РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – КНЕЖА

УТВЪРЖДАВАМ:

Пламен Тодоров
И. ф. Административен ръководител -
Председател на РС – Кнежа

ПРОЦЕДУРА ЗА ДЕЙСТВИЯ ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В РАЙОНЕН СЪД КНЕЖА

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

1. Терминологични уточнения – по смисъла на тази процедура:

1.1. „Нарушение на сигурността на личните данни“ е 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).

1.2. „Унищожаване“ е налице, когато личните данни ги няма или ги няма във вид, в който администраторът може да ги използва.

1.3. „Повреждане“ е налице, когато личните данни са променени, подправени или станали вече непълни.

1.4. „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.

1.5. „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.

2. Признаци за нарушение на сигурността на личните данни

2.1. При установяване на признаци за нарушение на сигурността на личните данни всеки служител на Районен съд Кнежа е длъжен незабавно да информира административния си ръководител или длъжностното лице по защита на данните.

2.2. Признаците на нарушенията на сигурността 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

Вярно с оригинала

лични данни и други подобни, при които е вероятно да има унищожаване, повреждане, загуба или нерегламентиран достъп до лични данни, констатирани несъответствия между установените мерки за защита и практическото им прилагане.

2.3. При разглеждане на сигнала или анализа на признаците за нарушаване администраторът ползва съдействието на длъжностното лице по защита на данните.

3. Установяване на естеството на нарушението

3.1. Председателят на Районен съд Кнежа със съдействието на длъжностното лице по защита на данните преценява дали има нарушение на сигурността на личните данни и ако да, в какво се изразява неговото естество.

3.2.Административният ръководител – председател може да свика при необходимост екип за реагиране при нарушения на сигурността на информацията в Районен съд – Кнежа. Постоянният състав на екипа за реагиране при нарушения на сигурността на информацията в Районен съд – Кнежа се състои от: Административният ръководител – председател на съда или неговият заместник на основание Заповед за заместване; административният секретар на съда; длъжностно лице по защита на личните данни на съда и системният администратор на съда В зависимост от нивото на риска и възможните последици, определени по Методологията за оценка на тежестта на пробив в сигурността на личните данни в Районен съд – Тутракан, Административният ръководител – председател на съда може да включи към постоянния състав на екипа и други магистрати и/или служители от съда, със заповед за конкретния случай. Екипът за реагиране при нарушения на сигурността на информацията в Районен съд – Кнежа осъществява дейността си до отстраняване на риска и последиците от възникналата ситуация. При необходимост за дейността на екипа може да бъдат съставяни писмени документи.

3.3. Преценка на получената първоначална информация може да се направи по следните критеии:

- налице ли е несъответствие с нормативно предписани изисквания, свързани със защитата на личните данни;

- налице ли е несъответствие с вътрешни правила, установени в структурата на администратора/обработващия лични данни;

- има ли неразрешена или случайно разкриване или достъп до лични данни;

- има ли неразрешена или случайна промяна на лични данни;

-има ли неразрешена или случайна загуба на достъп до или унищожаване на лични данни;

- недостъпност на личните данни, от което следват негативни последици за субектите на данни – например невъзможност да упражняват техните права, опасност за техния живот или здраве и др. (нарушение на достъпността).

3.4 Нарушенията на сигурността на личните данни се категоризират в следните видове, както и в каквато и да е комбинация от тях:

а) нарушение на поверителността – когато има неразрешено или случайно разкриване

или достъп до лични данни;

б) нарушение на целостта – когато има неразрешена или случайна промяна на лични данни;

в) 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.

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

3.5 В случай че не са установени признаци на нарушение на сигурността на личните данни, но има данни за неизпълнение на изискванията на Регламент ЕС 2016/679, ЗЗЛД или други нормативни актове, свързани със защитата на личните данни, администраторът предприема своевременно мерки за отстраняване на констатираните слабости или за оптимизиране на прилаганите технически и организационни мерки.

