Приложение № 1

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ

Долуподписаният/ата.....
ЕГН..... ,
адрес:.....

ДЕКЛАРИРАМ, ЧЕ

Се задължавам да не разгласявам лични данни, които се обработват от администратора и до които съм получил достъп при и по повод изпълнение на служебните ми задължения, като .....
(*заемана длъжност*)

Дата: Декларатор:

Приложение № 2

ИНФОРМИРАНО СЪГЛАСИЕ

За прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, Закона за защита на личните данни и подзаконовите нормативни актове по неговото прилагане

Информиран/а съм, че данните, които предоставям с показване на моята лична карта или друг документ за самоличност, са лични данни и попадат под специален режим на защита по смисъла на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, Закона за защита на личните данни и подзаконовите нормативни актове по неговото прилагане.

Информиран/а съм, че Районен съд – Кнежа в качеството на администратор на лични данни събира моите лични данни за постигане на законово допустими и позволени цели и заявявам, че изцяло доброволно предоставям личните си данни, за да бъдат използвани за постигане на посочените по-горе цели.

Информиран/а съм, че имам право на достъп до моите данни и право на изтриване /да бъда забравен/; право на коригиране и ограничаване използването на личните ми данни, право на възражение и на жалба срещу обработването на събраните в противоречие на закона или на даденото от мен съгласие лични данни; право на информиране при условие, че сигурността на личните ми данни бъде нарушена.

Информиран/а съм, че Районен съд – Кнежа в качеството на администратор на лични данни, поема задължение да събира, обработва, съхранява, архивира и унищожава моите лични данни само в рамките на законово уредените за съответните видове данни срокове, като гарантира тяхната сигурност и опазване в тайна от трети лица, както и да не събира,

обработва, разкрива, използва или предоставя на трети лица личните ми данни за други, различни от посочените по-горе цели.

С полагане на своя подпис удостоверявам, че съм запознат/а с посочените в настоящата информация права и последици, както и когато това е необходимо за реализиране на моите права и интереси.

гр.Кнежа

.....

Дата:.....

/име, презиме, фамилия/

.....

/подпис/

ДЕКЛАРАЦИЯ – СЪГЛАСИЕ

за обработване на лични данни във връзка с участие в конкурс за служител на длъжността „.....“ в Районен съд – Кнежа

Долуподписаният/ната .....

(име, презиме и фамилия на лицето)

Адрес:.....

.....

Телефон:.....

e-mail:.....

ДЕКЛАРИРАМ:

1. Съгласен/на съм Районен съд – Кнежа, в качеството на администратор на лични данни, да съхранява и обработва личните ми данни съгласно изискванията на Общия регламент относно защитата на данните (ЕС) 2016/679 и приложимото право на Европейския съюз и законодателство на Република България относно защитата на личните данни, които предоставям във връзка с участието ми в конкурс за служител на длъжността „.....“ в Районен съд – Кнежа.

2. Запознат/а с информацията по чл. 13 и чл. 14 от Общия регламент за защита на данните и със съобщението за поверителност на личните данни на кандидатите за работа, предоставена от Районен съд – Кнежа, с правата ми на субект на личните данни съгласно Регламента.

3. Известно ми е, че:

- моите лични данни, които съм представил/а на Районен съд – Кнежа в рамките на процедурата по кандидатстване в конкурс за служител на длъжността „.....“ се обработват от Районен съд – Кнежа за целите на конкурсната процедура;

- информиран/а съм, че Районен съд – Кнежа може да обработва моите лични данни само докато и доколкото това е необходимо във връзка с конкурсната процедура. За обработка извън тези рамки Районен съд – Кнежа се нуждае от моето допълнително съгласие в съответствие с разпоредбите за защита на личните данни.

- заявлението и всички приложени към него документи се съхраняват в Районен съд – Кнежа за срок от шест месеца, като срокът по чл. 25к от ЗЗЛД започва да тече от момента на приключване на конкурсната процедура респ. сред изтичане на сроковете за обжалването й, като е налице правна възможност за удължаване на 6-месечния срок със съгласието на кандидата, като той има право по всяко време и без да излага причина да оттегли своето съгласие, в резултат на което по-нататъшното обработване на данните трябва да бъде преустановено, като същите следва да бъдат изтрити или унищожени от администратора на лични данни. При писмено изразено искане всеки кандидат може да получи обратно предоставените за целите на конкурса оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, в 6-месечен срок от окончателното приключване на процедурата, освен ако специален закон предвижда друго.

- доброволния характер на предоставянето на данните; правото на достъп и на коригиране на събраните данни; правото да оттегля даденото съгласие по всяко време. Съзнавам, че оттеглянето на съгласието ми по - късно няма да засегне законосъобразността на обработването, основано на даденото от мен сега съгласие.

4. Давам съгласие резултатите от проведения конкурс да бъдат публикувани на интернет страницата на Районен съд – Кнежа и да бъдат оповестени на таблото за съобщения в съда.

5. ДАВАМ СЪГЛАСИЕ / ОТКАЗВАМ трите ми имена да бъдат публикувани на интернет страницата на Районен съд – Кнежа и да бъдат оповестени на таблото за съобщения в съда във връзка с участието ми в конкурса.

/ При отказ от публикуване на трите имена на кандидата ще бъде публикуван входящият номер, получен при подаване на документите за участие в обявения конкурс/.

дата .....

гр. Кнежа ДЕКЛАРАТОР:.....

ОТТЕГЛЯНЕ НА СЪГЛАСИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Данни лицето:

Име: .....

В качеството на .....

Оттеглям съгласието си ..... Районен съд Кнежа в качеството си на администратор на лични данни, да обработва предоставените от мен лични данни за целите на .....

Известно ми е, че оттеглянето на съгласието не засяга законосъобразността на обработването на личните данни от администратора преди оттеглянето.

Информиран/а съм за последиците от оттеглянето на съгласието за обработване на личните ми данни, което прекратява участието ми в .....

Дата: .....20..... г. **Подпис**.....

Приложение № 5

УВЕДОМЛЕНИЕ ДО КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ОТНОСНО НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

В РАЙОНЕН СЪД – КНЕЖА

ДО

Председателя

на Комисията за зашита на личните данни,

бул. „Проф. Цветан Лазаров"[4] № 2 София, 1592

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО ПРЕДСЕДАТЕЛ НА КЗЛД,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, в изпълнение на чл. 33 от Общия регламент за защита на данните (ОРЗД -Регламент (ЕС) 2016/679), Ви уведомяваме, че е констатирано следното нарушение/я:

Данни за нарушението

Описание на естеството на нарушението	*(свободен текст)*
Категории засегнати субекти на данни и техният приблизителен брой	*(съобразно описаното в Регистъра на дейностите по обработка на личните данни и наличната техническа информация)*
Категории засегнати лични данни и приблизително количество на засегнатите записи	*(съобразно описаното в Регистъра на дейностите по обработка на личните данни и наличната техническа информация)*
Дата и час на установяване на нарушението	*(свободен текст)*
Причини за забавяне на настоящото уведомление (когато не е подадено в срок от 72 часа)	*(свободен текст - ако е приложимо)*

Описание на евентуалните последици от нарушението, според категориите лични данни

№	Категория лични данни	Описание
1		
2		

Технически и организационни мерки за справяне с нарушението и последиците от него

№ на последица	Описание на мерките

Данни за администратора

Наименование на администратора	
	(наименование на институцията)
Координати за връзка	
	(имейл адрес, телефон)
Съвместни администратори	
	(наименование, координати за връ и<и - ако е приложимо)
Длъжностно лице по защита на личните данни / Отговорно лице в съответствие с вътрешните процедури на институцията	
	(име, фамилия, координати за връзка)

С уважение:

Административен ръководител –

Председател на Районен съд - Кнежа
(подпис, печат)

(име, фамилия)

Приложение № 6

УВЕДОМЛЕНИЕ ДО ИНСПЕКТОРАТА НА ВИСШИЯ СЪДЕБЕН СЪВЕТ

ОТНОСНО НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

В РАЙОНЕН СЪД – КНЕЖА

ДО

ГЛАВНИЯ ИНСПЕКТОР НА ИВСС
ГР. СОФИЯ, П.К. 1000
УЛ. "ГЕОРГ ВАШИНГТОН" №17

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО ГЛАВЕН ИНСПЕКТОР,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, в изпълнение на чл. 33 от Общия регламент за защита на данните (ОРЗД -Регламент (ЕС) 2016/679) и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година, Ви уведомяваме, че е констатирано следното нарушение/я:

