, при които не се изисква съобщаване

В член 34, параграф 3 са посочени три условия, при които, ако са изпълнени, не се изисква съобщение до физическите лица в случай на нарушение. Тези условия са:

- Администраторът е предприел подходящи технически и организационни мерки за защита на личните данни преди нарушението, по-специално мерките, правещи личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях. Това може да включва например защита на личните данни със съвременни методи на криптиране или с въвеждане на токени.
- Непосредствено след нарушението администраторът е взел мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на физическите лица. В зависимост от обстоятелствата при случая администраторът може например незабавно да е идентифицирал и да е предприел мерки срещу физическото лице, което е получило достъп до лични данни, преди да е имало възможност да направи нещо с тях. Дължимото внимание следва да се обърне на евентуалните последици от всяко нарушение на поверителността, отново в зависимост от естеството на съответните данни.
- Съобщаването би довело до непропорционални усилия[37] за установяване на връзка с физическите лица, евентуално ако данните им за връзка са били изгубени в резултат на нарушение или са били поначало неизвестни. Например складът на статистическа служба е наводнен, а документите, съдържащи лични данни, са били съхранявани само на хартиен носител. В такъв случай администраторът трябва да направи публично съобщение или да предприеме друга подобна мярка, така че физическите лица да бъдат в еднаква степен ефективно информирани. В случая с непропорционални усилия също могат да се предвидят технически мерки, за да се даде достъп при поискване до информацията за нарушението, което може да се окаже полезно за онези физически лица, които може да са били засегнати от нарушението, но с които администраторът не може да установи връзка по друг начин.

В съответствие с принципа на отчетността администраторите следва да са в състояние да докажат на надзорния орган, че изпълняват едно или повече от тези условия [38]. Следва да се има предвид, че макар първоначално да не се налага уведомяване, ако няма вероятност от риск за правата и свободите на физическите лица, това може да се промени след време и да се наложи повторна оценка на риска.

Ако администраторът реши да не съобщава за нарушение на физическото лице, в член 34, параграф 4 се пояснява, че надзорният орган може да изиска от него да направи това, ако сметне, че има вероятност нарушението да породи висок риск за физическите лица. От друга страна, той може да приеме, че условията в член 34, параграф 3 са изпълнени и в такъв случай не се изисква уведомяване на физическите лица. Ако надзорният орган заключи, че решението да не се съобщава на субектите на данни е недостатъчно обосновано, той може да разгледа възможността за използване на предоставените му правомощия и санкции.

[37] Вж Насоки на РГ 29 относно прозрачността, където ще бъде разгледан въпросът с непропорционалните усилия, на следния адрес: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Вж. член 5, параграф 2.

IV. **Оценка за риск и висок риск**

А. Рискът като предпоставка за задействане на уведомяването

Въпреки че с ОРЗД се въвежда задължението за уведомяване за нарушение, това не е изискване, валидно при всички обстоятелства.

- Уведомяването на компетентния надзорен орган е задължително, освен ако липсва вероятност нарушението да породи риск за правата и свободите на физическите лица.
- За нарушение се съобщава на физическите лица само когато има вероятност то да породи висок риск за техните права и свободи.

Това означава, че непосредствено след като разбере за нарушение, от жизненоважно значение е задължението на администратора не само да се постарае да ограничи инцидента, но и да оцени риска, до който може да доведе той. Има две важни причини за това: първо, ако администраторът знае каква е вероятността и потенциалната тежест на въздействието за физическото лице, това ще му помогне да предприеме ефективни мерки за ограничаване на нарушението и справяне с него; второ, ще му помогне да установи дали е задължително да уведоми надзорния орган, и, ако е необходимо, засегнатите физически лица.

Както бе обяснено по-горе, уведомяването за нарушение е задължително, освен ако липсва вероятност то да породи риск за правата и свободите на физическите лица, като основният фактор за задействане на уведомяване на субектите на данни за нарушение е дали има вероятност то да породи *висок* риск за правата и свободите на физическите лица. Такъв риск съществува, когато нарушението може да доведе до физически, материални или нематериални вреди за физическите лица, чиито данни са били засегнати. Примери за такива вреди са дискриминация, кражба на самоличност или измама с фалшива самоличност, финансова загуба и накърняване на репутацията. Когато нарушението засяга лични данни, разкриващи расов или етнически произход, политически убеждения, религиозни или философски схващания или членство в професионална организация, или включва генетични данни, данни за здравословното състояние или сексуалния живот, или за присъди и правонарушения или свързани с тях мерки за сигурност, следва да се приеме, че има вероятност да настъпят такива вреди[39].