3.6. Във всеки случаи когато се установи нарушение на сигурността на личните данни, изразяващо се в загуба на поверителност, цялостност, наличност или достъпност на личните данни или каквато и да е комбинация от тях, се извършва анализ на риска от нарушението спрямо правата и свободите на засегнатите субекти на данни.

4. Анализ на риска от нарушението за правата и свободите на физическите лица

4.1. 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 (§ 1, т. 16 от Допълнителните разпоредби на Закона за защита на личните данни).

4.2. При определяне на вероятността и тежестта на риска се отчитат следните обстоятелства:

а) 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.

б) 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.

в) 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 могат да упражняват правата си в областта на защитата на данните.

г) цел на обработването – отчитане на първоначалните цели, за които данните а

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 на всички цели на обработването.

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

е). лесната 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.

ж). 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.

з) 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.

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

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

4.3. 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.

4.4. 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.

4.5. За обективност на анализа се използват Препоръките за методология на оценката на тежестта на нарушенията на личните данни (Recommendations for a methodology of the assessment of severity of personal data breaches) на Агенцията на Европейския съюз за киберсигурност (European Union Agency for Cybersecurity, ENISA), част от които се съдържат в Приложение 1 към настоящата процедура.

4.6. Администраторът, респ. длъжностното лице по защита на данните документира анализа, който прави относно тежестта на нарушението и на рисковете, които то поражда, в съответствие с принципа на отчетност.

5. Предприемане на мерки за ограничаване на неблагоприятните последици

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

а) 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;

б) при нарушение на цялостността: 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;

в) 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.

5.2. 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.

6. Уведомяване на надзорния орган за нарушението на сигурността на личните данни

6.1. На основание чл. 33 от Регламент (ЕС) 2016/679 администраторът уведомява надзорния орган – за Република България Комисията за защита на личните данни с адрес София 1592, бул. „Проф. Цветан Лазаров“ № 2, електронна поща kzld@cpdp.bg, интернет страница www.cpdp.bg или Инспектората към Висшия съдебен съвет с адрес гр. София, ул. "Георг Вашингтон" №17, ivss@inspectoratvss.bg, интернет страница https://www.inspectoratvss.bg, 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. Например няма да има риск, респ. не се изисква уведомяване на надзорния орган, ако е откраднатa/изгубена флаш памет с криптирани данни и уникалният код не е разкрит. Ако кодът е разкрит по-късно, уведомяването е задължително. Не се изисква уведомяване при краткотрайна загуба на наличността, например при прекъсване на електрозахранването, но такъв инцидент подлежи на

вписване в регистъра на нарушенията на сигурността на личните данни.

6.2. 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.

6.3. Информацията до надзорния орган трябва да съдържа обстоятелствата по чл. 33, пар. 3 от Регламент (ЕС) 2016/679:

а) 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 количеството 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 евентуални неблагоприятни последици;

Ако уведомлението е подадено след изтичане на 72-часовия срок от узнаването, в него трябва да се съдържат и причините за забавянето.

6.4. Регламент (ЕС) 2016/679 допуска информацията в уведомлението да се подава поетапно, когато и доколкото не е възможно да се даде едновременно. Поетапното уведомяване вероятно ще се прилага при по-сложни инциденти, при които пълното изясняване на обстоятелствата не е възможно в срока за уведомяване.

За уведомяването на Комисията за защита на личните данни се използва формуляр, утвърден от Комисията – Приложение 2 към настоящата процедура.

7. Съобщаване на засегнатите от нарушението субекти на данни

7.1. 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.* При определянето на риска се вземат предвид всички обстоятелства по т. 4 от настоящата процедура, както и нововъзникнали, новонастъпили или узнати, открити или по друг начин станали впоследствие известни на администратора обстоятелства след извършването на анализа на риска.

7.2. 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.

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

а) описание на естеството на нарушението на сигурността на личните данни;

б) 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;

в) описание на евентуалните последици от нарушението;

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

7.4. 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:

а) 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;

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

в) съобщаването би довело до непропорционални усилия, в който случай Регламентът изисква да се направи публично съобщение или да се вземе друга подобна мярка, така че субектите на данни да бъдат 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.