Данни за нарушението

Описание на естеството на нарушението	*(свободен текст)*
Категории засегнати субекти на данни и техният приблизителен брой	*(съобразно описаното в Регистъра на дейностите по обработка на личните данни и наличната техническа информация)*
Категории засегнати лични данни и приблизително количество на засегнатите записи	*(съобразно описаното в Регистъра на дейностите по обработка на личните данни и наличната техническа информация)*
Дата и час на установяване на нарушението	*(свободен текст)*
Причини за забавяне на настоящото уведомление (когато не е подадено в срок от 72 часа)	*(свободен текст - ако е приложимо)*

Приложение № 6

Описание на евентуалните последици от нарушението, според категориите лични данни

№	Категория лични данни	Описание
1		
2		

Технически и организационни мерки за справяне с нарушението и последиците от него

№ на последица	Описание на мерките

Данни за администратора

Наименование на администратора	
	(наименование на институцията)
Координати за връзка	
	(имейл адрес, телефон)
Съвместни администратори	
	(наименование, координати за връ и<и - ако е приложимо)
Длъжностно лице по защита на личните данни / Отговорно лице в съответствие с вътрешните процедури на институцията	
	(име, фамилия, координати за връзка)

С уважение:

Административен ръководител –

Председател на Районен съд - Кнежа
(подпис, печат)

(име, фамилия)

РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – КНЕЖА

Приложение № 7

Изх. № ...../..... 20..... г.

ДО
.....
(посочва се субектът на данни)

СЪОБЩЕНИЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ НА ОСНОВАНИЕ ЧЛ. 34, ПАР. 1 ОТ РЕГЛАМЕНТ (ЕС) 2016/679 ОТ РАЙОНЕН СЪД - КНЕЖА

УВАЖАЕМИ ГОСПОДИН/ГОСПОЖО .....,

Във връзка с установено нарушение на сигурността на обработвани от нас лични данни, което може да породи висок риск за Вашите права и свободи като засегнат субект на данни, в изпълнение на чл. 34, пар. 1 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), Ви предоставяме следната информация:

1. Естество на нарушението на сигурността на личните данни

Нарушението на сигурността, което засяга Ваши лични данни, се изразява в .....*(описва се естеството на нарушението, засегнатите от него лични данни и причините, поради които се очаква висок риск за правата и свободите на субекта на данни)*

2. Име и координати за връзка с длъжностното лице по защита на данните (или друга точка за контакт, от която може да се получи повече информация)

Име на длъжностното лице по защита на данните или друга точка за контакт	
Координати за връзка	

3. Описание на евентуалните последици от нарушението, според категориите лични данни

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)*

4. Описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни

съобщение до субекта на данни при нарушение на сигурността на личните данни

За справяне с нарушението на сигурността на личните данни са предприети следните действия: .....*(опишете предприетите действия)*

За намаляване на евентуални неблагоприятни последици от нарушението на сигурността са предприети/планирани следните действия ..... *(опишете, ако е приложимо за случая)*

В случай, че имате допълнителни въпроси във връзка с нарушението на сигурността на личните Ви данни, не се колебайте да се свържете с нас, като използвате посочените по-горе координати за връзка.

Дата ..... **Председател.....**

Приложение № 8

РЕГИСТЪР НА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

РЕГИСТЪР НА НАРУШЕНИЯТА

	Дата и час на установяване на нарушението	Описание на нарушението (източник, вид и мащаб на засегнатите данни, причини за нарушението – ако е приложимо)	Засегнати субекти, категория и брой	Оценка на тежестта на пробива (приложение № 2)	Риск за правата и свободите на физическите лица	Възможни последици от нарушението	Предприети действия	Дата на изпълнение	Отговорни лица	Дата на уведомяване на засегнатото лице (ако е извършено)	Дата на уведомяване на надзорния орган (ИВСС или КЗЛД)	Причинни за забавяне на уведомлението (повече от 72 часа)
1.												
2.												
...												

МЕТОДОЛОГИЯ ЗА ОЦЕНКА НА ТЕЖЕСТТА НА ПРОБИВ В СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

ВЪВЕДЕНИЕ

1. Настоящата методология за оценка на тежестта на пробив в сигурността на личните данни разглежда изискванията, посочени в чл. 33 и чл. 34 от ОРЗД за уведомяване на надзорните органи и субекти на данни за установени пробиви в сигурността в контекста на адаптирана Методология за оценка на степента на тежест на нарушение на сигурността на личните данни, разработена и публикувана от European Union Agency for Network and Information Security (Агенция за мрежова и информационна сигурност на Европейския съюз).

НОРМАТИВНИ ОГРАНИЧЕНИЯ

2. Уведомленията по чл. 33и чл. 34 **са задължителни само** в следните случаи:

2.1. надзорният орган се уведомява само ако пробивът **може да доведе до риск** за правата и свободите на субектите на данни, засегнати от този пробив;

2.2. субектът на данни се уведомява само ако пробивът **може да доведе до висок риск** за правата и свободите на субектите на данни, засегнати от този пробив.

ПРОБИВ В СИГУРНОСТТА

3. Под **пробив в сигурността** следва да се разбира пробив в:

3.1. достъпа до информацията (конфиденциалност) - неразрешено или случайно разкриване на или достъп до лични данни;

3.2. целостта на информацията (интегритет) - неразрешена или случайна промяна на личните данни;

3.3. наличността на информацията (наличност) - случайна или неразрешена загуба на достъп до или унищожаване на лични данни.

РИСКОВЕ

4. Съгласно ОРЗД рискът за правата и свободите на физическите лица, с различна вероятност и тежест произтича от обработване на лични данни:

4.1. което би могло да доведе до физически, материални или нематериални вреди, по-специално когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия;

4.2. когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни;

4.3. които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална институция, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност;

4.4. оценяващо лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето,

личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили:

4.5. на уязвими лица. по-специално на деца;

4.6. включващо голям обем лични данни и засяга голям брой субекти на данни.

НИВО НА РИСК

5. Следните нива на риска се припознават от институцията, съобразено с възможните изисквания за уведомяване:

5.1. без риск;

5.2. нисък риск;

5.3. висок риск.

ОЦЕНКА НА РИСКА

6. Критериите, използвани за оценка на риска, са:

6.1. контекст на обработването на данни (КО)

6.2. възможност за идентификация на субекта на данни (ВИ)

6.3. обстоятелства относно пробива (ОП)

7. Изчисляването на риска се извършва по следната формула

РИСК = КО x ВИ + ОП

8. Извършва се следното приравняване на изчисления риск към нивото на риск и възможните последици

Ниво на риск	Приравняване	Възможни последици
	РИСК < 2	субектите на данни е възможно да изпитат няколко незначителни неудобства, които ще преодолеят без никакъв проблем (време, прекарано в повторно въвеждане на информация, раздразнение, объркване и т.н.)
Нисък риск	2 < РИСК < 3	субектите на данни е възможно да изпитат значителни неудобства, които те ще могат да преодолеят въпреки някои трудности (допълнителни разходи, отказ от достъп до услуги, страх, липса на разбиране, стрес, дребни физически неразположения и т.н.)
	3 <РИСК	субектите на данни е възможно да изпитат значителни последствия, които биха преодолели, макар и със сериозни трудности или необратими последици, които не могат да преодолеят (злоупотреби с финансови средства, черни списъци от финансови институции, имуществени щети, загуба на работа, призовка, влошаване на здравето, неработоспособност, дългосрочни психологически или физически заболявания, подлагане на дискриминация, смърт

КОНТЕКСТ НА ОБРАБОТВАНЕТО НА ДАННИ

9. Контекстът на обработваните данни се определя от тяхната дефиниция и свързване с една от следните групи, на базата на която се получава базовата стойност:

10.