Б. Фактори, които трябва да бъдат взети предвид при оценка на риска

Съгласно съображения 75 и 76 от ОРЗД, когато се оценява рискът, под внимание следва да се вземат по принцип както вероятността, така и тежестта на риска за правата и свободите на субектите на данни. Казано е по-нататък, че рискът следва да се оценява въз основа на обективна преценка.

Следва да се отбележи, че при оценка на риска за правата и свободите на хората в резултат на нарушение уронването е различно от това при риска, разглеждан при оценка на въздействието върху защитата на данните[40]. Във втория случай се разглеждат както рисковете от обработване на данни, извършено съгласно очакванията, така и рисковете в случай на нарушение. Когато се разглежда евентуално нарушение, в общи линии се преценява вероятността то да се случи и вредите за субектите на данни, до които може да доведе; с други думи, става въпрос за оценка на хипотетично събитие. При действително нарушение събитието вече е настъпило, така че

[39] Вж. съображения 75 и 85.

[40] Вж. Насоки на Работната група относно оценката на въздействието върху защитата на данните тук: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

ударението се поставя изцяло върху риска, породен от въздействието на нарушението за физическите лица.

Пример

В оценка на въздействието върху защитата на данните се твърди, че предложението за използване на определен софтуерен продукт за сигурност с цел защита на личните данни е подходяща мярка за постигане на ниво на сигурност, подходящо за риска, на който обработването би изложило в противен случай физическите лица. Ако обаче впоследствие се установи уязвимост, това би направило софтуера неподходящ за ограничаване на риска за защитените лични данни, така че ще се наложи той да бъде оценен повторно като част от продължаваща оценка на въздействието върху защитата на данните.

По-късно е използвана уязвимост на продукта и е извършено нарушение. Администраторът следва да направи оценка на специфичните обстоятелства на нарушението, засегнатите данни и евентуалната тежест на въздействието за физическите лица, както и вероятността за материализиране на този риск.

Следователно, когато преценява риска за физическите лица в резултат на нарушение, администраторът следва да направи оценка на специфичните обстоятелства на нарушението, включително на тежестта на евентуалното въздействие и вероятността то да настъпи. С оглед на това РГ 29 препоръчва при оценката да се вземат предвид най-малко следните критерии[41]:

- Вид на нарушението

Видът на извършеното нарушение може да окаже въздействие върху нивото на риска за физическите лица. Така например нарушение на поверителността, при което медицинска информация е разкрита пред неоправомощени страни, може да доведе до различен набор от последици за съответното физическо лице, в сравнение с нарушение, при което медицински данни за него са били изгубени и не са вече налични.

- Естество, чувствителност и обем на личните данни

Когато се извършва оценка на риска, ключов фактор естествено е видът и чувствителността на личните данни, които са засегнати от нарушението. Обикновено колкото по-чувствителни са данните, толкова по-висок е рискът от вреди за засегнатите хора, трябва обаче да се вземат предвид и други лични данни, които може да са вече достъпни за субекта на данни. Така например разкриването на името и адреса на дадено лице при обикновени обстоятелства едва ли ще причини съществени вреди. Ако обаче името и адресът на осиновител бъде разкрито на истинския родител, последиците могат да бъдат много сериозни както за осиновителя, така и за детето.

Нарушения, свързани с данни за здравния статус, документи за самоличност или финансови данни, като подробности за банкови карти, могат да причинят вреди и сами по себе си, но ако се използват съвместно, могат да послужат за кражба на самоличност. Комбинация от лични данни е по принцип по-чувствителна от отделно взети лични данни.

[41] В член 3, параграф 2 от Регламент (ЕС) № 611/2013 са дадени указания относно факторите, които следва да се вземат под внимание във връзка с уведомяването за нарушения в сектора на електронните съобщителни услуги, които може да бъдат от полза при уведомяване съгласно ОРЗД. Вж. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:bg:PDF

Някои видове лични данни може да изглеждат на пръв поглед безопасни, но трябва внимателно да се проучи какво биха могли да разкрият те за засегнатото физическо лице. Списък на клиенти, получаващи редовни доставки, може да не е особено чувствителен, но същите данни за клиенти, които са поискали доставките им да бъдат спрени, докато са на почивка, ще бъде полезна информация за извършители на престъпления.

