



РЕПУБЛИКА БЪЛГАРИЯ
ВЪРХОВЕН
КАСАЦИОНЕН
СЪД

УТВЪРЖДАВАМ: _____

ГАЛИНА ЗАХАРОВА
ПРЕДСЕДАТЕЛ НА
ВЪРХОВНИЯ КАСАЦИОНЕН СЪД
(заповед: ... 808 / 30.08.2023 г.)

АНАЛИЗ НА РИСКА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ В ДЕЙНОСТА НА ВЪРХОВНИЯ КАСАЦИОНЕН СЪД

1. Методика за извършване на анализа на риска във Върховния касационен съд

1.1. Критерии за оценка на риска

Като 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:

- 1) Вероятност за поява (Вп) и
- 2) 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 дружеството.

$$\text{ИР (изчислен риск)} = \text{Вп} * \text{Вз}$$

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) и синята скала (със стойност 5), се определят като „ниски“;
- 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“.

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. Мерките за защита се ориентират приоритетно към тях.

1.3. Определяне на остатъчния риск

След действията за овладяване и/или въздействие върху риска, се определят степените на ново въздействие (НВз) и нова вероятност (НВр).

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

Остатъчният риск (ОР) се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност: $ОР = ИР - (НВз * НВр)$.

2. Идентифициране на рисковите фактори за защитата на личните данни в контекста на Регламент (ЕС) 2016/679 и Закона за защита на личните данни

В изпълнение на чл. 32, пар. 2 от Регламент (ЕС) 2016/679 се вземат предвид рисковете, които са свързани с обработването, по-специално 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. Обработването и на някои категории „обикновени“ данни може да бъде съпроводено 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. Отчита се динамичният характер на този критерий, доколкото с течение на времето обхватът на обработването може да варира.

- **контекст на обработването.** Контекстът на обработването и по-специално дали обработването се извършва в трудовия контекст, за архивиране в обществен интерес, за статистически цели или научни изследвания, 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.

- **целта на обработването.** При анализа на риска трябва да 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, например за научни или статистически цели.

- **последниците за субектите на данни от загуба на наличност, цялостност и поверителност на личните данни.** 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.

3. Анализ на риска при обработването на лични данни във Върховния касационен съд

3.1. Регистър „Граждански дела“

Естество на обработваните лични данни: Лични данни, свързани с физическата идентичност, икономическата идентичност, социална идентичност, семейна идентичност, данни за съдебното минало, данни относно здравословното състояние, в зависимост от предмета на съответното дело. Личните данни се

диференцират и според ролята на субектите на данни в съответното производство – страни, свидетели, вещи лица, тълковници, преводачи.

Обхват на обработването: Анализът е извършен на база преценка за броя на делата за последните две години. Въпреки високата натовареност на съда, дейността му като върховна инстанция обуславя факта, че съхранението на делата след тяхното приключване не се осъществява в неговата структура, а в първоинстанционния съд. Поради това броят на делата за съответната година е условен ориентир за обхвата на обработването за целите на правораздаването по граждански дела.

Контекст на обработването: Обработването се осъществява при условията на стриктна нормативна уредба за дейността на съдилищата, произтичаща от Конституцията, Гражданския процесуален кодекс, Закона за съдебната власт, Правилника за администрацията на ВКС, Наредба № 4 от 16.03.2017 г. за воденето, съхраняването и достъпа до регистъра на актовете на съдилищата и други. Ако произтича от задължения, поети с международни договори, обработването на лични данни може да включва предаване в трети държави или международни организации, при спазване на другите изисквания на Регламент (ЕС) 2016/679 и при наличие на решение за адекватност на Европейската комисия по чл. 45 от Регламент (ЕС) 2016/679 или подходяща гаранция по чл. 46, пар. 2, б. „а“ от Регламент (ЕС) 2016/679 (инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури).

Цел на обработването: Защита на правата и законните интереси на гражданите, юридическите лица и държавата и в рамките на тази цел личните данни се използват за изпращане на призовки, съдебни книжа и друга кореспонденция, свързана с входящи и изходящи документи по повод движението и обработването на съдебните дела. Като съвместими с тази цел на обработването, по силата на нормативни задължения данните се използват за целите на архивирането в обществен интерес, статистически цели и научни изследвания.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид съчетаването на данните от съдебните дела на хартиен и електронен носител, вероятността от загуба на наличност и цялостност не е голяма. Освен това в чл. 71 от Правилника за администрацията на ВКС се съдържат правила за възстановяване на изгубено или унищожено дело. Предвидено е възстановяване на делото, а ако това не е възможно, делото може да бъде заведено повторно, без да се събират отново държавни такси. Поради това рискът от загуба на наличност и цялостност се определя като нисък.

