*Приложение 4*

# АНАЛИЗ НА РИСКА
# ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ
# В ДЕЙНОСТА НА АДМИНИСТРАТИВЕН СЪД - ПЛЕВЕН

## I. Характеристики на обработването на лични данни

### 1. Особености на администратора на лични данни

Административен съд - Плевен 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 Административен съд - Плевен 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 Административен съд - Плевен 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 Административен съд - Плевен, 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 Административен съд - Плевен

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)** | ***Изчислен риск*** | | | | |
|---|---|---|---|---|---|
| 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 (Приложена към Вътрешните правила за защита на личните данни в Административен съд - Плевен), 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 за 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:

- Административен съд - Плевен се помещава в сграда, 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, Вътрешните правила за защита на личните данни в Административен съд - Плевен, 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 Административен съд - Плевен, се поддържат на хартиен или електронен носител.
- Обработването на личните данни се извършва в рамките на работното време на Административен съд - Плевен. 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 Административен съд - Плевен, 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 Административен съд - Плевен.
- 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 Административен съд - Плевен, Вътрешните правила за защита на личните данни в Административен съд - Плевен, Закон за защита на личните данни и др.
- Личните данни на хартиен носител се съхраняват в определените за целта служебни помещения в сградата на съда.
- Архивирането на лични данни на хартиен носител се осъществява в съответствие с Вътрешните правила за организацията и дейността на учрежденския архив в Административен съд - Плевен.
- 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 на документите от регистрите, същите се унищожават. Унищожението се извършва посредством възлагане на изпълнител 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 Административен съд - Плевен, 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.
- Когато информацията е класифицирана по смисъла на ЗЗКИ, помещението, в което се съхраняват информационните носители е с контролиран достъп, заключва се и се охранява със сигналноохранителна техника, като се прилага 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 Административен съд - Плевен 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 Единна деловодна информационна система (ЕДИС), внедрен във Върховния административен съд и административните съдилища, както и САС „Съдебно деловодство“, създаден и поддържан от „Информационно обслужване“ АД. С тези продукти се съхраняват и обработват данните за участниците в съдебния процес. Базата данни се намира и съхранява в специализирани сървъри във Върховния административен съд (за ЕДИС) и в Административен съд - Плевен (за САС) със съответните правила за защита от нерегламентиран достъп и създаване на резервни копия. Достъпът до модулите на продукта се извършва чрез индивидуални потребителски имена и пароли за оторизираните за работа с него лица.

б) За служба „Счетоводство“:

- Софтуерен продукт „RZ Win“ и софтуерен продукт „Hon Win“ – в които се съхраняват и обработват данните за съдии и служители, вещи лица, съдебни преводачи, особени представители, както и модул за електронно разплащане, предоставен от обслужващата съда банка. Базата данни се намира и съхранява на сървър на Административен съд - Плевен 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 възнаграждения и други плащания на съдии, съдебни служители, вещи лица, преводачи, свидетели,

особени представители, контрагенти и др. ПП е реализиран от Висшия съдебен съвет, достъпен онлайн и не е базиран на сървър на Административен съд - Плевен.

в) За служителя „Човешки ресурси“:

- Софтуерен продукт „Човешки ресурси“ - съхранява и обработва лични данни за магистрати и съдебни служители, работещи в Административен съд - Плевен. Базата данни се намира и съхранява на сървър на Административен съд - Плевен 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.

г) За регистриране и обработване на общоадминистративния документооборот на съда (несвързан със съдебните дела):

Програмен продукт „Eventis“, в който се съхраняват и обработват несвързани със съдебните дела данни на магистрати, съдебни служители, заявители, жалбоподатели, податели на сигнали, контрагенти, участници в инициативи на съда и др. Базата данни се намира и съхранява на сървър на Върховния административен съд.

## IV. Анализ на риска при обработването на лични данни в Административен съд - Плевен

### 4.1. За регистър „Персонал (съдии и съдебни служители) и участници в конкурсни процедури (респ. кандидати за работа)“

**Естество на обработваните лични данни**: В регистъра за съдии и съдебни служители 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 Административен съд - Плевен като работодател се обработват и специални категории лични данни (за здравословното състояние и др.). В регистъра, в определени от Кодекса на труда, случаи се обработват и данни за присъди и нарушения.