По подобен начин малък обем високо чувствителни лични данни могат да доведат до голямо въздействие за дадено физическо лице, а голям набор от подробности може да разкрие по-голям обем от информация за това лице. Също така нарушение, засягащо големи обеми лични данни за много субекти на данни, може да доведе до последици за съответно голям брой физически лица.

- Леснота на идентифициране на физическите лица

Важен фактор, който трябва да се има предвид, е колко лесно ще бъде за страна, която има достъп до засегнати лични данни, да идентифицира определени физически лица или да съчетае данните с друга информация за идентифициране на физическите лица. В зависимост от обстоятелствата идентифицирането може да стане непосредствено от личните данни, чиято сигурност е нарушена, без да е необходимо специално проучване за откриване на самоличността на физическото лице, или може да е изключително трудно личните данни да се свържат с определено лице, но това би могло все пак да се окаже възможно при определени условия. Идентифицирането може да стане пряко или косвено от засегнатите данни, но може да зависи и от специфичния контекст на нарушението и от публичната наличност на свързани с тях лични данни. Това може да се окаже от по-голямо значение при нарушения на поверителността и наличността.

Както бе посочено по-горе, личните данни, защитени с подходящо ниво на криптиране, са неразбираеми за неоправомощени лица без ключа за декриптиране. Освен това подходящо извършената псевдонимизация (определена в член 4, параграф 5 като „обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано“) може също така да намали вероятността за идентифициране на физическите лица в случай на нарушение. Техниките на псевдонимизация не могат да се разглеждат сами по себе си като гаранция за неразбираемостта на данните.

- Сериозност на последиците за физическите лица

В зависимост от естеството на личните данни, засегнати при нарушение, например за специални категории данни, евентуално нанесените вреди за физическите лица могат да бъдат особено сериозни, по-конкретно когато нарушението може да доведе до кражба на самоличност, телесна повреда, психологически стрес, унижение или накърняване на репутацията. Ако нарушението засяга лични данни за физически лица в уязвимо положение, възможно е те да бъдат изложени на по-голям риск от вреди.

Обстоятелството дали администраторът е наясно, че личните данни са в ръцете на хора, чиито намерения са неизвестни или може би зловредни, може да повлияе на степента на възможния риск. Възможно е да има нарушение на поверителността, при което личните данни се разкриват пред трета страна, определена в член 4, параграф 10, или погрешка пред друг получател. Това може да стане например когато личните данни бъдат изпратени погрешка на друго поделение на дадена организация или на широко използвана организация за доставки. Администраторът може да поиска от получателя да върне или да унищожи по сигурен начин получените от него данни. И в двата случая, с оглед на това, че администраторът има стабилни отношения с получателя и може да познава неговите процедури, историята му и други

относими подробности, той може да се разглежда като „заслужаващ доверие“. С други думи, администраторът може да изпитва достатъчно доверие към получателя, така че да има разумни очаквания той да не прочете и да не установи достъп до изпратените погрешка данни, а да изпълни указанията му да ги върне. Дори ако е бил установен достъп до данните, администраторът може все пак да се довери на получателя, че няма да предприеме други действия с тях, а ще ги върне веднага на администратора и ще съдейства за тяхното възстановяване. В тези случаи това може да бъде взето под внимание при оценката риска, която администраторът извършва след нарушението — фактът, че получателят заслужава доверие, може да елиминира сериозността на последиците от нарушението, но не означава, че не е имало нарушение. Това, на свой ред, може обаче да отстрани вероятността от риск за физическите лица, така че да стане излишно да се уведомява както надзорният орган, така и засегнатите физически лица. Това също ще зависи конкретно от всеки отделен случай. Въпреки това администраторът остава длъжен да съхранява информация относно нарушението като част от общото си задължение да поддържа регистър за нарушенията (вж. раздел V по-долу).

Внимание следва да се обърне и на дълготрайността на последиците за физическите лица, при което въздействието може да се разглежда като по-голямо, ако последиците са дългосрочни.

- Специални характеристики на физическото лице

Нарушението може да засегне лични данни относно деца или други лица в уязвимо положение, които в резултат могат да бъдат изложени на по-голям риск. Възможно е да има други фактори относно физическото лице, които да повлияят на степента на въздействие на нарушението върху него.