Група	Описание	Базова стойност
Прости данни	биографични данни, данни за контакт, пълно име, данни за образованието. семейния живот, професионалния опит и т.н.	1
Поведенчески данни	местоположение, данни за трафика, данни за личните предпочитания и навици и др.	2
Финансови данни	всички видове финансови данни (например доходи, финансови транзакции, банкови извлечения, инвестиции, кредитни карти, фактури и т.н.), вкл. данни за социалното благосъстояние, свързани с финансовата информация	3
Чувствителни данни	съгласно ОРЗД расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни за разпознаване, здравословно състояние, сексуален живот, сексуална ориентация	4
Данни, свързани с присъди и нарушения	Лични данни, включително имена, адрес; вид и размер на наказанието. всяка информация, която се отнася до конкретен човек, ако с нея той може да бъде ясно идентифициран.	5

11. В случай, че данните принадлежат към повече от една категория, те се изследват във всяка от тях и се взема най-високия получен резултат.

12. Базовата стойност е възможно да бъде адаптирана, отчитайки други контекстни фактори

12.1. Увеличаващи риска фактори

а) обем на данните (включително като време и/или съдържание);

б) особености на администраторите (по отношение на сектора и продуктите/услугите, които предлагат);

в) особености на физическите лица (по отношение на обхващането на специфични групи от субекти напр. неравностойно положение, деца);

ВЪЗМОЖНОСТ ЗА ИДЕНТИФИКАЦИЯ НА СУБЕКТА НА ДАННИ

13. Дефинирани са четири нива на оценка на възможната идентификация на субекта на данни. Най-ниската оценка е в случай, че изключително може трудно да се установи субектът, макар и да е възможно. Най-високата оценка предполага директно идентифициране на субекта от придобитите данни.

Ниво	Пренебрежимо	Ограничено	Значително	Максимално
Стойност	0.25	0.5	0.75	**1**

14. **Нивото е производно в на възможността за комбиниране на придобитите данни с публични такива или на трети страни,** което да позволи идентифицирането на субекта.

15. При придобиване на криптирани данни, без ключа за декриптиране да е станал достояние, възможността за идентификация се приема за 0.

ОБСТОЯТЕЛСТВА ОТНОСНО ПРОБИВА

16. Обстоятелствата, относно пробива се изчисляват въз основа на вида на пробива в сигурността и неговия характер (случаен или целенасочен/зло намерен).

16.1 злонамерен характер предполага, че пробивът не е в следствие на грешка, човешка или техническа, или е причинен от умишлено действие на злонамерено намерение;

16.2 незлонамерените нарушения включват случаи на случайна загуба, неадекватно изхвърляне, човешка грешка и софтуерни грешки или неправилно конфигуриране;

16.3 злонамерените нарушения могат да включват (неизчерпателно):

а) случаи на кражба и „хакване" с цел да се навреди на субектите (например чрез излагане на личните им данни на неупълномощени трети страни);

б) прехвърляне на лични данни на трети страни с цел печалба (например продажба на списъци на лични данни);

в) действия, целящи да навредят на администратора на данни (например чрез кражба и предаване на лични данни на неразрешени страни).

16.4 възможно е да са налице повече от едно обстоятелство. В този случай, общото обстоятелство е равно на сбора на стойностите на отделните обстоятелства;

16.5 примери за оценка на обстоятелства, относно пробива по категории (бази):

База	**Стойност**	**Примери**
Конфиденциалност	0	Примери за данни, изложени на риск **без доказателства за настъпила незаконна обработка:** • при пренос се загубва хартиен файл или лаптоп; • оборудването е изхвърлено без унищожаване на личните данни.
	0.25	Примери за данни, предоставени на **известни** получатели: • e-mail с лични данни е изпратен неправилно до известен брой получатели; • някои клиенти имат достъп до акаунти на други клиенти в онлайн услуга.
	0.5	Примери за данни, предоставени на **неизвестен** брой получатели: • данните се публикуват в интернет съвет за съобщения; • данните се качват на P2P сайт; • служител продава CD ROM с данни за клиента; • неправилно конфигуриран уеб сайт ги прави публично достъпни чрез интернет данни на вътрешни потребители
Интегритет	0	Примери за **променени данни,** но без определена неправилна или незаконна употреба: • записите на база с лични данни са актуализирани неправилно, но оригиналът е възстановен, преди да е настъпило каквото и да е използване на променените данни.
	0.25	Примери за **данни, променени и евентуално използвани по неправилен или незаконен начин,** но с възможност да се възстановят: • записът, необходим за предоставянето на онлайн социална услуга, е променен и лицето трябва да поиска услугата по

		офлайн начин: • документ, който е важен за точността на файла на индивида в онлайн медицинска услуга, е променен
	0.5	Примери за данни, **променени и евентуално използвани по неправилен или незаконен начин,** без възможност за това възстановяване: • предишните примери, но оригиналите не могат да бъдат възстановени.
Наличност	0	Примери за **възстановяване на данни без затруднения:** • копие от файла се губи, но има други копия; • базата данни е повредена, но може лесно да бъде възстановена от други бази данни.
	0.25	Примери за **временна неналичност:** • базата данни е повредена, но може да бъде възстановена от други бази данни, макар чрез допълнителна обработка; • файлът е изгубен, но информацията може да бъде предоставена отново от субекта.
	0.5	Примери за **пълна липса на данни** (данните не могат да бъдат възстановени от администратора или от физически лица): • файлът е изгубен, базата данни е повредена, няма резервно копие на тази информация и тя не може да бъде предоставена от субекта.
Злонамереност	0.5	Нарушението се дължи на **умишлено действие** и/или с цел да навреди на субектите: служител на институцията умишлено споделя частни данни публично в социалните медии; служител на институцията продава частни данни на друга компания; членовете на дадена социална мрежа умишлено изпращат информация до други членове на семейството на субекта, за да им навредят

СПЕЦИФИЧНИ ФАКТОРИ

17 . В случай, че се касае за нарушение на интегритета или наличността на лични данни, които не могат да бъдат възстановени поради тяхната уникалност и те са необходими за осъществяване на правата и свободите на субектите на данни, то нивото на риска се приема за високо.

Регистър на дейностите по обработка на лични

Приложение № 10

Регистър	Цел на обработването	Субекти на данните	Категории лични данни	Категории получатели, пред които се разкриват данните	Основание за законосъобразност на обработването	Източник на данните	Длъжностни лица с достъп до данните	Средства, с които се обработват личните данни	Срок за съхранение на личните данни
1.Персонал-магистрати, съдии и съдебни служители	Изпълнение на функциите на работодател, изпълнение на дейности по осъществяване на трудови и осигурителни права на работещите по трудови правоотношения в Районен съд – Кнежа	Магистрати, ДСИ, Съдия по вписванията, съдебни служители	-физическа идентичност – имена, ЕГН- адрес, телефон, имейл, данни на документ за самоличност; -лични данни относно съдебно минало (свидетелство за съдимост); -данни за здравословно състояние – медицински свидетелства, болнични листове, епикризи, ТЕЛК; -социална идентичност – длъжност, семейно положение, професионална квалификация; -финансово положение – ведомости, доходи по трудово правоотношение, декларации на съдебните служители по ЗПКОНПИ -данни за физическата и психическата годност на субектите	НАП, НОИ, Банки, Служба по трудова медицина и др.	Изпълнение на договор или спазване на законово задължение (чл.6, пар.1, т."б" и т."в"; чл.9, пар.2, б."в"(ОРЗД); ЗСВ, КТ, КСО, ЗСч, ЗНАФ и др.	Субекта на данните; здравни заведения, ВСС, МП и др.	Административен ръководител-председател, административен секретар, системен администратор, счетоводител	Технически средства, АИС и мрежи, хартиен носител	50 години след прекратяване на трудовите правоотношения
2. Кандидати за съдебни служители	Изпълнение на функциите на юридическо лице-работодател, изпълнение на дейности по набиране на съдебни служители	Кандидати за вакантни длъжности в съдебната администрация	-физическа идентичност – имена, ЕГН- адрес, телефон, имейл, данни на документ за самоличност; -лични данни относно съдебно минало (свидетелство за съдимост); -данни за здравословно състояние-медицинско свидетелство-данни за физическата и психическата годност на кандидатите. -социална идентичност – длъжност, професионална квалификация	Органа по назначаване РС-Кнежа	Спазване на законово задължение (чл.6, пар.1, т."б" от ОРЗД) - предприемане на стъпки преди сключване на договор ; ЗСВ, НАС, КТ и др.	Субекта на данните	Административен ръководител, административен секретар,членове на конкурсната комисия	Хартиен и/или електронен носител	3 години след приключване на конкурсната процедура или след извършен одит
3.Съдебни дела, страни в съдебни производства	1.За служебни цели, свързани с индивидуализиране на страните и участниците в процеса, както и за всички дейности, свързани със съществуване, изменение и прекратяване на участието им в наказателния, гражданския, административния и	1.Страни и участници в съдебните производства;	-физическа идентичност – имена, ЕГН, адрес, телефон, имейл. -социална идентичност – данни относно образование, трудова дейност, месторабота, стаж и др. -семейна идентичност – данни относно семейното положение на физическото лице /наличие на брак, развод/ и родствени	Органи на съдебната власт, държавни органи и органи на местното самоуправление /напр. съд, прокуратура, ОД на МВР,	Спазване на законово задължение (чл.6, пар.1, т."в" от ОРЗД) Изпълнение на правомощията на съда при осъществяване на правораздавателната дейност и спазване на законови задължения, произтичащи от нормативните актове: Конституцията на РБ, ГПК, НПК, АПК, ЗСВ, ЗДОИ, ЗЕС,	Органи на съдебната власт; субекта на данните.	Регистратура, деловодства, архив, участниците в съдебния процес.	Технически средства, АИС и мрежи, хартиен носител	Съгласно нормативно установените срокове в Номенклатурата на делата със срокове на съхранение в Районен съд – Кнежа и други нормативни актове.