8. 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. Регламент (ЕС) 2016/679 изрично посочва значението на тази документация – да дава възможност на надзорния орган да провери дали са спазени изискванията на чл. 33 от Регламент (ЕС) 2016/679. За целта длъжностното лице по защита на данните своевременно попълва регистъра на нарушенията на сигурността на личните данни, предвиден като образец във Вътрешните правила за мерките и средствата за защита на личните данни, обработвани в Районен съд Кнежа.

Процедурата за действия при нарушаване на сигурността на личните данни в РС Кнежа е утвърдена със Заповед № 110-АД/17.12.2024г. на и. ф. административния ръководител-председател на съда и влиза в сила от датата на утвърждаването й.

Приложение № 1 към раздел VI

УВЕДОМЛЕНИЕ

за нарушаване на сигурността на данните

на основание чл. 33 от Регламент (ЕС) 2016/679 (Общия регламент относно защитата на личните данни) или на основание чл. 67 от Закона за защита на личните данни

Този формуляр е за администратори на лични данни, които са имали нарушение на сигурността и трябва да докладват на Комисията за защита на личните данни (КЗЛД).

Трябва да се уверите, че предоставената информация е възможно най-точна и да предоставите възможно най-много подробности.

1.Тип на уведомлението

1.1 Първоначално ДА НЕ

(В случай че не е налице цялата информация за нарушението на данните и ще бъде представено без ненужна забавяне последващо уведомление. Ако е имало забавяне при докладването на това нарушение, моля обяснете защо.)

.....

1.2 Последващо ДА НЕ

(В случай, че това уведомление е последващо, моля, посочете № и дата на първоначално подаденото уведомление относно нарушението)

.....

2. За нарушението

2.1. Продължаващо нарушение ДА НЕ

.....

2.2. Кога (начална дата и час) е настъпило нарушението: .....

(Ако не знаете точните дата/час , моля, посочете приблизителни - година / месец / дата / час)

2.3. Кога (начална дата и час) е установено нарушението: .....

(Ако не знаете точните дата/ час , моля, посочете приблизителни - година / месец / дата / час)

2.4. Моля, опишете как открихте/разбрахте за нарушението?

.....

2.5. Причини за неспазването на 72-часовия срок .....

(Задължително се попълва, в случай че са изминали повече от 72 часа от узнаване за нарушението)

2.6. Дата на уведомяване от обработващия (ако е приложимо).....

(Ако не знаете точните дата/ час , моля, посочете приблизителни. Попълва се само в случай, че обработващият лични данни Ви е уведомил за нарушението на данните)

2.7. Коментари за датите.....

(По желание - можете да предоставите допълнителна информация относно датите на уведомяване, както и да посочите дали не са Ви известни точните дати, ако смятате, че е необходимо.)

3. Данни за нарушението

3.1. Описание на нарушението (Моля, опишете какво се е случило)

.....

3.2. Моля, опишете как е станал инцидентът?

.....

3.3. Моля, уточнете, според Вас, дали това е:

3.3.1. Нарушение на поверителността? ДА НЕ

(Попълвате "ДА" в случай на неправомерно, преднамерено или случайно разкриване или достъп до лични данни. Това 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. неразрешено разкриване на данните или неоторизиран достъп до данните и т.н.)

И / ИЛИ

3.3.2.Нарушение на целостта? ДА НЕ

(Попълвате "ДА" в случай на преднамерено или случайно повреждане на лични данни. „Повреждане" е налице, когато личните данни са променени, подменени/преправени или са непълни.)

И / ИЛИ

3.3.3. Нарушение на наличността? ДА НЕ

(Попълвате "ДА" в случай преднамерена или случайна загуба на данни, унищожаване на данни или неналичена услуга. „Загуба" на лични данни е състояние, при което данните може да са все още налични, но администраторът на лични данни (АЛД) е загубил контрол или достъп до тях или вече не ги притежава. „Унищожаване" на лични данни е налице, когато данните вече ги няма или ги няма във вид, в който може да бъдат използвани.)