- Специални характеристики на администратора на лични данни

Естеството и ролята на администратора и неговите дейности може да повлияят на степента на риска за физическите лица, породен от нарушение. Медицинските организации например обработват специални категории лични данни, така че има по-голяма заплаха за физическите лица при нарушение на сигурността на личните им данни, отколкото на списъка с адреси на някой вестник.

- Брой на засегнатите физически лица

Нарушението може да засяга не само едно или няколко физически лица, но и няколко хиляди, ако не и много повече. По принцип, колкото по-голям е броят на засегнатите физически лица, толкова по-голямо въздействие може да окаже нарушението. Нарушението може обаче да въздейства сериозно дори само на едно физическо лице в зависимост от естеството на личните данни и контекста, в който е била засегната сигурността им. И в този случай от ключово значение е да се разгледат вероятността и сериозността на въздействието за засегнатите лица.

- Общи положения

Следователно когато преценява риска, който вероятно ще бъде породен от нарушението, администраторът следва да направи оценка на комбинация от сериозността на евентуалното въздействие за правата и свободите на физическите лица и вероятността то да настъпи. Ясно е, че когато последиците от нарушението са по-сериозни, рискът е по-висок, както и че когато вероятността те да настъпят е по-голяма, рискът също се повишава. Ако изпитва съмнения, администраторът следва да бъде особено предпазлив и да изпрати уведомление. В приложение Б са дадени няколко полезни примера за различни видове нарушения, представляващи риск или висок риск за физическите лица.

Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) направи препоръки за методология за оценка на сериозността на нарушението, които може да бъдат

полезни за администраторите и обработващите лични данни, когато изготвят своя план за реагиране при нарушение[42].

V. Отчетност и поддържане на регистър

A. Документиране на нарушенията

Независимо от това дали за дадено нарушение трябва да се уведоми надзорният орган, администраторът е длъжен да поддържа документация за всички нарушения, както се пояснява в член 33, параграф 5:

> „Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали е спазен настоящият член.“

Това е свързано с принципа на отчетността на ОРЗД, изложен в член 5, параграф 2. Целта за регистриране на нарушенията, независимо дали подлежат или не на уведомяване, е свързана и със задълженията на администратора съгласно член 24, като надзорният орган може да поиска да види този регистър. Ето защо администраторите се приканват да създадат вътрешен регистър на нарушения, независимо дали са длъжни да уведомяват за тях, или не[43].

Администраторът може да реши какъв метод и каква структура да използва при документирането на нарушения, но по отношение на подлежащата на документиране информация има ключови елементи, които следва да бъдат включени във всички случаи. Съгласно изискванията на член 33, параграф 5 администраторът трябва да регистрира всички подробности, свързани с нарушението, които следва да включват причините за него, какво точно е станало и личните данни, които са били засегнати. Следва да бъдат включени също така последиците от нарушението, както и коригиращите действия, предприети от администратора.

В ОРЗД не е посочен срок за съхранение на тази документация. Когато в този регистър се съдържат лични данни, задължение на администратора е да определи подходящия срок на съхранение в съответствие с принципите относно обработването на лични данни[44] и да спазва правното основание за обработването[45]. Той трябва да поддържа документацията в съответствие с член 33, параграф 5, ако му бъде поискано да предостави на надзорния орган доказателство за спазване на изискванията на този член или, по-общо казано, на принципа на

---

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (Препоръки за методология за оценка на сериозността на нарушения на сигурността на лични данни), https://www.enisa.europa.eu/publications/dbn-severity

[43] Администраторът може да реши да документира нарушенията като част от своя регистър на дейностите по обработване, който се поддържа в съответствие с член 30. Не е задължително да има отделен регистър, при условие че информацията, отнасяща се до нарушението, е ясно разпознаваема като такава и може да бъде извлечена при поискване.

[44] Вж. член 5.

[45] Вж. съображение 6 и член 9.

отчетността. Ясно е, че ако в самия регистър не се съдържат лични данни, то принципът на ОРЗД за ограничение на съхранението не се прилага[46].

В допълнение на тези подробности работната група по член 29 препоръчва администраторът да документира и своите основания за решенията, взети за реагиране на нарушението. По-специално, ако за дадено нарушение не се уведомява, следва да се документира основание за това решение. То следва да включва причините, поради които администраторът смята, че няма вероятност нарушението да породи риск за правата и свободите на физическите лица[47]. От друга страна, ако администраторът смята, че е изпълнено някое от условията в член 34, параграф 3, той трябва да е в състояние да предостави достатъчно доказателство, че това наистина е така.