Рискът от загуба на поверителност, поради възможното наличие на специални категории лични данни в някои от делата, а и поради високия материален интерес на делата и без наличие на специални категории лични данни, определя по-сериозно въздействие върху страните, поради което не се квалифицира като нисък, а като среден, заради естеството на данните.

Оценяване на риска: Предвид взетите в администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност и цялостност, се определя като малка, но по отношение на загубата на поверителност се допуска умерена вероятност да се случи. 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 т. 1 от настоящия анализ на риска: $ИР = Вп * Вз = 3 * 3 = 9$.

Обобщение за регистър „Граждански дела“:

Рискът от обработването на лични данни в регистър „Граждански дела“ 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 материалният интерес по делата.

3.2. Регистър „Търговски дела“

Естество на обработваните лични данни: Лични данни, свързани с физическата идентичност, икономическата идентичност, социална идентичност, семейна идентичност, данни за съдебното минало, данни относно здравословното състояние, в зависимост от предмета на съответното дело. Личните данни се диференцират и според ролята на субектите на данни в съответното производство – страни, свидетели, вещи лица, тълковници, преводачи.

Обхват на обработването: Анализът е извършен на база преценка за броя на делата за последните две години. Въпреки високата натовареност на съда, дейността му като върховна инстанция обуславя факта, че съхранението на делата след тяхното приключване не се осъществява в неговата структура, а в първоинстанционния съд. Поради това броят на делата за съответната година е условен ориентир за обхвата на обработването за целите на правораздаването по търговски дела.

Контекст на обработването: Обработването се осъществява при условията на стриктна нормативна уредба за дейността на съдилищата, произтичаща от Конституцията, Гражданския процесуален кодекс, Закона за съдебната власт, Правилника за администрацията на ВКС, Наредба № 4 от 16.03.2017 г. за воденето, съхраняването и достъпа до регистъра на актовете на съдилищата и други. Ако произтича от задължения, поети с международни договори, обработването на лични данни може да включва предаване в трети държави или международни организации, при спазване на другите изисквания на Регламент (ЕС) 2016/679 и при наличие на решение за адекватност на Европейската комисия по чл. 45 от Регламент (ЕС) 2016/679 или подходяща гаранция по чл. 46, пар. 2, б. „а“ от Регламент (ЕС) 2016/679 (инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури).

Цел на обработването: Защита на правата и законните интереси на гражданите, юридическите лица и държавата и в рамките на тази цел личните данни се използват за изпращане на призовки, съдебни книжа и друга кореспонденция, свързана с входящи и изходящи документи по повод движението и обработването на съдебните дела. Като съвместими с тази цел на обработването, по силата на нормативни задължения данните се използват за целите на архивирането в обществен интерес, статистически цели и научни изследвания.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид съчетаването на данните от съдебните дела на хартиен и електронен носител, вероятността от загуба на наличност и цялостност не е голяма. Освен това в чл. 71 от Правилника за администрацията на ВКС се съдържат правила за възстановяване на изгубено или унищожено дело. Предвидено е възстановяване на делото, а ако това не е възможно, делото може да бъде заведено повторно, без да се събират отново държавни такси. Поради това рискът от загуба на наличност и цялостност се определя като нисък.

Рискът от загуба на поверителност, поради възможното наличие на специални категории лични данни в някои от делата, а и поради високия материален интерес на делата и без наличие на специални категории лични данни, определя по-сериозно въздействие върху страните, поради което не се квалифицира като нисък, а като среден, заради естеството на данните.

Оценяване на риска: Предвид взетите в администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност и цялостност, се определя като малка, но по отношение на загубата на поверителност се допуска

умерена вероятност да се случи. 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 т. 1 от настоящия анализ на риска: $IP = V_p * V_z = 3 * 3 = 9$.

Обобщение за регистър „Търговски дела“:

Рискът от обработването на лични данни в регистър „Търговски дела“ 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 материалният интерес по делата.

3.3. Регистър „Наказателни дела“

Естество на обработваните лични данни: Лични данни, свързани с физическата идентичност, икономическата идентичност, социална идентичност, семейна идентичност, данни за съдебното минало, данни относно здравословното състояние, в зависимост от предмета на съответното дело. Личните данни се диференцират и според процесуалното качество субектите на данни в наказателното производство и признаците от състава на съответното престъпление.