Дейност	Цел на обработването	Субекти на данните	Категории лични данни	Категории получатели, пред които се разкриват данните	Основание за законосъобразност на обработването	Източник на данните	Местоположение на личните данни	Средства, с които се обработват личните данни	Срок за съхранение на личните данни
	изпълнителния процес; 2.За изготвяне на всякакви документи на лицата в тази връзка(служебни бележки, справки, удостоверения, счетоводни документи.		връзки. -лични данни относно гражданско-правния статус, необходим в хода на съдебния процес /напр. свидетелства и справки за съдимост/. -лични данни, които се отнасят до здравето: данните се съдържат в медицински свидетелства, медицински експертизи, болнични листи, експертни лекарски решения и др. -лични данни, свързани с имотното и финансово състояние на лицата.	РПУ, НАП, НОИ и др./.	ЗЗЛД, КТ, Наредба за вписването, квалификацията и възнагражденията на вещите лица, Наредба за съдебните заседатели, Наредба за съдебните преводачи и др. законови основания. Когато обработването на личните данни е за нуждите на наказателно преследване, основанието за тяхното обработване е чл. 49, вр.чл. 42, ал.1 от Закона за защита на личните данни.				
4.Вещи лица, съдебни заседатели и преводачи	За изготвяне на документи на лицата (служебни бележки, справки, удостоверения, счетоводни документи за изплащане възнагражденията на вещите лица и съдебните заседатели, и др.);	Вещи лица, съдебни заседатели, преводачи	-физическа идентичност – имена, ЕГН, адрес, телефон, имейл. -социална идентичност – данни относно образование, трудова дейност, месторабота, стаж и др. -семейна идентичност – данни относно семейното положение на физическото лице /наличие на брак, развод и родствени връзки.	Органи на съдебната власт, държавни органи и органи на местното самоуправление /напр. съд, прокуратура, ОД на МВР, РПУ, НАП, НОИ и др./.	Спазване на законово задължение. Изпълнение на правомощията на съда при осъществяване на правораздавателната дейност и спазване на законови задължения, произтичащи от нормативните актове: ГПК, НПК, АПК, ЗСВ, Наредба за вписването, квалификацията и възнагражденията на вещите лица. Наредба за съдебните заседатели, Наредба за съдебните преводачи и др. законови основания.	Субекта на данните	Регистратура, деловодства, архив,счетоводство.	Технически средства, АИС и мрежи, хартиен носител	Съгласно нормативно установените срокове в Номенклатурата на делата със срокове на съхранение в Районен съд - Кнежа и други нормативни актове.
5. Лица подаващи молби, жалби, предложения, сигнали и искания	Изпълнение на нормативни изисквания	Лица, сезирали Районен съд Кнежа и неговата администрация с жалби, искове, молби, искания, предложения, сигнали и др.	-физическа идентичност – имена, ЕГН, адрес, телефон, имейл. -социална идентичност – данни относно образование, трудова дейност, месторабота, стаж и др. -други данни, посочени от лицата в подадените от тях жалби, искови молби, молби, искания, предложения, сигнали, както и други, предоставени от органи на съдебната власт, държавни органи и органи на местното самоуправление.	Органи на съдебната власт, държавни органи и органи на местното самоуправление /напр. съд, прокуратура, ОД на МВР, РПУ, НАП, НОИ и др./	Спазване на законово задължение. Изпълнение на правомощията на съда при осъществяване на правораздавателната дейност и спазване на законови задължения, произтичащи от нормативните актове: ГПК, НПК, АПК,	Органи на съдебната власт; субекта на данните, подател на сигнала	Подалите молби, жалби, предложения, сигнали и искания лица.	Технически средства, АИС и мрежи, хартиен носител	Съгласно нормативно установените срокове в Номенклатурата на делата със срокове на съхранение в Районен съд Кнежа и други нормативни актове.
6.Бюро съдимост	За издаване на свидетелства за съдимост, както и справки за	Лица, подали заявления за издаване на	-физическа идентичност – имена, ЕГН, адрес, месторождение.	Органи на съдебната власт (съд,	Спазване на законово задължение (чл.6, пар.1, т."в" от ОРЗД) за изпълнение на	Субекта на данните, органи на	Служител в бюро съдимост, а в негово отсъствие от	Хартиен и технически носител и АИС	Съгласно нормативните изисквания на

Дейност	Цел на обработването	Субекти на данните	Категории лични данни	Категории получатели, пред които се разкриват данните	Основание за законосъобразност на обработването	Източник на данните	Местоположение на личните данни	Средства, с които се обработват личните данни	Срок за съхранение на личните данни
	съдимост за служебни цели.	свидетелства за съдимост	-семейна идентичност - данни относно имена на родители и ЕГН.-социална идентичност - данни относно месторабота и наименование на длъжността -лични данни относно съдебното минало на лицата.	прокуратура, разследващи органи) и други държавни органи и институции само при наличие на законово основание; На физическите лица, за които се отнасят данните	нормативните изисквания на НК, НПК, Наредба № 8 от 26.02.2018 г. за функциите и организацията на дейността на бюрата за съдимост и др.законови основания и индивидуализиране на осъдените лица по вида на наказанията. Когато обработването на личните данни е за нуждите на наказателното преследване, основанието за тяхното обработване е чл. 49, вр.чл. 42, ал.1 от Закона за защита на личните данни.	съдебната власт	заместващите го съдебни служители, определени със заповед на административния ръководител; съдебните деловодители в наказателното деловодство.	и мрежи	Наредба № 8 от 26.02.2018 г. за функциите и организацията на дейността на бюрата за съдимост и Поменклатурата на делата със срокове на съхранение в Районен съд - Кнежа.
7.Контрагенти	Изпълнение на нормативните изисквания на ЗСВ, ЗЗД, ЗОП, Търговски закон и др.; финансово-счетоводна дейност, осигуряване на материално-техническа база на Районен съд Кнежа	Физически лица в изпълнение страни по договор	-физическа идентичност - имена, ЕГН, паспортни данни номер на лична карта, дата и място на издаване , адрес, телефон за връзка, имейл. -социална идентичност данни относно образование, трудова дейност, стаж, професионална биография и др.	Държавни институции - банки, органи на съдебната власт, контролни органи и други органи по закон	Спазване на законово задължение (чл.6, пар 1, т."в" от ОРЗД) Данните се обработват за изпълнение на нормативните изисквания на Закона за задълженията и договорите, Закона за съдебната власт, Закона за обществените поръчки, Търговския закон и др.	Субекта на данните.	Административен секретар, счетоводител	Хартиен и технически носител.	Пет години след прекратяване на договора и извършен одит.
8.Инициативи в Районен съд - Кнежа	Информиране на обществеността за дейността на Районен съд – Кнежа; повишаване квалификацията на студенти от специалност „Право" и други обществено значими цели за развитието на органа на съдебната власт.	Студенти специалност „Право", стажант-юристи, ученици от различни училища, участващи в инициативата „Ден на отворените врати" на Районен съд - Кнежа и лични данни на магистрати, участващи като лектори и наставници в обучения, провеждани от РС Кнежа	-физическа идентичност - имена, ЕГН, адрес, телефон, имейл и др. -социална идентичност данни относно образование, трудова дейност, имена на родители и др.	Държавни органи и институции с оглед изпълнение на нормативно задължение.	Спазване на законово задължение (чл.6, пар.1, т."в" от ОРЗД)	Субекта на данните.	Съдии и съдебни служители - организатори	Хартиен и/или технически носител.	Данните в регистъра се съхраняват за срок от три години.