4. Категории данни на физическите лица, засегнати от нарушението

Идентичност на физическите лица:

- ○ име;
- ○ ЕГН;
- ○ адрес;
- ○ паспортни данни;

Биометрични и генетични данни:

- ○ човешки геном;
- ○ дактилоскопични отпечатъци;
- ○ снимки на ретина;
- ○ ДНК;
- ○ хромозоми;

○ месторождение;
○ телефон;
○ е-мейл
○ други:.....

○ други:.....

Икономическа идентичност:
○ имотно състояние;
○ финансово състояние;
○ участие и/или притежаване на дялове или ценни книжа в дружества;
○ други:.....

Семейна идентичност:
○ семейно положение;
○ родствени връзки;
○ други: .....

Социална и културна идентичност:
○ произход;
○ образование;
○ трудова дейност;
○ среда;
○ навици;
○ интереси;
○ хоби;
○ други:.....

Лични данни, които разкриват:
○ произход (расов, етнически)
○ убеждения (политически, религиозни, философски)
○ членство в политически партии, организации, сдружения с религиозни, философски, политически или синдикални цели
○ сексуалния живот и/или сексуалната ориентация
○ други: .....

○ **Лични данни, които се отнасят до наказателни присъди и престъпления.**

○ **Лични данни, които се отнасят до физическото и психическо здраве.**

○ **Лични данни, които се отнасят до местоположение, например координати.**

○ **Данни и/или съвкупност от гореизброените данни, които могат да послужат за профилиране.**

5. Брой записи на лични данни, засегнати от нарушението .....

6. Брой субекти на данни (физически лица), засегнати от нарушението .....

(Един и същи субект може да фигурира в няколко записа на данни и/или в един запис да се съдържат данни за повече от едно физическо лице)

7. Колко субекти на данни може да бъдат засегнати .....

8. Категории субекти на данни:

- ○ служители/персонал
- ○ потребители
- ○ абонати
- ○ клиенти
- ○ контрагенти
- ○ кандидати за работа
- ○ жалбоподатели
- ○ членове и поддръжници на политически партии
- ○ пациенти
- ○ учащи
- ○ нарушители или заподозрени
- ○ деца
- ○ хора с увреждания
- ○ възрастни хора
- ○ граждани на други държави от ЕС
- ○ граждани на други държави извън ЕС
- ○ други .....

9. Превантивни технически и организационни мерки, предприети от АЛД/ОЛД
(Подробно описание на техническите и организационни мерки преди нарушението)

.....

10. Потенциални последствия за правата и свободите на засегнатите субекти на данни от нарушението.

10.1 Възможно ли е идентифициране на засегнатите лица? Моля, обяснете:

.....

10.2. Налице ли е загуба на способността да се предоставя критична услуга за засегнатите субекти на данни? Моля, опишете:

.....

10.3. Естество на потенциалното въздействие върху субекта на данните. Моля, опишете:

.....

(Примери: Загуба на контрол над лични данни, ограничаване на права, дискриминация, кражба на самоличност, финансови загуби, засягане на репутацията, загуба на поверителност на личните данни, защитени от професионална тайна, неоторизирано превръщане на псевдонимизирани данни в обикновени данни или други (моля, уточнете)

10.4. Тежест на потенциалното въздействие .....

(незначително - ограничено - значително – максимално. Тук посочете резултата от извършената оценка на въздействието на нарушението по отношение на правата на субектите на данни)

11. Възможно ли е нарушението на личните данни да доведе до висок риск за субектите на данни? Моля, дайте подробности.....

12. Опишете действията, които сте предприели или предлагате да предприемете в отговор на нарушението.

.....

13. Предприели ли сте действия за ограничаване на нарушението? Моля, опишете тези коригиращи действия .....

(Описание на мерките, предприети от администратора, за отстраняване на нарушението в рамките на 72 часа и в последствие)

14. Моля, очертайте всички стъпки, които предприемате, за да предотвратите повторение на нарушението и в какъв срок очаквате те да бъдат изпълнени.

.....

15. Уведомили сте субектите на данни за нарушението?

.....

16. Моля, посочете средства за комуникация, които сте използвали за информиране на субектите на данни.

.....