Обхват на обработването: Анализът е извършен на база преценка за броя на делата за последните две години. Въпреки високата натовареност на съда, дейността му като върховна инстанция обуславя факта, че съхранението на делата след тяхното приключване не се осъществява в неговата структура, а в първоинстанционния съд. Поради това броят на делата за съответната година е условен ориентир за обхвата на обработването за целите на правораздаването по наказателни дела.

Контекст на обработването: Обработването се осъществява при условията на стриктна нормативна уредба за дейността на съдилищата, произтичаща от Конституцията, Наказателно-процесуалния кодекс, Закона за съдебната власт, Правилника за администрацията ВКС, Наредба № 4 от 16.03.2017 г. за воденето, съхраняването и достъпа до регистъра на актовете на съдилищата и други. Ако произтича от задължения, поети с международни договори и са налице условията по чл. 72-77 от Закона за защита на личните данни, обработването на лични данни може да включва предаване в трети държави или международни организации.

Цел на обработването: Осигуряване на защитата от престъпни посегателства срещу Република България, срещу живота, свободата, честта, правата и законните интереси на гражданите, както и срещу правата и законните интереси на юридическите лица. В рамките на тази цел личните данни се използват за изпращане на призовки, съдебни книжа и друга кореспонденция, свързана с входящи и изходящи документи по повод движението и обработването на съдебните дела. Като съвместими с тази цел на обработването, по силата на нормативни задължения данните се използват за целите на архивирането в обществен интерес, статистически цели и научни изследвания.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид съчетаването на данните от съдебните дела на хартиен и електронен носител, вероятността от загуба на наличност и цялостност не е голяма. Освен това в чл. 71 от Правилника за администрацията на ВКС се съдържат правила за възстановяване на изгубено или унищожено дело. Предвидено е възстановяване на делото, а ако това не е възможно, делото може да бъде заведено повторно, без да се събират отново държавни такси. Поради това рискът от загуба на наличност и цялостност се определя като нисък.

Рискът от загуба на поверителност, поради обстоятелството, че данните се обработват в рамките на наказателно производство и с оглед презумпцията за невинност, обуславя по-сериозно въздействие върху страните, поради което не се квалифицира като нисък, а като среден. Единствено липсата на мащабност на обработването на лични данни поради ограничения срок за съхранение на делото само в рамките на разглеждането му в касационната инстанция обуславя решението на администратора на настоящия етап да не квалифицира дейността като високорискова.

Оценяване на риска: Предвид взетите в администратора мерки за защита, вероятността от настъпване на събитие, свързано със загуба на наличност и цялостност, се определя като малка, но по отношение на загубата на поверителност се допуска умерена вероятност да се случи. 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 т. 1 от настоящия анализ на риска: $ИР = Вп * Вз = 3 * 3 = 9$.

Обобщение за регистър „Наказателни дела“: Рискът от обработването на лични данни в регистър „Наказателни дела“ 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 материалният интерес по делата.

3.4. Регистър „Човешки ресурси“

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 и ЗСВ. Обхващат се и специални категории лични данни (за здравословното състояние) за изпълнение на специфичните задължения на съда като орган по назначаване. В регистъра в определени от Закона за съдебната власт случаи се обработват и данни за присъди и нарушения.

Обхват на обработването: Обработването обхваща личните данни на около 310 настоящи магистрати и съдебни служители, както и съхраняване на ведомости за заплати за приблизително още 400 бивши магистрати и служители и кандидати за назначаване на работа.

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 в 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 т. 1 от настоящия анализ на риска: $IP = Vп * Vз = 2 * 3 = 6$.

Обобщение за регистър „Човешки ресурси“:

Рискът от обработването на лични данни в регистър „Човешки ресурси“ 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.

3.5. Регистър „Заявления, сигнали и други искания“

Естество на обработваните лични данни: В зависимост от естеството на искането личните данни се отнасят до физическа, социална или друга идентичност на лицето, което подава съответното заявление, сигнал или друго искане, както и лични данни за други лица, посочени с оглед естеството на искането.

Обхват на обработването: Като база за определяне на обхвата на обработването се използва статистическа информация за 2021 г. и за 2022 г., както следва: около 60 сигнали и искания и 22 заявления по Закона за достъп до обществена информация. Като се отчита срокът за съхранение съгласно Номенклатурата на делата със срокове за съхранение, обработването не се определя като мащабно.