Приложение № 11

АНАЛИЗ НА РИСКА
ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ
В ДЕЙНОСТА НА РАЙОНЕН СЪД – КНЕЖА

I. Характеристики на обработването на лични данни

1. Особености на администратора на лични данни

Районен съд – Кнежа е администратор на лични данни по смисъла на Регламент (ЕС) 2016/679, на Директива (ЕС) 2016/680 и на Закона за защита на личните данни. Той обработва личните данни законосъобразно, добросъвестно и прозрачно, съгласно чл. 5 и чл. 6 от Регламент (ЕС) 2016/679, чл. 4 от Директива (ЕС) 2016/680 и Закона за защита на личните данни като съблюдава тяхната точност, цялостност и поверителност, с оглед на това същите да бъдат защитени срещу непозволено и/или незаконно обработване, загуба, унищожаване или нарушаване. За тази цел Районен съд – Кнежа е въвел подходящи технически и организационни мерки, за да докаже, че обработването се извършва в съответствие с нормативните актове.

Понятието „*риск*" като дефиниция се определя като възможност за настъпване на вреда за субекта на данни при определени условия, оценена от гледна точка на нейната тежест и вероятност. Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определи с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оцени въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск.

Управлението на риска е систематичен, аналитичен процес, насочен към своевременно отчитане на вероятностите дадена заплаха да въздейства върху администратора на лични данни.

С извършване на настоящия анализ на риска при обработване на личните данни Районен съд – Кнежа в качеството си на администратор на лични данни предприема целенасочени контролирани дейности, чрез които да постигне сигурност на обработваните лични данни. При анализа на риска взема предвид рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни, както и рисковете от настъпване на неблагоприятни материални и нематериални последици в правната сфера на субектите, чиито лични данни се обработват от Районен съд – Кнежа, като отчита, че рисковете за сигурността на личните данни е възможно да настъпят, както в резултат на преднамерени действия, така и поради случайно събитие.

2. Критерии за определяне на рисковете при обработваните регистри с лични данни в Районен съд – Кнежа

В изпълнение на чл. 32, пар. 2 от Регламент (ЕС) 2016/679 се вземат предвид по-специално рисковете, които са свързани с обработването, рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни. При анализа и оценката на риска се отчитат обективни критерии, като:

- **естеството на обработваните лични данни**. От значение е дали обработваните данни са „обикновени“ или специални категории. Обработването на специални категории лични данни се подчинява на специална защита, тъй като рисковете за правата на физическите лица могат да бъдат значителни. Неправомерното им обработване може да накърни конституционно признати и гарантирани права, като например принципа за равенството, свободата на убежденията, неприкосновеността на личността и личния живот. Наред с това обработването и на някои категории „обикновени“ данни може да бъде съпровождано със специфични рискове за физическите лица, например ако нерегламентираният достъп до тях може да доведе до кражба на самоличност, морални или материални вреди.
- **обхват на обработването**. Този критерий се свързва с мащаба на обработваните данни. Обработването на значителен обем лични данни на регионално, национално и наднационално равнище, може да засегне голям брой субекти на данни и те да бъдат възпрепятствани да упражняват своите права Следва да се има предвид динамичния характер на този критерий, доколкото с течение на времето може да варира.
- **контекст на обработването**. Контекстът на обработването и по-специално дали обработването се извършва в трудовия контекст или за статистически цели, или в една или повече от една държава членка на ЕС, или предполага трансфер извън ЕС, има отношение към специфични рискове, които съпътстват правата на физическите лица при обработване на личните им данни.
- **цели на обработването**. При анализа на риска се имат предвид не само целите, за които първоначално се събират личните данни, но и последващите съвместими цели, за които данните могат да бъдат използвани, напр. за научни или статистически цели.

3. Последици за субектите на данни от загуба на наличност, цялостност и поверителност.

Преценката им е в изпълнение на чл. 32, пар. 2 от Регламент (ЕС) 2016/679 да се отчитат по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни. В случая последиците може да повлияят върху неприкосновеността на личния живот, правото на труд в аспекта право на трудово възнаграждение, почивки и отпуски, правото на здравно и обществено осигуряване, контрола върху личните данни, добрата репутация, финансовата сигурност, псевдонимизацията, да доведат до дискриминация, да нарушат опазването на самоличността, до заплаха за сигурността за живота и здравето на субектите на данни и на близките им.

II. Идентифициране на рисковите фактори за правата и свободите на субектите на данни

1. Определяне на вероятността от настъпване на заплаха, която може да въздейства неблагоприятно върху защитата на личните данни

1.1. Критерии за оценка на риска

Като се отчита понятието „риск“ по смисъла на § 1, т. 16 от Допълнителните разпоредби на Закона за защита на личните данни, за оценката на риска се използват два

критерия – Вероятност за поява (Вп) и Въздействие (Вз) на събитието, което може да породи материални или нематериални вреди за субектите на данни. Всеки от критериите се оценява с точки по възходящ ред от 1 до 5, като 5 е най-високата стойност.

Степени на вероятност от настъпването на събитието:

1- неправдоподобно да се случи

2- малка вероятност да се случи

3- умерена вероятност да се случи

4- голяма вероятност да се случи

5- почти сигурно е, че ще се случи

Степени на въздействие, в случай, че събитието възникне:

1- пренебрежимо ниско въздействие

2- незначително въздействие

3- умерено въздействие

4- голямо въздействие

5- сериозно въздействие с важни последици

Критериите се групират в следната матрица за измерване на нивото на риска:

Вероятност за поява (Вп)					
5- почти сигурно	5	10	15	20	25
4- голяма вероятност	4	8	12	16	20
3- умерена вероятност	3	6	9	12	15
2- малка вероятност	2	4	6	8	10
1- неправдоподобно	1	2	3	4	5
Въздействие (Вз)	**1- пренебрежимо ниско въздействие**	**2- незначително въздействие**	**3-умерено въздействие**	**4-голямо въздействие**	**5-сериозно въздействие с важни последици**

1.2. Оценяване на риска

Рискът се изчислява като произведение на стойностите на двата критерия и във връзка с цялостност, достъпност, наличност и конфиденциалност на информацията в дейността на институцията.

ИР (изчислен риск) = Вп х Вз

Изчисленият риск може да има следните стойности – 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 20 и 25.

Всеки риск се оценява (класифицира) спрямо позицията си по матрицата, по следните критерии:

- Рисковете, попадащи в зелената скала (със стойности между 1 и 4), се определят като „ниски“;

- Рисковете, попадащи в синята скала (със стойности 5), се определят като „приемливи“;

- Рисковете, попадащи в жълтата скала (със стойности между 6 и 10), се определят като „средни“;

- Рисковете, попадащи в червената скала (със стойности между 12 и 25), се определят като „високи“.

2. Тежестта на последиците за субектите на данни се определя съобразно т. 8 от Методологията за оценка на тежестта за пробив в сигурността на личните данни (Приложение 10 от Вътрешните правила за защита на личните данни в Районен съд – Кнежа), а именно:

Извършва се следното приравняване на изчисления риск към нивото на риск и възможните последици

Ниво на риск	Приравняване	Възможни последици
Нисък риск	РИСК < 2	субектите на данни е възможно да изпитат няколко незначителни неудобства, които ще преодолеят без никакъв проблем (време, прекарано в повторно въвеждане на информация, раздразнение, объркване и т.н.)
Среден риск	2 < РИСК < 3	субектите на данни е възможно да изпитат значителни неудобства, които те ще могат да преодолеят въпреки някои трудности (допълнителни разходи, отказ от достъп до услуги, страх, липса на разбиране, стрес, дребни физически неразположения и т.н.)
Висок риск	3 <РИСК	субектите на данни е възможно да изпитат значителни последствия, които биха преодолели, макар и със сериозни трудности или необратими последици, които не могат да преодолеят (злоупотреби с финансови средства, черни списъци от финансови институции, имуществени щети, загуба на работа, влошаване на здравето, неработоспособност, дългосрочни психологически или физически заболявания, подлагане на дискриминация, смърт.