Когато администраторът уведомява надзорния орган за нарушение, но уведомяването е забавено, администраторът трябва да може да посочи причини за това забавяне; документация в тази връзка може да помогне да се докаже, че забавянето при уведомяването е обосновано и не е прекомерно.

Когато администраторът съобщава за нарушение на засегнатите физически лица, той следва да направи това прозрачно, ефективно и своевременно. По този начин това ще помогне на администратора да покаже отчетност и спазване на изискванията, като запази доказателства за такъв начин на съобщаване.

За да си помогнат за спазване на изискванията на членове 33 и 34, добре е както администраторите, така и обработващите лични данни, да са въвели процедура за документиране на уведомленията, определяща стъпките, които да се предприемат след откриването на нарушение, включително начините за ограничаване, управление и справяне с инцидента, както и оценяване на риска и уведомяване на нарушението. В тази връзка, с оглед да се покаже спазване на изискванията на ОРЗД, може да е от полза също така да се докаже, че служителите са били уведомени за съществуването на такива процедури и механизми и че знаят как да реагират при нарушения.

Следва да се отбележи, че неизпълнение на задължението за надлежно документиране на нарушенията може да подтикне надзорния орган да упражни правомощията си по член 58 и/или да наложи административна глоба в съответствие с член 83.

Б. Роля на длъжностното лице по защита на данните

Администраторът или обработващият лични данни може да има длъжностно лице по защита на данните (ДЛЗД)[48] съгласно изискванията на член 37 или на доброволна основа като проява на добра практика. В член 39 от ОРЗД се определят редица задължителни задачи на ДЛЗД, но това не е пречка да му бъдат възложени допълнителни задачи от администратора, ако е целесъобразно.

По-специално във връзка с уведомяването за нарушение сред задължителните задачи на ДЛЗД са, наред с други задължения, предоставяне на съвети и информация относно защитата на данни на администратора или обработващия лични данни, наблюдение на спазването на ОРЗД и предоставяне на съвети във връзка с оценката на въздействието върху защитата на данните.

[46] Вж. член 5, параграф 1, буква д).

[47] Вж. съображение 85.

[48] Вж. насоките на работната група относно ДЛЗД тук: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

ДЛЗД трябва също така да си сътрудничи с надзорния орган и да действа като точка за контакт за надзорния орган и за субектите на данни. Следва също да се отбележи, че при уведомяване на надзорния орган за нарушение член 33, параграф 3, буква б) задължава администратора да посочи името и координатите за връзка на своето ДЛЗД или на друга точка за контакт.

При документиране на нарушенията администраторът или обработващият лични данни може да поиска становището на ДЛЗД относно структурата, организирането и администрирането на тази документация. На ДЛЗД може освен това да му бъде възложена допълнително задачата за поддържането на такъв регистър.

Тези фактори означават, че ДЛЗД следва да изпълнява ключова роля при предотвратяването на или подготовката за реагиране при нарушение, като предоставя съвети и наблюдава спазването на изискванията както по време на нарушение (т.е. при уведомяване на надзорния орган), така и при евентуално последващо разследване от надзорния орган. С оглед на това РГ 29 препоръчва ДЛЗД да бъде незабавно уведомено за съществуването на нарушение, като участва в целия процес на управление на нарушението и уведомяване за него.

VI. Задължения за уведомяване съгласно други правни инструменти

В допълнение на и независимо от уведомяването и съобщаването за нарушения съгласно ОРЗД, администраторите следва да познават също така всяко изискване за уведомяване относно инциденти, свързани със сигурността, съгласно други свързани законодателни актове, които може да са приложими за тях, както и дали те могат да ги задължат да уведомяват надзорния орган същевременно за нарушение на сигурността на лични данни. Такива изисквания може да са различни в отделните държави членки, но сред примерите за изисквания за уведомяване в други правни инструменти и как те си взаимодействат с ОРЗД, са следните:

- Регламент (ЕС) № 910/2014 относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар (Регламент относно електронната идентификация и удостоверителните услуги)[49].

С член 19, параграф 2 от Регламента относно електронната идентификация и удостоверителните услуги доставчиците на удостоверителни услуги се задължават да уведомяват своя надзорен орган за нарушение на сигурността или загуба на целостта, които оказват значително въздействие върху представяните удостоверителни услуги или върху съдържащите се в тях лични данни. Когато е приложимо — т.е. когато такова нарушение или такава загуба е и нарушение на сигурността на лични данни съгласно ОРЗД, доставчикът на доверителни услуги следва също да уведоми надзорния орган.

- Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (Директива за МИС)[50].

Членове 14 и 16 от Директивата за МИС изискват от операторите на основни услуги и доставчиците на цифрови услуги да уведомяват надзорния си орган за инциденти, свързани със сигурността. Както се потвърждава в съображение 63 от МИС[51], при инциденти, свързани със

[49] Вж. https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32014R0910&from=EN

[50] Вж. https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[51] Съображение 63: *„В много случаи вследствие на инциденти се засягат лични данни. В този контекст компетентните органи и органите за защита на данните следва да си сътрудничат и да обменят*

сигурността, често се засягат лични данни. МИС задължава компетентните органи и надзорните органи да си сътрудничат и да обменят информация в този контекст, но положението остава такова, че когато такива инциденти са или станат нарушения на сигурността на лични данни съгласно ОРЗД, тези оператори и/или доставчици ще бъдат длъжни да уведомят надзорния орган, независимо от изискванията на МИС за уведомяване относно инциденти.

Пример

На доставчик на услуги „в облак“, който уведомява за нарушение съгласно Директивата за МИС, може да му се наложи да уведоми и администратор, ако е налице нарушения на сигурността на лични данни. Също така и на доставчик на доверителни услуги, който уведомява съгласно Регламента относно електронната идентификация и удостоверителните услуги, може да бъде задължен да уведоми съответния орган за защита на данните в случай на нарушение.

- Директива 2009/136/ЕО (Директива за правата на гражданите) и Регламент (ЕС) № 611/2013 (Регламент за уведомяване относно нарушение).

Доставчиците на публично достъпни електронни комуникационни услуги в контекста на Директива 2002/58/ЕО[52] трябва да уведомяват за нарушения компетентните национални органи.

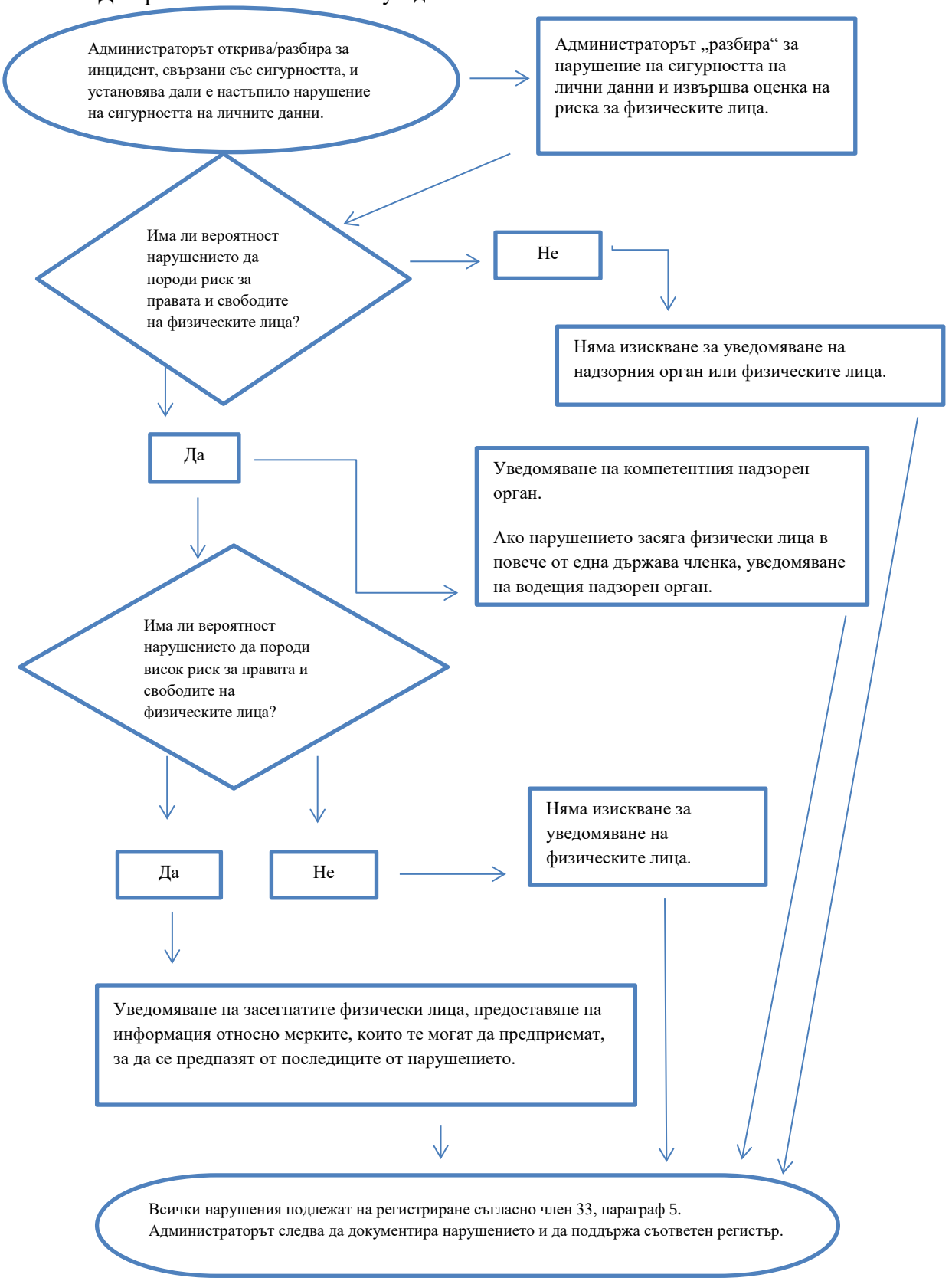
Администраторите на лични данни следва също така да познават всички допълнителни правни, медицински или професионални задължения за уведомяване по силата на други приложими режими.