Контекст на обработването: Обработването на лични данни в регистъра не предполага предаване на лични данни в трети държави или международни организации, поради което не включва международен контекст.

Цел на обработването: Изпълнение на законови задължения, които произтичат за Върховния касационен съд.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид свеждането на данните до минимум и изпълнението на законови задължения за тяхното обработване, последиците за субектите на данни при загуба на наличност и цялостност могат да се свързват със забавяне при разглеждане на техните искания. Загубата на поверителност, ако личните данни са специални категории, може да рефлектира негативно неприкосновеността на личния живот.

Оценяване на риска: Предвид взетите в 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 т. 1 от настоящия анализ на риска: $IP = Vп * Vз = 2 * 3 = 6$.

Обобщение за регистър „Заявления, сигнали и други искания“:

Рискът от обработването на лични данни в регистър „Заявления, сигнали и други 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 и възможността за засягане на съответните права на субектите на данни, по повод на които са подадени съответните заявления, сигнали и други искания.

3.6. Регистър „Контрагенти“

Естество на обработваните лични данни: Лични данни, необходими за сключване и изпълнение на договора – данни за физическа и икономическа идентичност. При сключване на договори с юридически лица се събират лични данни за физическите лица, които ги представляват (с оглед сключването на договора) и които изпълняват дейности по договора (с оглед изпълнението на договора).

Обхват на обработването: Обхватът на обработването се определя на базата на сключените през 2021 и 2022 г. договори. Сключените през 2021 г. договори са 38, през 2022 г. – 35, до настоящия момент през 2023 г. – 26. С оглед сроковете за съхранение на договорите и броя на сключването им на годишна база, обработването на личните данни на контрагенти или техни представляващи не се определя като мащабно.

Контекст на обработването: Обработването на лични данни в регистъра не предполага предаване на лични данни в трети държави или международни организации, поради което не включва международен контекст.

Цел на обработването: Спазване на законови задължения при сключване на договори, произтичащи от Закона за обществените поръчки, Закона за задълженията и договорите и други нормативни актове, както и гарантирането на законосъобразност и прозрачност при разходването и отчитането на бюджетни средства.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид свеждането на данните до минимум и изпълнението на законови задължения за тяхното обработване, последиците за субектите на данни при загуба на наличност и цялостност могат да се свързват незначителни последици за субектите на данни. Загубата на поверителност също не би предизвикала риск, доколкото задължението за публичност по Закона за обществените поръчки и в контекста на § 1, т. 5, б. „е“ от Закона за достъп до обществена информация обуславя в редица случаи публикуване на информацията относно договорите. („5. Не представляват „производствена или търговска тайна“ факти, информация, решения и данни, свързани със стопанска дейност, чието запазване в тайна е в интерес на правоимащите, но е налице надделяващ обществен интерес от разкриването ѝ. До доказване на противното обществен интерес от разкриването е налице, когато тя: ... е) е свързана със страните, подизпълнителите, предмета, цената, правата и задълженията, условията, сроковете, санкциите, определени в договори, по които едната страна е задължен субект по чл. 3).

Оценяване на риска: Предвид взетите в 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 ниска. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в т. 1 от настоящия анализ на риска: $IP = Vп * Vз = 2 * 2 = 4$.

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, като изисква мониторинг чрез прилагане на подходящи технически и организационни мерки с цел да не се повиши неговата оценка. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и ограниченият им обем, както и липсата на специални категории лични данни.

3.7. Регистър „Видеонаблюдение“

Естество на обработваните лични данни: Обработваните лични данни обхващат данните за образа и местонахождението на лицата, които попадат в обхвата на средствата за наблюдение, установени в адвокатска стая и служба „Архив“ (в обща стая) и регистратурата за класифицирана информация.

Обхват на обработването: Обработването обхваща намиращите се в помещението с видеонаблюдение служители, страните и техните процесуални представители, които имат достъп до делата. Предвид това обхватът на обработването се определя на база данните за регистър „Граждански дела“, регистър „Търговски дела“ и регистър „Наказателни дела“, както и броя на служителите в адвокатска стая и архив и регистратурата за класифицирана информация. С оглед на констатациите за съответните регистри, обработването на лични данни и в този регистър не се определя като мащабно.