Действия, които се предприемат с оглед на риска:

- Рисковете с оценка „ниски“ се считат да приемливи. Те подлежат на мониторинг с цел да не се повиши тяхната оценка и при възможност да се избегне вероятността от възникването и въздействието им.
- Рисковете с оценка „средни“ се считат за потенциално опасни. Върху тях се прилагат мерки с цел понижаване на стойностите им до степен „ниска“, когато е възможно и ефективно.

- Рисковете с оценка „високи“ се считат за критични. Те се обработват приоритетно, като се преглежда и възможността за разпределянето им с трети страни, например застрахователи.

III. Технически и организационни мерки за защита на данните

1. **Физическата защита** на личните данни се осъществява при спазване на следните мерки:

- Районен съд – Кнежа се помещава в Съдебната палата, която е с контролиран достъп на външни лица.
- Сградата е оборудвана с пожароизвестителна система, разполага и с пожарогасители.
- Личните данни се обработват в кабинетите на лицата, в чиито длъжностни характеристики е определено задължението за обработване на данни от определени регистри.
- Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове в кабинетите на упълномощените лица.
- Помещенията, в които се обработват лични данни, се заключват.
- Елементите на комуникационно-информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.
- Външни лица имат достъп до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

2. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

- Лицата, обработващи лични данни, се запознават с Общия регламент за защита на данните, Закона за защита на личните данни, настоящите Вътрешни правила, както и с други нормативни актове, относими към съответната дейност по обработване.
- Лицата, обработващи лични данни, се запознават с опасностите за личните данни, обработвани от администратора.

3. Документалната защита на личните данни се осъществява при спазване на следните мерки:

- Регистрите с лични данни, обработвани от Районен съд – Кнежа, се поддържат на хартиен или електронен носител.
- Обработването на личните данни се извършва в рамките на работното време на Районен съд – Кнежа. Обработването на лични данни, свързани със съдебното производство, е допустимо и след края на работното време, както и в неработни дни, в случай, че съдебните заседания се провеждат по това време.
- Достъп до регистрите с лични данни, обработвани от Районен съд – Кнежа, имат само служители, в чиито длъжностни характеристики е определено задължение за обработване на данните, или на които е поставена конкретна задача.
- Личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания към Районен съд – Кнежа.

- Сроковете за съхранение на личните данни от различните регистри са определени в Правилника за администрацията в съдилищата, Номенклатура на делата със срокове за съхранение в Районен съд – Кнежа.
- Личните данни на хартиен носител се съхраняват в определените за целта служебни помещения в Съдебната палата.
- Архивирането на лични данни на хартиен носител се осъществява в съответствие с Вътрешните правила за архивиране на делата в Районен съд – Кнежа.
- Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители, само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от държавни органи или упълномощени лица.
- Временните документи, копия от документи и работни материали от регистрите, които са на хартиен носител и съдържат лични данни, се унищожават чрез машини за унищожаване на документи (шредер).
- След изтичане на срока за съхранение документите от регистрите същите се унищожават. Унищожението се извършва посредством възлагане на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

4. Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

- При работа с данните от регистрите, поддържани от Районен съд – Кнежа, се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър. В автоматизираните информационни системи за обработка на съдебни дела, се поддържа системен журнал за извършените действия от потребителя.
- В съдебните зали - на работното място на съдебните секретари - се използват индивидуални потребителски имена и пароли за достъп за всеки съдебен секретар.
- Когато информацията е класифицирана по смисъла на ЗЗКИ, помещението, в което се съхраняват информационните носители се заключва и охранява със сигналноохранителна техника, като се използва и списък на оторизираните лица съгласно нормативните изисквания.
- Системният администратор създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.
- За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

- Помещенията, в които са разположени компютърни и комуникационни средства, се заключват. Осигурена е система за ограничаване на достъпа и сигнално-охранителна система.

5. Организационни мерки за гарантиране нивото на сигурност:

- а) Охраната на сградата в Районен съд-Кнежа е целодневна и непрекъсната в рамките на работното време и се осъществява от ОЗ „Охрана“-Плевен, към Главна дирекция „Охрана“ към Министерство на правосъдието;
- б) Забранено е използването на преносими лични носители на данни за съхранение или копиране на документи, попадащи в обхвата на настоящите правила.
- в) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.
- г) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

6. Електронните регистри, съдържащи лични данни, се обработват и съхраняват чрез съответните специализирани софтуерни продукти както следва:

а) за Управление на съдебните дела - Софтуерен продукт „САС – Съдебно деловодство“, създаден и поддържан от „Информационно обслужване“ – Варна и Единна информационна система на съдилищата – от „Информационно обслужване“ АД. С тези продукти се съхраняват и обработват данните за участниците в съдебния процес. Базата данни се намира и съхранява в специализиран сървър на Районен съд – Кнежа под управлението на операционна система Microsoft Server със съответните правила за защита от нерегламентиран достъп и създаване на резервни копия. Достъпът до модулите на продукта се извършват чрез индивидуални потребителски имена и пароли за оторизираните за работа с него лица.

б) За управление на изпълнителните дела в служба „Държавен съдебен изпълнител“ е създаден и внедрен ПП „JES“, създаден и поддържан от доц. Еди Чакъров. С този софтуерен продукт се съхраняват и обработват данните на участниците в изпълнителния процес, по изпълнителни дела. Базата данни се намира и съхранява в специализиран сървър на Районен съд – Кнежа под управлението на операционна система Microsoft Server със съответните правила за защита от нерегламентиран достъп и създаване на резервни копия. Достъпът до модулите на продукта се извършват чрез индивидуални потребителски имена и пароли за оторизираните за работа с него лица.

б) за служба счетоводно отчитане:

- Софтуерен продукт „Омекс“ – съхранява и обработва данните за магистрати, съдии и служители, съдебни заседатели, вещи лица, както и модул за разплащане. Базата данни се намира и съхранява на компютър на Районен съд – Кнежа със съответните правила за защита от нерегламентиран достъп и създаване на резервни копия. Достъпът до модулите на продукта се извършват чрез индивидуални потребителски имена и пароли за оторизираните за работа с него лица.

- Софтуерен продукт „Конто“- съхранява и обработва данните за магистрати, и съдебни служители, в който се въвеждат данни относно изплащане на възнагражденията на магистрати, съдии и служители. ПП е достъпен онлайн и не е базиран на сървър на Районен съд-Кнежа.

б) за служба „Бюро съдимост“:

- Софтуерен продукт АИС “Съдебен статус“- съхранява и обработва данни за физически лица относно съдебното им минало в служба „Бюро съдимост“ в Районен съд – Кнежа. ПП е достъпен онлайн и не е базиран на сървър на Районен съд-Кнежа.

Комуникацията с Единната деловодна система на съдилищата се осъществява по защитена VPN връзка.

3. Анализ на риска при обработването на лични данни в Районен съд – Кнежа

3.1. За регистър „Персонал- магистрати, съдии и съдебни служители“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни (за физическа, социална, семейна и икономическа идентичност), сведени до минимум с оглед защитата на личните данни и изискванията на трудовото законодателство. За изпълнение на специфичните задължения на Районен съд - Кнежа като работодател се обработват и специални категории лични данни (за здравословното състояние). В регистъра в определени от Кодекса на труда случаи се обработват и данни за присъди и нарушения.

Обхват на обработването: Обработването обхваща лични данни на работещите в Районен съд – Кнежа, свързани с физическа и социална идентичност (данни относно образование и трудова дейност, стаж, семейното положение; данни относно банкови сметки – за изплащане на трудово възнаграждение; лични данни относно съдебното минало на лицата;

Контекст на обработването: Обработването се осъществява изцяло в трудовия контекст при отчитане на чл. 88 от Регламент (ЕС) 2016/679 и българското законодателство. Обработването не предполага предаване на лични данни в трети държави (извън ЕС), освен ако данните не са необходими за целите на командироването и Наредбата за условията и реда за издаване на визи и определяне на визовия режим.

Цел на обработването: управление на човешките ресурси, изпълнение на нормативни задължения и финансово-счетоводна отчетност.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Засягане на следните основни права на субектите на данни: неприкосновеност на личния живот, незаконна намеса в семейния живот, правото на труд в аспекта право на трудово възнаграждение, почивки и отпуски, право на здравно осигуряване и право на обществено осигуряване. Наличието на специални категории лични данни е обстоятелство, което се отчита като увеличаващо обичайно съществуващия риск.