17. Уведомяване на други органи/организации за нарушението:

17.1. За които имате задължение за уведомяване по закон/нормативен акт.

.....

17.2. Други администратори на лични данни, на които сте предавали/изпращали личните данни, засегнати от нарушението.

.....

17.3. Други надзорни органи

.....

18. Данни за администратора на лични данни, засегнат от нарушението

- Име на организацията .....
- ЕИК/БУЛСТАТ Регистрационен номер на компанията (ако е наличен) .....
- Сфера на дейност .....

(За юридическо лице или публичен орган е достатъчно да бъдат попълнени само от част I, т. 1 „Код по БУЛСТАТ/ЕИК", т. 4 и част II, в случай, че другите данни са част от публичен регистър (регистър БУЛСТАТ

и Търговски регистър). Необходимите данни ще бъдат събрани служебно от администрацията на КЗЛД в съответствие с чл. 2 от Закона за електронното управление.)

- Данни за контакт .....
- Длъжностно лице за защита на данните или име и позиция на лицето за контакт относно нарушението
- Електронна поща
- Телефонен номер
- Пощенски адрес

19. Други администратори или обработващи лични данни, свързани с нарушението

19.1. Участие на други администратори или обработващи, свързани с нарушението

ДА НЕ

19.2. Име и качество на другите участващи страни .....

(Тук се въвеждат име и качество на другата (ите) организация (и), участваща (и) в нарушението, и дават подробности за тяхното участие (попълва се само в случай, че отговорът по-горе е ДА)

УКАЗАНИЯ ЗА ПОДАВАНЕ:

1. Начин за подаване на Уведомлението в КЗЛД:

   1.1. Лично, на хартиен носител – в деловодството на КЗЛД на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2;

   1.2. С писмо на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров" № 2, Комисия за защита на личните данни;

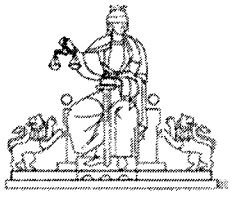
   1.3. На мейла на КЗЛД - kzld@cpdp.bg. В този случай, Уведомлението трябва да бъде подписано с Квалифициран електронен подпис (КЕП).

   1.4. Чрез Системата за сигурно електронно връчване, поддържана от Държавна агенция „Електронно управление". В този случай Уведомлението трябва да бъде попълнено и съответният електронен файл да бъде изпратен чрез тази система.

2. Уведомлението се подава от администратора или от изрично упълномощено от него лице с изрично нотариално заверено пълномощно при представителство от лица или организации или с нарочно адвокатско пълномощно (пълномощното се прилага и е неразделна част от Уведомлението).

3. Адресни данни, които са извън територията на Република България се вписват само в частта „Адрес".

ДАТА: **ПОДПИС:**



РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – КНЕЖА

Приложение № 2 към раздел VII

ДО

(посочва се съответният субект на данни)

Съобщение за нарушение на сигурността на личните данни на основание чл. 34, пар. 1 от Регламент (ЕС) 2016/679, чл. 68, ал. 1 и л от Закона за защита на личните данни от

.....
(посочва се администраторът на лични данни, които изпраща съобщението за нарушение на сигурността на личните данни)

Уважаеми г-н ..... /Уважаема г-жо .....

На..... година *(посочва се датата/моментът, в които администраторът е узнал, че е настъпило нарушение на сигурността)* .....
(посочва се администраторът) установи, че е настъпило нарушение на сигурността на личните данни, от което съществува вероятност да бъде породен висок риск за правата и свободите на физическите лица, чиито данни са обект на нарушението. Тъй като Вие сте сред тези лица, Ви предоставяме следната информация:

1. Естество на нарушението:
Нарушението се изразява в .....

(описва се естеството на нарушението, напр. осъществен нерегламентиран достъп до лични данни, неразрешено разкриване на данни, промяна, загуба на данни, неправомерно унищожаване на данни).

Нарушението засяга следните категории лични данни:.....

