РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – ПЕТРИЧ

УТВЪРЖДАВАМ:
АТАНАС КОБУРОВ
ПРЕДСЕДАТЕЛ НА РС – ПЕТРИЧ
Заповед №14/22.02.2024 г.

ДЕЙСТВИЯ ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В РАЙОНЕН СЪД – ПЕТРИЧ

Процедурата е разработена с цел да подпомогне дейността на Районен съд – Петрич при реагиране на нарушения на сигурността на личните данни.

I. ИЗПОЛЗВАНА ТЕРМИНОЛОГИЯ

- „Нарушение на сигурността на личните данни" означава 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 (чл. 4, т. 12 от Регламент (ЕС) 2016/679).
- „Унищожаване" е налице, когато личните данни ги няма или ги няма във вид, в който администраторът може да ги използва.
- „Повреждане" е налице, когато личните данни са променени, подправени или станали вече непълни.
- „Загубата" е състояние, при което данните може все още да са налични, но администраторът е загубил контрол или достъп до тях или те не са вече притежавани от него.
- „Неразрешено разкриване" е разкриване на лични данни пред или предоставяне на достъп до тях на получатели, които не са оправомощени да ги получат или да имат достъп до тях.

II. ПРИЗНАЦИ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

- При установяване на признаци за нарушение на сигурността на личните данни всеки служител на Районен съд – Петрич е длъжен незабавно да информира административния ръководител или длъжностното лице по защита на личните данни.
- Признаците на нарушенията на сигурносгга могат да включват: индикатори от системите за физическа защита, загуба на документи, съдържащи лични данни или на носители на лични данни, недостъпност на информационни системи, в които се обработват лични данни и други подобни, при които е вероятно да има унищожаване, повреждане, загуба или нерегламентиран достъп до лични данни.

III. УСТАНОВЯВАНЕ НА ЕСТЕСТВОТО НА НАРУШЕНИЕТО

1. Председателят на Районен съд – Петрич със съдействието на длъжностното лице по защита на личните данни преценява дали има нарушение на сигурността на личните данни и ако да – в какво се изразява неговото естество.

2. Нарушенията на сигурността на личните данни се категоризират в следните видове:

– 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 до или унищожаване на лични данни. Загуба на наличността за определен период от време също е вид нарушение, ако може да окаже значително въздействие върху правата и свободите на физическите лица.

3. Естеството на нарушението се отчита при прилагане на мерките за справяне с последиците от нарушението на сигурността на личните данни.

IV. АНАЛИЗ НА РИСКА ОТ НАРУШЕНИЕТО ЗА ПРАВАТА И СВОБОДИТЕ НА ФИЗИЧЕСКИТЕ ЛИЦА

- Рискът се определя като възможност за настъпване на имуществена или неимуществена вреда за субекта на данните при определени условия, оценена от гледна точка на нейната тежест и вероятност.
- При определяне на вероятността и тежестта на риска се отчитат следните обстоятелства:

✓ естество на данните, обект на нарушението на сигурността – рискът може да бъде различен в зависимост от това дали данните, обект на нарушението, са „обикновени" или специални категории или данни, свързани с присъди и нарушения. Очаквано е рискът да е по-висок при специалните категории лични данни и при личните данни, свързани с присъди и нарушения.

✓ обхват на нарушението – каква част от обработваните лични данни засяга; засегнатите лични данни представляват ли значителен обем на регионално, национално или наднационално равнище; с течение на времето обхватът на нарушението може ли да нараства като мащаб.

✓ контекст на обработването – определяне на обстоятелствата, при които са обработвани личните данни, например в трудовия контекст, обработване за статистически изследвания, има ли трансгранично движение на личните данни, предавани ли са извън Европейския съюз, което може да затрудни физическите лица.

✓ цел на обработването – отчитане на първоначалните цели, за които данните са събирани, но и всякакви други съвместими с тях последващи цели, за които данните са използвани. Анализът на риска трябва да отчита евентуалното засягане на правата и свободите на субектите при обработване за всички цели.

✓ естество на нарушението – категоризация дали нарушението засяга поверителността, целостта или наличността на личните данни или представлява комбинация от тях.

✓ леснота на идентифициране на физическите лица – рискът се увеличава, ако въз основа на личните данни, засегнати от нарушението, физическите лица се идентифицират или лесно могат да бъдат идентифицирани, респ. се изключва, ако лицата не могат да бъдат идентифицирани.

✓ сериозност на последиците за засегнатите лица – отчита се като комбинация от вероятността за настъпване на вредоносни последици (ниска, средна, висока) и тяхната тежест, определена според засегнатите права и свободи.

✓ специални характеристики на засегнатите физическите лица – изследва се дали кръгът на засегнатите лица е съставен от уязвими групи, например деца, служители и други с оглед особеностите на конкретния случай.

✓ приблизителен брой на засегнатите физически лица – определяне като общ брой, а при възможност диференциране според естеството на нарушението.

✓ приблизителен брой на засегнатите записи от лични данни – индикативно за обхвата на нарушението.

- Риск от нарушението на сигурността на личните данни е налице, когато администраторът не е в състояние да спазва принципите, свързани с обработването на

личните данни - законосъобразност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, отчетност.

- Висок риск от нарушение на сигурността на личните данни има, когато могат да бъдат причинени физически, материални или нематериални вреди за засегнатите физически лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица. Високият риск може да произтича от уязвимостта на лицата, чиито данни се обработват, например деца, или от обема на личните данни и засягането на голям брой субекти на данни.
- Администраторът документира анализа, който прави относно тежестта на нарушението и на рисковете, които то поражда, в съответствие с принципа на отчетност.