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и

поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, се определя като умерена. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 2 х 3 = 6

Обобщение за регистър „Персонал-магистрати, съдии и съдебни служители“:

Рискът от обработването на лични данни в регистър „Персонал-магистрати, съдии и съдебни служители“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и конкретно наличието на специални категории лични данни в регистъра, както и специфичния трудов контекст, в който се осъществява обработването.

3.2. За регистър „Кандидати за съдебни служители“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни (за физическа, социална, семейна и икономическа идентичност), сведени до минимум с оглед защитата на личните данни и изискванията на трудовото законодателство. Обхващат се и специални категории лични данни (за здравословното и психическото състояние) за изпълнение на специфичните задължения на институцията като работодател, респ. права на служителите, произтичащи от трудовото и осигурителното законодателство. В регистъра в определени от Кодекса на труда случаи се обработват и данни за присъди и нарушения.

Обхват на обработването: Обработването обхваща лични данни на кандидатите за съдебни служители в Районен съд – Кнежа, свързани с физическа и социална идентичност - данни относно образование, трудова дейност, стаж, както и относно съдебното минало на лицата. Обработват се и специални категории лични данни, свързани със здравословното състояние на кандидатите

Контекст на обработването: Обработването се осъществява изцяло в трудовия контекст при отчитане на чл. 88 от Регламент (ЕС) 2016/679 и българското законодателство. Обработването не предполага предаване на лични данни в трети държави (извън ЕС).

Цел на обработването: управление на човешките ресурси – подбор на персонал, изпълнение на нормативни задължения.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Засягане на следните основни права на субектите на данни: неприкосновеност на личния и семейния живот. Наличието на специални категории лични данни е обстоятелство, което се отчита като увеличаващо обичайно съществуващия риск.

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като умерена. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, се определя като умерена. Изчисленият риск има стойността на произведението на

възможността за поява и въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 3 х 3 = 9

Обобщение за регистър „Кандидати за съдебни служители“:

Рискът от обработването на лични данни в регистър „Кандидати за съдебни служители“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и конкретно наличието на специални категории лични данни в регистъра, както и специфичния трудов контекст, в който се осъществява обработването

3.3 За регистър „Съдебни дела, страни в съдебни производства“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни, свързани с физическа, социална, семейна и икономическа идентичност, както и *„специални“* лични данни относно присъди и нарушения на участниците в граждански или в наказателен съдебен процес, тяхното здравословно и психическо състояние.

Обхват на обработването: Обработването обхваща лични данни на участниците в съдебен процес, свързани с физическа и социална идентичност - данни относно образование, трудова дейност, стаж, съдебното минало на лицата, здравословното им състояние.

Контекст на обработването: Обработването се осъществява изцяло в контекста на целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване (Директива (ЕС) 2016/680 и българското законодателство. Предаване на лични данни на трети държави или международни организации става при прилагане на глава V от Директива /ЕС/2016/680 относно защитата на физическите лица във връзка с обработването на личните данни и относно свободното движение на такива данни.

Цел на обработването: Правораздавателна дейност.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: загуба на контрол върху личните данни или ограничаване на правата, накърняване на репутацията, финансови загуби, неразрешено премахване на псевдонимизацията, дискриминация, кражба на самоличност или измама с фалшива самоличност, нарушена неприкосновеност на личния и семейния живот, заплаха за живота и здравето на субектите на данни и на близките им.

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, но и евентуалните последици за субектите на лични данни, се определя като сериозна. Изчисленият риск има стойността на произведението на възможността за поява и

въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 2 х 5 = 10

Обобщение за регистър „Съдебни дела,страни в съдебни производства“:

Рискът от обработването на лични данни в регистър „Съдебни дела, страни в съдебни производства“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и най-вече възможните последици за субектите на лични данни.

3.4 За регистър „Вещи лица, съдебни заседатели и преводачи“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни, свързани с физическа, социална, семейна и икономическа идентичност, както и *„специални“* лични данни относно присъди и нарушения на вещи лица, преводачи и съдебни заседатели, тяхното здравословно и психическо състояние.

Обхват на обработването: Обработването обхваща лични данни, свързани с физическа и социална идентичност - данни относно образование, трудова дейност, стаж, съдебното минало на лицата, здравословното им състояние.

Контекст на обработването: Обработването се осъществява изцяло в контекста на целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване (Директива (ЕС) 2016/680 и българското законодателство. Предаване на лични данни на трети държави или международни организации става при прилагане на глава V от Директива /ЕС/2016/680 относно защитата на физическите лица във връзка с обработването на личните данни и относно свободното движение на такива данни.

Цел на обработването: Правораздавателна дейност.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: загуба на контрол върху личните данни или ограничаване на правата, накърняване на репутацията, финансови загуби, кражба на самоличност или измама с фалшива самоличност, нарушена неприкосновеност на личния и семейния живот, заплаха за живота и здравето на субектите на данни и на близките им.

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, но и евентуалните последици за субектите на лични данни, се определя като голяма. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 2 х 4 = 8

Обобщение за регистър „Вещи лица, съдебни заседатели и преводачи “:

Рискът от обработването на лични данни в регистър „Вещи лица, съдебни заседатели и преводачи“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и най-вече възможните последици за субектите на лични данни.

3.5 За регистър „Лица, подаващи молби, жалби, предложения, сигнали и искания“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни за физическа, социална и семейна идентичност, сведени до минимум с оглед защитата на личните данни, както и специални категории лични данни (за здравословното и психическото състояние) за изпълнение на специфичните задължения на институцията.

Обхват на обработването: Обработването обхваща лични данни на подалите молби, жалби, предложения, сигнали и искания, свързани с физическа и социална идентичност – имена, адрес, месторабота или пенсионен статус, здравословно състояние и др. в зависимост от съдържанието на жалбата, искането и т.н.

Контекст на обработването: Обработването се осъществява в контекста на изпълнение на функциите на институцията, както и за обратна връзка със субектите на данни.

Цел на обработването: Изпълнение на нормативните изисквания.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: загуба на контрол върху личните данни или ограничаване на правата, накърняване на репутацията, финансови загуби, кражба на самоличност или измама с фалшива самоличност, нарушена неприкосновеност на личния и семейния живот, заплаха за живота и здравето на субектите на данни и на близките им

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, се определя като умерена. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 2 х 3 = 6

Обобщение за регистър „Лица, подаващи молби, жалби, предложения, сигнали и искания“:

Рискът от обработването на лични данни в регистър „Лица, подаващи молби, жалби, предложения, сигнали и искания“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и конкретно наличието на специални категории лични данни в регистъра.

3.7 За регистър „Бюро съдимост“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни за физическа и социална идентичност, както и лични данни, свързани с присъди и нарушения – съгласно член 10 от Регламент (ЕС) 2016/679.

Обхват на обработването: Обработването обхваща лични данни на подалите молби за издаване на свидетелства и справки за съдимост, свързани с физическа и социална идентичност – имена, адрес, родствени връзки и др.

Контекст на обработването: Обработването се осъществява в контекста на изпълнение на функциите на институцията, както и за обратна връзка със субектите на данни.

Цел на обработването: Изпълнение на нормативните изисквания.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: загуба на контрол върху личните данни или ограничаване на правата, накърняване на репутацията, финансови загуби, кражба на самоличност или измама с фалшива самоличност, нарушена неприкосновеност на личния и семейния живот

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, се определя като умерена. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска: ИР= Вп х Вз= 2 х 3 = 6

Обобщение за регистър „Бюро съдимост“:

Рискът от обработването на лични данни в регистър „Бюро съдимост“ попада в жълтата скала, определя се като **„среден“** и се счита за потенциално опасен, като изисква прилагане на подходящи технически и организационни мерки. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и конкретно наличието на специални категории лични данни в регистъра.

3.8 За регистър „Контрагенти“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни (за физическа, социална и икономическа идентичност), сведени до минимум с оглед защитата на личните данни и изискванията на законодателството в областта на търговските взаимоотношения.

Обхват на обработването: Обработването обхваща лични данни на физически лица, които представляват юридически лица, с които Районен съд – Кнежа е страна по договор и се използват само за целите на договорните му задължения.