(описват са самите категории данни, ако същите са известни на администратора, напр. данни за физическа идентичност, като имена, ЕГН, номер на личен документ, постоянен адрес, подпис, електронна поща; данни относно икономическа идентичност, като данни за банкова сметка; данни за социална идентичност, като длъжност, образование, стаж, възнаграждение; данни относно физиологичната идентичност, като данни за диагноза, данни за пълна кръвна картина).

2. Координати за връзка е длъжностното лице по защита на данните или друга точка за контакт:
За контакт с администратора и допълнителна информация може да се обръщате към.....

(описват се координатите на длъжностното лице по защита на данните или на друга точка за контакт).

3. Евентуални последици от нарушението:

Нарушението на сигурността би могло да доведе до следните последици.....

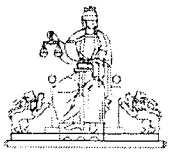
(описват се евентуалните неблагоприятни последици от нарушението, както и евентуалните рискове върху правата и свободите на субектите на данни, напр. кражба на самоличност. Ако администраторът счита, че от нарушението не се очаква да настъпят каквито и да било последици за субектите на данни, той следва да посочи съответни аргументи за този извод, напр. липса на неблагоприятни последици поради ограничен брой засегнати субекти на данни и/или ограничен брой засегнати данни, и/или естество на данните - обект на нарушението).

4. Мерки за справяне с нарушението на сигурността на личните данни:

За справяне с нарушението на сигурността на личните данни сме предприели технически и организационни мерки, както следва:

.....

(описват се видовете мерки, предприети от администратора за отстраняване на нарушението и/или за намаляване или преодоляване на неговите неблагоприятни последици, напр. уведомяване на засегнатите субекти на данни; уведомяване на органите на полицията или прокуратурата, в случай че нарушението на сигурността осъществява състав на престъпление; временно преустановяване на достъпа до електронна услуга, която е обект на нарушението и др. в зависимост от конкретните обстоятелства на нарушението и възможностите за реакция на администратора).



РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – КНЕЖА

РЕГИСТЪР НА НАРУШЕНИЯТА НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

№	Регистър с лични данни	Естество на нарушението	Място на нарушението	Време на възникване на нарушението	Време на узнаване за нарушението	Категории лични данни/ брой записи	Категории субекти на данни	Субекти на данни в други държави	Носители на данни	Уведомление до надзорния орган	Съобщения до субектите на данни	Причини за забавяне	Неблагоприятни последици	Предприети мерки
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

1. **Графа 1** служи за създаване на номерация на нарушенията, валидна за структурата на администратора.
2. В **графа 2** се посочва регистърът на лични данни, засегнат от нарушението.
3. В **графа 3** се отбелязва естеството на нарушението - изтриване, унищожаване и, загуба, промяна, неоторизиран достъп, разкриване, разпространяване или оповестяване на данни по друг начин, който ги прави достъпни без правно основание.
4. **Графа 4** служи за посочване на физическото място на възникване на нарушението.
5. В **графа 5** се отразява предполагаемото време на възникване на нарушението.
6. В **графа 6** се отразява времето на узнаване за нарушението.
7. В **графа 7** се посочват категориите лични данни и приблизителния брой записи, засегнати от нарушението.
8. В **графа 8** се отразяват категориите субекти на данни, засегнати от нарушението и техния приблизителен брой.
9. В **графа 9** се посочват категориите субекти на данни в други държави, засегнати от нарушението и техния приблизителен брой.
10. В **графа 10** се отразяват носителите на данни, засегнати от нарушението – документи на хартиен носител, носители за многократен запис, автоматизирани информационни системи, аудиозаписи, видеозаписи и други.
11. В **графа** 11 се отразява уведомлението до надзорния орган и датата, на която е направено.
12. В **графа 12** се посочва дали са направени съобщения за нарушения на сигурността на личните данни до субектите на данни.

13. В **графа 13** се посочват причините за забавяне в сроковете за уведомяване.
14. **Графа 14** служи за отразяване на констатираните и/или очаквани неблагоприятни последици на нарушението.
15. В **графа 15** се отразяват предприетите технически и организационни мерки за справяне с нарушението и за намаляване на неблагоприятните му последици.