В регистъра за участници в конкурсни процедури (респ. кандидати за работа) 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 работещите в Административен съд - Плевен, 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, и др.;

Обработването обхваща също така лични данни на кандидатите за съдебни служители в Административен съд - Плевен, 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 на данните в регистъра за персонала 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.

Обработването на данните в регистъра на кандидатите за работа (в т.ч. участниците в конкурсни процедури) 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**:

За регистъра на персонала – управление на човешките ресурси, изпълнение на нормативни задължения и финансово-счетоводна отчетност.

За регистъра на кандидати за работа – управление на човешките ресурси – подбор на персонал, изпълнение на нормативни задължения.

**Последици за субектите на данни от загуба на наличност, цялостност и поверителност:**

За регистъра на персонала – 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.

За регистъра на кандидати за работа - 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:**

За персонала:

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.

За кандидатите за работа:

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 (съдии и съдебни служители) и участници в конкурсни процедури (респ. кандидати за работа):**

Рискът от обработването на лични данни в регистъра за персонала 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.

Рискът от обработването на лични данни в регистъра за кандидатите за работа 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.

**4.2. 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 Административен съд - Плевен 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 Административен съд - Плевен 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 Административен съд - Плевен и др.

**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.

**4.3. За регистър „Лични данни на лица, подали 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 „Лични данни на лица, подали молби, жалби, предложения, сигнали и искания“:**

Рискът от обработването на лични данни в регистъра 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.

**4.4. За регистър „Съдебни дела (физически лица, страни или участници в административни или касационни административнонаказателни 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 съдебен статус на участниците в съдебните процеси, 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 и др..

**Контекст на обработването**: Обработването се осъществява изцяло в контекста на правораздавателната дейност на Административен съд - Плевен, съгл. Регламент (ЕС) 2016/679. Предаване на лични данни на трети държави или международни организации става по изключение, само при наличие на нормативно регламентирани предпоставки и правно-обосновани изисквания.

**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 (физически лица, страни или участници в административни или касационни административнонаказателни производства):**

Рискът от обработването на лични данни в регистъра попада в горния регистър на 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.

**4.5. За регистър „Вещи лица, съдебни преводачи, свидетели и стажант-юристи“:**

**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 свидетели, тяхното здравословно и психическо състояние.

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

**Контекст на обработването**: Обработването на данните за вещи лица, съдебни преводачи и свидетели се осъществява изцяло в контекста на нуждите на правораздавателния процес. Предаване на лични данни на трети държави или международни организации става по изключение, само при наличие на нормативно регламентирани предпоставки и правно-обосновани изисквания. Обработването на данните за стажант-юристите се извършва във връзка с нормативноопределените изисквания за провеждане на основния и професионалния стаж на тези лица и не предвижда предаването на такива данни на трети държави или международни организации..

**Цел на обработването**: Правораздавателна дейност; нормативни изисквания за осигуряване на провеждането на основен и професионален стаж на стажант-юристите.

**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 преводачи, свидетели и стажант-юристи“:**

Рискът от обработването на лични данни в регистъра 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.

**4.6. За регистър „Инициативи на Административен съд - Плевен“:**

**Естество на обработваните лични данни:** В регистъра се обработват *„обикновени“* лични данни за физическа (в т.ч. снимкови или видеоматериали) и социална идентичност, сведени до минимум, с оглед защитата на личните данни.

**Обхват на обработването:** Обработването обхваща лични данни ученици, техните родители, магистрати, съдебни служители, наставници и други участници в инициативи на Административен съд - Плевен.

**Контекст на обработването**: Обработването се осъществява за реализирането на инициативи на Административен съд - Плевен. Обработването не предполага предаване на лични данни в трети държави (извън ЕС) и международни организации.

**Цел на обработването**: Изпълнение на образователни програми, програми за информиране на обществеността за дейността на съда и др. инициативи.

**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 на Административен съд - Плевен“:**

Рискът от обработването на лични данни в регистърапопада 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.