информация относно всички съответни въпроси с цел справяне с нарушенията на сигурността на лични данни, предизвикани от инциденти.“

[52] На 10 януари 2017 г. Европейската комисия предложи Регламент за правото на неприкосновеността на личния живот и електронните съобщения, който ще замени Директива 2009/136/ЕО и ще премахне изискванията за уведомяване. Докато това предложение не бъде одобрено от Европейския парламент, съществуващото изискване за уведомяване остава обаче в сила, вж. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Приложение**

A. Диаграма на изискванията за уведомяване



Б. Примери за нарушения на сигурността на лични данни и за това кой трябва да бъде уведомяван

Следващите неизчерпателни примери ще помогнат на администраторите да определят дали трябва да уведомяват при различни сценарии за нарушение на сигурността на лични данни. Тези примери може също така да помогнат да се направи разлика между риск и висок риск за правата и свободите на физическите лица.

Пример	**Уведомяване на надзорния орган?**	**Уведомяване на субекта на данни?**	**Бележки/препоръки**
i. Администраторът е запазил резервно копие на архив от лични данни, криптирани на устройство за съхранение на данни с USB интерфейс. Флаш паметта е откраднатa при влизане с взлом.	Не.	Не.	Стига данните да са криптирани със съвременен алгоритъм, да има техни резервни копия, уникалният код да не е разкрит и данните да могат да бъдат възстановени в разумен срок, нарушението може да не подлежи на задължително уведомяване. Ако обаче кодът бъде по-късно разкрит, уведомяването е задължително.
ii. Администраторът поддържа онлайн услуга. В резултат на кибератака на тази услуга са изтеглени лични данни на физически лица. Администраторът има клиенти само в една държава членка.	Да, докладва се на надзорния орган, ако има вероятност да настъпят последици за физическите лица.	Да, докладва се на физическите лица в зависимост от естеството на засегнатите лични данни и ако сериозността на вероятните последици за тях е голяма.	
iii. Кратко прекъсване на електрозахранването за няколко минути в център за обаждания на администратора, което означава, че клиентите не могат да се обаждат на администратора и да получават достъп до записаните си данни.	Не.	Не.	Това нарушение не подлежи на уведомяване, но е все пак инцидент, който задължително се регистрира съгласно член 33, параграф 5. Администраторът следва да поддържа съответен регистър.
iv. Администратор е	Да, докладва се на	Да, докладва се на	Ако е имало резервно