Контекст на обработването: Обработването на лични данни в регистъра не предполага предаване на лични данни в трети държави или международни организации, поради което не включва международен контекст.

Цел на обработването: Охранителна цел с оглед опазването на наличността, цялостността и поверителността на материалите по делата.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Последиците за субектите на данни от нарушения на сигурността на личните данни могат да се свържат със засягане на неприкосновеността на личността, но предвид ограничения обем на обхвата на заснемането не се очакват съществени последици.

Оценяване на риска: Предвид взетите в 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 ниска. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в т. 1 от настоящия анализ на риска: $IP = Vп * Vз = 2 * 2 = 4$.

Обобщение за регистър „Видеонаблюдение“:

Рискът от обработването на лични данни в регистър „Видеонаблюдение“ попада в зелената скала, определя се като „нисък“ и се счита за приемлив, като изисква мониторинг чрез прилагане на подходящи технически и организационни мерки с цел да не се повиши неговата оценка. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и ограниченият им обем, както и липсата на специални категории лични данни.

3.8. Регистър „Инициативи“

Естество на обработваните лични данни: Данни за идентифициране на участниците в инициативите, сведени до имена и евентуално снимков материал от съответната инициатива при съгласие на участниците.

Обхват на обработването: Обработването обхваща лични данни на не повече от 50 лица годишно.

Контекст на обработването: Обработването на лични данни в регистъра не предполага предаване на лични данни в трети държави или международни организации, поради което не включва международен контекст.

Цел на обработването: Постигане на обществено значими цели за повишаване на информираността на ученици за дейността на съдилищата.

Последици за субектите на данни от загуба на наличност, цялостност и поверителност: Предвид осъществяването на инициативите само въз основа на съгласие на участниците не се очакват негативни последици за тях.

Оценяване на риска: Предвид взетите в 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 ниска. Изчисленият риск има стойността на произведението на възможността за поява и въздействието. Изразено с показателите по методиката в т. 1 от настоящия анализ на риска: $ИР = Вп * Вз = 2 * 2 = 4$.

Обобщение за регистър „Инициативи“:

Рискът от обработването на лични данни в регистър „Инициативи“ попада в зелената скала, определя се като „нисък“ и се счита за приемлив, като изисква мониторинг чрез прилагане на подходящи технически и организационни мерки с цел да не се повиши неговата оценка. Основните фактори, които обуславят преценката за този риск, са естеството на обработваните лични данни и ограниченият им обем, както и липсата на специални категории лични данни.

4. Общо ниво на риска

Идентифицираните нива на риска за отделните регистри с лични данни води до следните резултати:

Регистър с лични данни	Идентифициран риск
Граждански и търговски дела	Среден риск
Наказателни дела	Среден риск
Човешки ресурси	Среден риск
Заявления, сигнали и други искания	Среден риск
Контрагенти	Нисък риск
Видеонаблюдение	Нисък риск
Инициативи	Нисък риск

Администраторът определя среден риск за правата и свободите на засегнатите от обработването субекти на данни, при наличие на обстоятелства, които засягат наличността, цялостността, достъпността и/или поверителността на данните. Предвид това на настоящия етап не се предприемат стъпки за извършване на оценка на въздействието върху защитата на данните, а в настоящия анализ се идентифицират подходящи технически и организационни мерки и въз основа на тях се преценява нивото на остатъчния риск.

5. Технически и организационни мерки за защита на личните данни

5.1. 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	София, бул. „Витоша“ 2, партер
Определяне на организация на физическия достъп	Служебни карти за достъп
Определяне на използваните технически	Заклучване на помещенията, сигнално-

средства за физическа защита	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

5.2. 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

5.3. 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	В Правилника за администрация на ВКС

5.4. 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
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
Поддръжане/ експлоатация	Регулярно наблюдение от служители на администратора

5.5. Криптографска защита

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

6. 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, определена в методиката по т. 1 от настоящия анализ:

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

За всеки регистър с лични данни остатъчният риск се изчислява като разлика от изчисления риск и произведението на новото въздействие и новата вероятност по следната формула: $OP = IP - (NBz * NBp)$

За обработваните регистри с лични данни остатъчният риск се оценява без изменения спрямо първоначалната оценка, с цел да се даде възможност преценката да бъде направена емпирично, въз основа на наблюдение на процеса на прилагане на техническите и организационните мерки в настоящия анализ.

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 2025 г., освен ако няма промени в естеството, обхвата, контекста и целта на обработването, както и в използваната технология за обработване.