**4.7. За регистър „Видеонаблюдение“**

**Естество на обработваните лични данни**: В регистъра се обработват *„обикновени“* лични данни за физическа идентичност (видеоизображения); косвено могат да бъдат обработени и специални данни за здравословното състояние на лицата – когато то е видно от видеоизображенията.

**Обхват на обработването**: Обработването обхваща видеоизображения на работещите в съда, участниците в съдебния процес и други посетители в сградата.

**Контекст на обработването**: Обработването се осъществява в контекста на нуждата от контрол на достъпа и охрана на сградата, инвентара, работещите и посетителите в сградата на съда. Обработването не предполага предаване на лични данни в трети държави (извън ЕС) и международни организации.

**Цел на обработването**: Спазване на законово задължение, което се прилага спрямо администратора, произтичащо от Закона за съдебната власт и правомощията на ГД „Охрана“.

**Последици за субектите на данни от загуба на наличност, цялостност и поверителност:** нарушена неприкосновеност на събираните лични данни, накърняване на репутацията, косвено разкриване на здравословното състояние, когато то е видно от записаните видеоизображения.

**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 „Видеонаблюдение“:**

Рискът от обработването на лични данни в регистъра 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 евентуалното наличие на специални категории лични данни в регистъра.

## V. Технически и организационни мерки за защита на личните данни в Административен съд - Плевен

### 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 | Вътрешна организация на дейността в Административен съд - Плевен |
| Определяне на организация на физическия достъп | Служебни/лични карти, система за контрол на достъпа |
| 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 |

### 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 по отношение защитата 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, както и съгласно нормативно определени задължения |
| 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 администрацията на съдилищата |

### 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 (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 |

**5.5. 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 |

**VI. 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, новото въздействие 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 (съдии и съдебни служители) и участници в конкурсни процедури (респ. кандидати за работа)“**

За персонала:

Нова вероятност – стойност 2, ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новата вероятност и новото въздействие по следната формула: ОР = ИР – (НВр х НВз) = 6 – (2 х 2) = 2.

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

За кандидатите за работа (в т.ч. участниците в конкурсни процедури):

Нова вероятност – стойност 2, ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новата вероятност и новото въздействие по следната формула: ОР = ИР – (НВр х НВз) = 6 – (2 х 2) = 2.

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

**6.2. За регистър „Контрагенти“:**

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

Остатъчен риск е сведен до минимум, но въпреки това предприетите технически и организационни мерки следва да бъда проверявани.

**6.3. За регистър „Лични данни на лица, подали 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 новата вероятност и новото въздействие по следната формула: ОР = ИР – (НВр х НВз) = 6 – (2 х 2) = 2.

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

**6.4. За регистър „Съдебни дела (физически лица, страни или участници в административни и касационни административнонаказателни производства):**

Нова вероятност – стойност 3, ново въздействие – стойност 3. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новата вероятност и новото въздействие по следната формула: ОР = ИР – (НВр х НВз) = 10 – (3 х 3) = 1.

Остатъчният риск е малък. Въпреки това, предвид евентуалния обхват на засегнатите лица, както и въздействието на риска при неговото реализиране, предприетите технически и организационни мерки подлежат на ежедневен и задълбочен мониторинг.

**6.5. За регистър „Вещи лица, съдебни преводачи, свидетели и стажант-юристи“:**

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

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

**6.6. За регистър „ Инициативи на Административен съд - Плевен“**

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

Остатъчният риск е сведен до минимум. Въпреки това предприетите организационни и технически мерки подлежат на мониторинг.

**6.7. За регистър „Видеонаблюдение“:**

Нова вероятност – стойност 2, ново въздействие – стойност 2. Остатъчният риск се изчислява като разлика от изчисления риск и произведението на новата вероятност и новото въздействие по следната формула: ОР = ИР – (НВр х НВз) = 6 – (2 х 2) = 2.

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

## VII. Мониторинг 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 регистрирана промяна в някой от параметрите, взети предвид при идентифицирането на риска, неговата оценка, предприетите мерки и оценката на остатъчния риск, както и при идентифициране/проявление на нови рискове.

*Изготвил: (п)*
*Свилен Александров –*
*дл.лице по защита на данните*