Контекст на обработването: Обработването се осъществява изцяло в контекста на договорните отношения на Районен съд – Кнежа при отчитане на чл. 86 от Регламент (ЕС) 2016/679 и българското законодателство. Обработването не предполага предаване на лични данни в трети държави (извън ЕС).

Цел на обработването: Изпълнение на нормативни задължения, управление на човешките ресурси, финансово счетоводна дейност, осигуряване на материално-техническата база на Районен съд – Кнежа.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: кражба на самоличност, финансови загуби, засягане правото на труд, накърняване на репутацията

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, също се определя като малка. Изчисленият риск, изразен с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска, е: ИР= Вп х Вз= 2 х 2 = 4

Обобщение за регистър „Контрагенти“:

Рискът от обработването на лични данни в регистър „Контрагенти“ попада в зелената скала, определя се като **„нисък“** и се счита за приемлив. Обработването подлежи на мониторинг с цел да не се повиши оценката на риска - да се избегне вероятността от възникване и реализиране на вредни последици за субектите на лични данни.

3.8 За регистър „Инициативи в Районен съд – Кнежа“

Естество на обработваните лични данни: В регистъра се обработват *„обикновени“* лични данни за физическа и социална, сведени до минимум с оглед защитата на личните данни

Обхват на обработването: Обработването обхваща лични данни ученици, магистрати, съдебни служители и други участници наставници в инициативи на Районен съд – Кнежа

Контекст на обработването: Обработването се осъществява за реализирането на инициативи на Районен съд – Кнежа.

Цел на обработването: Изпълнение на образователни програми и програми за информиране на обществеността за дейността на съда

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: кражба на самоличност, накърняване на репутацията

Оценяване на риска: Предвид взетите от администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност, цялостност и поверителност, се определя като малка. Степента на въздействие, предвид свеждането на данните до минимум и изпълнение на нормативни изисквания при обработването, също се определя като малка. Изчисленият риск, изразен с показателите по методиката в раздел II, т. 1 от настоящия анализ на риска, е: ИР= Вп х Вз= 2 х 2 = 4

Обобщение за регистър „Инициативи в Районен съд – Кнежа“:

Рискът от обработването на лични данни в регистър „Инициативи в Районен съд-Кнежа“ попада в зелената скала, определя се като **„нисък“** и се счита за приемлив. Обработването подлежи на мониторинг с цел да не се повиши оценката на риска - да се

избегне вероятността от възникване и реализиране на вредни последици за субектите на лични данни.

4. Технически и организационни мерки за защита на личните данни за средно ниво на риска, въведени в Районен съд – Кнежа

4.1. Физическа защита

Организационни и технически мерки	***Описание***
Определяне на помещенията за обработване на лични данни и за разполагане на елементите на комуникационните и информационните системи	
Определяне на организация на физическия достъп	Служебни/лични карти
Определяне на използваните технически средства за физическа защита	Заключване на помещенията, сигнално-охранителна техника
Определяне на използваните технически средства за защита	Ключалки; шкафове; пожарогасителни средства; оборудване на помещенията
Определяне на зоните с контролиран достъп	Цялостно за служебните помещения

4.2. Персонална защита

Организационни мерки	***Описание***
Познаване на нормативната уредба в областта на защитата на личните данни	Организиране на обучения в областта на защитата на личните данни за служителите и запознаване на новопостъпили служители с вътрешни правила, процедури и политики
Знания за опасностите за защита на личните данни, обработвани от администратора	Периодични напомняния за рисковете при обработването на лични данни
Поемане на задължение за неразпространение на лични данни	Подписване на декларации или задължения по длъжностни характеристики на служителите, които имат достъп до лични данни при или по повод изпълнение на техните задълженията
Ограничения за споделяне на критична информация между персонала	Предвиждане на такива ограничения в мерките за постигане на информационна сигурност
Познаване на политиката, процедурите и други изисквания, свързани със защитата на личните данни	Разглежда се като постоянен процес
Тренировка на персонала за реакция при събития, застрашаващи сигурността на личните данни	Организиране на тренировки по преценка на ръководството

4.3. Документална защита

Организационни мерки	*Описание*
Определяне на регистрите, които ще се поддържат на хартиен носител	Във вътрешни правила и инструкции на администратора
Определяне на условията за обработване на лични данни	Във вътрешни правила и инструкции на администратора
Регламентиране на достъпа до регистрите с лични данни	Във вътрешни правила на администратора
Контрол на достъпа до регистрите	Във вътрешни правила на администратора
Определяне на срокове за съхранение	Номенклатура на делата със срокове за съхраняване
Процедури за унищожаване	Във вътрешни правила на администратора, в Правилника за администрация на съдилищата

4.4. Защита на комуникационните и информационни системи

Организационни и технически мерки	*Описание*
Персонална защита	Обучение на персонала за изискванията при работа с комуникационните и информационните системи
Идентификация и автентификация	Използване на потребителски имена, пароли и устройства за достъп (вкл. КЕП)
Външни връзки/свързване	Използване на сигурни протоколи
Защита от вируси	Периодично обновяване на антивирусните дефиниции
Копия/резервни копия за възстановяване	Периодично създаване на копия
Защита на носители на информация	Регулиране на употребата на преносими носители; защита на информационните системи
Телекомуникации и отдалечен достъп	Използване на сигурни протоколи
Поддържане/ експлоатация	Регулярно наблюдение от служители на администратора

4.5. Криптографска защита

Технически мерки	*Описание*
Стандартни криптографски възможности на операционните системи и комуникационното оборудване	Според оборудването
Използване на нормативно определени системи за електронен подпис	Съгласно действащата нормативна уредба

5. Оценяване на остатъчния риск

След действията за овладяване и/или въздействие върху риска, се определят степените на нова вероятност (НВр) и ново въздействие (НВз) за всеки от регистрите с лични данни по следната скала:

Определяне на НВр		Определяне на НВз	
Стойност	Примерна нова вероятност за поява след въздействието	Стойност	Описание, примерно ново въздействие
0	Без изменение, новата вероятност не се влияе от приложеното действие	0	Без изменение, новата вероятност не се влияе от приложеното действие
1	Рискът е нов, няма натрупан опит в управлението му, вероятността за поява е намалена малко	1	Рискът е нов, няма натрупан опит в управлението му, въздействието е намалено малко
2	Рискът се управлява, вероятността за поява е намалена реално	2	Рискът се управлява, въздействието е намалено реално
3	Рискът се управлява, вероятността за поява е намалена решително	3	Рискът се управлява, въздействието е намалено решително

6.1. За регистър „Персонал- магистрати, съдии и съдебни служители“

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=6-(2х2)=2

Остатъчният риск съществува, но се оценява като **нисък**, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

6.2. За регистър „ Кандидати за съдебни служители“

Нова вероятност – стойност 2, Ново въздействие – стойност 3. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=9-(2х3)=3

Остатъчният риск съществува, но се оценява като **нисък**, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

6.3 За регистър „Съдебни дела, страни в съдебни производства“

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=5-(2х4)= 1 (-3)

Остатъчният риск е минимален, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

6.4 За регистър „Вещи лица, съдебни заседатели и преводачи“

Нова вероятност – стойност 2, Ново въздействие – стойност 3. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=8-(2х3)=2

Остатъчният риск съществува, но се оценява като нисък, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

6.5 За регистър „Лица, подаващи молби, жалби, предложения, сигнали и искания“

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=6-(2х2)=2

Остатъчният риск съществува, но се оценява като нисък, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

***6.6* За регистър „Бюро съдимост“**

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=6-(2х2)=2

Остатъчният риск съществува, но се оценява като нисък, поради което идентифицираните технически и организационни мерки подлежат на мониторинг.

6.7 За регистър „Контрагенти“

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=4-(2х2)=0

Остатъчен риск няма.

6.8 За регистър „ Инициативи в Районен съд – Кнежа“

Нова вероятност – стойност 2, Ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: ОР=ИР-(НВзхНВр)=4-(2х2)=0

Остатъчен риск няма.

7. Преразглеждане на нивото на риска и мерките за защита

Оценката на риска, а в зависимост от нея и мерките за защита, се преразглеждат периодично най-малко веднъж на две години или при промяна в някой от критериите, при които е определен.

Следващ редовен преглед на нивото на риска ще бъде извършен не по-рано от 2027 г., освен ако няма промени в естеството, обхвата, контекста и целта на обработването, както и в използваната технология за обработване.

Подпис: .....