обект на атака със софтуер за изнудване, която води до криптиране на всички данни. Липсват резервни копия и данните не могат да бъдат възстановени. При разследването става ясно, че единствената функционалност на софтуера за изнудване е била криптиране на данните и че в системата няма друг зловреден софтуер.	надзорния орган, ако има вероятност да настъпят последици за физическите лица, тъй като става въпрос за загуба на наличността.	физическите лица в зависимост от естеството на засегнатите лични данни и възможните последици от липсата на наличност на данните, както и от други последици, за които има вероятност да настъпят.	копие и данните могат да бъдат възстановени в разумен срок, за инцидента не е необходимо да се докладва на надзорния орган, нито на физическите лица, тъй като не е имало трайна загуба на наличността или поверителността. Ако обаче надзорният орган е разбрал за инцидента по други начини, той може да обсъди възможността за провеждане на разследване с цел оценка на съответствието с по-широките изисквания за сигурност на член 32.
v. Физическо лице се свързва с центъра за обаждания на банка, за да докладва за нарушаване на сигурността на данни. Лицето е получило месечен отчет за друг човек. Администраторът провежда кратко разследване (което приключва в рамките на 24 часа) и установява с достатъчна степен на увереност, че е настъпило нарушение на сигурността на лични данни и дали има системен недостатък, което може да означава, че други физически лица са засегнати или могат да бъдат засегнати.	Да.	Уведомяват се само засегнатите физически лица, ако има висок риск и е ясно, че няма други засегнати.	Ако след допълнително разследване се установи, че са засегнати повече физически лица, следва да се изпрати актуализирана информация на надзорния орган и администраторът предприема допълнителната мярка за уведомяване на други физически лица, ако са изложени на висок риск.

vi. Администратор обслужва онлайн пазар и има клиенти в повече държави членки. Пазарът става обект на кибератака и потребителски имена, пароли и история на покупките са публикувани онлайн от атакуващия.	Да, докладва се на водещия надзорен орган, ако има трансгранично обработване на лични данни.	Да, тъй като може да доведе до висок риск.	Администраторът трябва да предприеме действия, например за принудителна промяна на засегнатите потребителски профили, както и други мерки за намаляване на риска. Администраторът следва освен това да разгледа всякакви други задължения за уведомяване, например по Директивата за МИС като доставчик на цифрови услуги.
vii. Фирма за уеб хостинг, действаща като лице, което обработва данните, установява грешка в кода за контрол на разрешения достъп на потребителите. Грешката води до това, че който и да е потребител може да има достъп до данните от потребителския профил на всеки друг потребител.	В качеството си на обработващ лични данни, фирмата за уеб хостинг трябва да уведоми своите засегнати клиенти (администраторите) без ненужно забавяне. Приемайки, че дружеството за уеб хостинг е провело свое собствено разследване, засегнатите администратори следва да имат разумна степен на увереност относно това дали всеки от тях е засегнат от нарушение и поради това може да се приеме, че „са разбрали“, след като са били уведомени от дружеството за хостинг (обработващия лични данни). Администраторът е длъжен тогава да уведоми надзорния	Ако няма вероятност за висок риск за физическите лица, не е необходимо те да бъдат уведомявани.	Фирмата за уеб хостинг (обработващият лични данни) трябва да разгледа всякакви други задължения за уведомяване (например по Директивата за МИС като доставчик на цифрови услуги). Ако няма доказателство, че тази уязвимост е била използвана при някои от администраторите на фирмата, може да не е настъпило подлежащо на уведомяване нарушение, но има вероятност то да подлежи на регистриране или да става въпрос за неизпълнение на изискванията по член 32.

	орган.		
viii. Медицинските досиета в дадена болница са недостъпни в продължение на 30 часа в резултат на кибератака.	Да, болницата е длъжна да уведоми за инцидента, тъй като той може да породи висок риск за благополучието и неприкосновеността на личния живот на пациентите.	Да, уведомяват се засегнатите физически лица.	
ix. Лични данни на голям брой ученици са изпратени погрешка до неправилно подбран списък с адреси на повече от хиляда получатели.	Да, докладва се на надзорния орган.	Да, докладва се на физическите лица в зависимост от обхвата и вида на засегнатите лични данни и тежестта на възможните последици.	
x. Маркетингово електронно съобщение е изпратено на получатели в полетата „до:“ или „копие до:“, с което е дадена възможност на всеки от получателите да види електронния адрес на други получатели.	Да, уведомяването на надзорния орган може да е задължително, ако голям брой физически лица са засегнати, ако са разкрити чувствителни данни (напр. списък с адреси на психотерапевт) или ако други фактори представляват високи рискове (напр. електронното писмо съдържа паролите за влизане).	Да, докладва се на физическите лица в зависимост от обхвата и вида на засегнатите лични данни и тежестта на възможните последици.	Уведомяване може да не е необходимо, ако не са разкрити чувствителни данни и ако са разкрити само незначителен брой електронни адреси.