V. ПРЕДПРИЕМАНЕ НА МЕРКИ ЗА ОГРАНИЧАВАНЕ НА НЕБЛАГОПРИЯТНИТЕ ПОСЛЕДИЦИ

1. В зависимост от вида на нарушението на сигурността на личните данни, се предприемат мерки за ограничаване на неблагоприятните му последици в следните насоки:

– при нарушение на поверителността: незабавно преустановяване на неразрешения достъп до лични данни; заличаване на личните данни във всички неразрешени публикации, включително отправяне на искания за премахване от кеширани версии на интернет страници, където са били публикувани; криптиране на лични данни при тяхното изпращане; уведомяване на прокуратурата и полицията, ако деянието съставлява престъпление; временно преустановяване на достъпа до електронна услуга, която е обект на нарушението; други мерки с превантивен или последващ характер;

– при нарушение на целостта: възстановяване на данните в състоянието преди неразрешената или случайната промяна; установяване дали неточни данни са предадени на получатели; уведомяване на получателите за коригиране на данните; други мерки с превантивен или последващ характер;

– при нарушение на наличността: определяне дали неразрешената или случайната загуба на достъп до лични данни е за определен период от време или постоянна; възстановяване на личните данни от резервни копия или от други източници; определяне дали има негативно въздействие върху правата и свободите на засегнатите физически лица от загубата на наличността; други мерки с превантивен или последващ характер.

2. Ако не е възможно да бъдат идентифицирани подходящи мерки за овладяване на нарушението на сигурността на личните данни, се предприема незабавно уведомяване на надзорния орган.

VI. УВЕДОМЯВАНЕ НА НАДЗОРНИЯ ОРГАН ЗА НАРУШЕНИЕТО НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

- На основание чл. 33 от Регламент (ЕС) 2016/679 и чл. 67, ал. 1 от ЗЗЛД администраторът уведомява надзорния орган – Комисията за защита на личните данни или Инспектората към Висшия съдебен съвет, съобразно техните правомощия.
- Задължението за уведомяване на надзорния орган се прилага в случай, че съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Без значение какво е нивото на риска, но такъв трябва да е идентифициран.

- Уведомяването на надзорния орган се извършва без ненужно забавяне и по възможност най-късно до 72 часа след узнаване за нарушението. Ако не могат да бъдат предприети мерки за ограничаване на неблагоприятните последици, надзорният орган се уведомява незабавно.
- Информацията до надзорния орган трябва да съдържа:

✓ описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

✓ 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;

✓ описание на евентуалните последици от нарушението на сигурността на личните данни;

✓ 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.

Чл. 67, ал. 4 от ЗЗЛД допуска информацията в уведомлението да се подава поетапно, когато и доколкото не е възможно да се даде едновременно. Поетапното уведомяване се прилага при по-сложни инциденти, при които пълното изясняване на обстоятелствата не е възможно в срока за уведомяване. Ако уведомлението е подадено след изтичане на 72-часовия срок от узнаването, в него трябва да се съдържат и причините за забавянето.

- За уведомяването на Комисията за защита на личните данни се използва образец на формуляр, утвърден от Комисията – Приложение 1 към настоящата процедура.

- За уведомяване на ИВСС – Приложение 2 към настоящата процедура.

VII. СЪОБЩАВАНЕ НА ЗАСЕГНАТИТЕ ОТ НАРУШЕНИЕТО СУБЕКТИ

Съобщаване на засегнатите от нарушението на сигурността субекти на данни се изисква, когато има вероятност нарушението да породи висок риск за правата и свободите на физическите лица.

Не е предвиден срок за съобщаване на нарушението на субекта на данни, но това се прави, когато е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват дадените от него насоки.

Съобщението трябва да се направи на ясен и прост език и да съдържа:

– описание на естеството на нарушението на сигурността на личните данни;

– посочване на името и координатите за връзка с длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

– описание на евентуалните последици от нарушението;

– описание на предприетите или предложените от администратора мерки за справяне с нарушението и за намаляване на евентуалните неблагоприятни последици.

Съобщението до засегнатите субекти на данни се прави в писмена/електронна форма при използване на образеца от настоящата процедура – Приложение 3.

В чл. 68, ал. 3 от ЗЗЛД съотв. в чл. 34, пар. 3 от Регламент (ЕС) 2017/679 са посочени три алтернативни условия, при които съобщаване на нарушението на субекта на данни не се изисква:

– администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките,

които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

– администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни;

– уведомяването би довело до непропорционални усилия; в този случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да са в еднаква степен ефективно информирани.

Ако реши да се позове на някое от тези условия, администраторът трябва да е в състояние да докаже на надзорния орган, че са налице съответните предпоставки. Предвид това е целесъобразно да бъдат документирани обстоятелствата, послужили като основание да не се съобщи нарушението на засегнатите субекти на данни.

VIII. ДОКУМЕНТИРАНЕ НА НАРУШЕНИЕТО

Администраторът е задължен да документира всяко нарушение на сигурността на личните данни, без значение дали съществува вероятност от него да се породи риск или да настъпи висок риск за правата и свободите на физическите лица. Целта на тази документация е да дава възможност на надзорния орган да провери дали са спазени изискванията на чл. 33 от Регламента и чл. 67, ал. 5 ЗЗЛД.

Нарушения на сигурността на личните данни се документират в Регистъра – Приложение 4 от настоящата процедура.