УТВЪРЖДАВАМ:

**СЛАВ БАКАЛОВ**

Административен ръководител –

Председател на

Административен съд –Сливен

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И

СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ,

 ОБРАБОТВАНИ В АДМИНИСТРАТИВЕН СЪД – СЛИВЕН

I. ОБЩИ ПОЛОЖЕНИЯ

**Чл. 1.** Настоящите правила уреждат организацията на обработване и регламентират механизмите за защита на лични данни на магистрати и съдебни служители, включително и на кандидатите за работа в съда, на контрагентите и партньорите на съда, както и на всички други групи физически лица, с които Административен съд – Сливен влиза в отношения при осъществяването на правомощията и дейността си, като гарантират нормативно установените принципи на обработване на лични данни - законосъобразност, добросъвестност, прозрачност, точност и съвместимост с целите.

II. АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ

**Чл. 2.** (1) Администратор на лични данни по смисъла на чл. 4, ал. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679 (Регламента) е Административен съд – Сливен - юридическо лице на бюджетна издръжка с адрес град Сливен, бул. Цар Освободител №12, Булстат: 119667813.

(2) Като администратор на лични данни, при обработването на лични данни Административен съд – Сливен спазва принципите за защита на личните данни, предвидени в Регламента и законодателството на Европейския съюз и Република България.

**Чл. 3.** Като юридическо лице, възникнало по силата на закон, Административен съд – Сливен осъществява правораздавателна дейност, регламентирана в Конституцията на Република България, Закона за съдебната власт, Административнопроцесуален кодекс и др. нормативни актове, във връзка с която обработва лични данни и сам определя целите и средствата за обработването им.

**Чл. 4.** (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

 (3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

**Чл. 5.** (1) Принципите за защита на личните данни са:

1. *Законосъобразност, добросъвестност и прозрачност* - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

2. *Ограничение на целите* – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

3. *Свеждане на данните до минимум* – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;

4. *Точност* – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

5. *Ограничение на съхранението* – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

6. *Цялостност и поверителност* – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. *Отчетност* – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(2) Ако конкретната цел или цели, за които се обработват лични данни от Административен съд – Сливен, не изискват или вече не изискват идентифициране на субекта на данните, Административен съд – Сливен не е задължен да поддържа, да се сдобие или да обработи допълнителна информация за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

III. ОТГОВОРНОСТИ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

**Чл. 6.** Административен съд – Сливен организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

**Чл. 7.** Административен съд – Сливен прилага адекватна защита на личните данни, която включва:

1. Физическа защита;

2. Персонална защита;

3. Документална защита;

4. Защита на автоматизирани информационни системи и мрежи;

5. Криптографска защита.

**Чл. 8.** (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на Административен съд – Сливен и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на Административен съд – Сливен на хартиен, технически и/или електронен носител се извършва по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 9. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от Административен съд – Сливен, подписват декларация за съгласие по образец (Приложение № 1).

Чл. 10.(1) Право на достъп до регистрите с лични данни имат само магистрати и служители в Административен съд – Сливен , съобразно възложените им от закона правомощия и нормативно определените им функции, както и обработващи лични данни, на които Административен съд – Сливен е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните (напр. Служба по трудова медицина).

(2) Съдиите и съдебните служители носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от щатния състав може да бъде основание за налагане на дисциплинарни санкции на съответните длъжностни лица.

(3) Съдиите и съдебните служители нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Чл. 11. (1) Всяко лице, действащо под ръководството на администратора, което има достъп до личните данни, обработва тези данни във връзка със своите служебни функции и не следва да ги разпространява на трети лица. Във връзка с осигуряването на мерки за защита на личните данни Администраторът или оправомощено от него лице провежда първоначален или инцидентен инструктаж на съдиите и служителите на Административен съд – Сливен за запознаване с настоящите правила /протокол, който се подписва собственоръчно от лицето, което ще има достъп до личните данни, и лицето, извършило инструктажа – Приложение № 2/. След прекратяване на правоотношенията с Административен съд – Сливен лицето с достъп до лични данни попълва декларация за конфиденциалност относно обработените от него лични данни, станали му известни при и по повод изпълнение на служебните функции /Приложение № 3, което се подписва собственоръчно от лицето, имало достъп до личните данни/. Декларацията се попълва към датата на прекратяване на правоотношенията и е със срок на действие не по-малко от 2 /две/ години.

 (3) При обработването на личните данни съдиите от състава на Административен съд – Сливен спазват Кодекса за етично поведение на българските магистрати, а съдебните служители - Етичния кодекс на съдебните служители.

**Чл. 12.** (1) Документите, преписките и делата, по които работата е приключила, се предават за архивиране по реда на Вътрешните правила за дейността на учрежденския архив на Административен съд - Сливен.

(2) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в учрежденския архив, за срокове, съобразени с действащото законодателство и Номенклатурата на делата в Административен съд - Сливен. Учрежденският архив е оборудван с пожароизвестителна система и пожарогасител, със система за контрол на достъпа и задължително се заключва.

(3) Достъп до архивното помещение има само съдебният архивар, а в негово отсъствие определен със заповед на административния ръководител заместващ го съдебен служител.

(4) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от оператор на лични данни (съдебен служител, определен със заповед на административния ръководител) с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните.

**Чл. 13.** С оглед защита на хартиените, техническите и информационните ресурси всички съдии и служители са длъжни да спазват правилата за противопожарна безопасност. Най-малко веднъж годишно те преминават периодичен инструктаж за пожаробезопасна експлоатация в обекта, провеждан от определеното със заповед на административния ръководител (Заповед № РД-13-205/21.09.2012 г.) длъжностно лице.

**Чл. 14.** (1) Най-малко веднъж годишно се извършва проверка за състоянието и целостта на личните данни, съдържащи се в обработваните от Административен съд – Сливен регистри. Проверките се осъществяват при провеждане на инвентаризации за наличност на съдебни и номенклатурни дела и инвентаризации на дълготрайни и недълготрайни материални активи, извършвани от комисия, назначена от административния ръководител на Административен съд – Сливен, която изготвя доклад за резултата от проверката. Докладът трябва да включва и преценка на необходимостта за обработка на личните данни или унищожаване.

**Чл. 15.** (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира административния ръководител. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

 (2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

 **Чл. 16.** (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, Административен съд – Сливен може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят веднъж на 2 години или при промяна на характера на обработваните лични данни.

 **Чл. 17.** (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните Административен съд – Сливен регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и във Вътрешните правила за дейността на учрежденския архив.

(2) В случаите, в които се налага унищожаване на носител на лични данни, Административен съд – Сливен прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

 1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

 2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

 (3) За унищожаването на носители на лични данни се съставя протокол(Приложение 4)

**Чл. 18.** (1) Достъп на физически лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство след подаване на заявление, респ. искане за достъп на информация и след тяхното легитимиране. Страните по съдебни дела не подават заявление.

(2) Решението за предоставяне или отказване достъп до лични данни за съответното лице се съобщава в 1-месечен срок от подаване на заявлението, респ. искането.

(3) Информацията може да бъде предоставенa под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(5) Третите страни получават достъп до лични данни, обработвани в Административен съд – Сливен, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ и др.п.).

# IV МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

**Чл. 18. *Физическата защита*** в Административен съд – Сливен се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на помещенията, в които се извършват дейности по обработване на лични данни.

**Чл. 19.** (1). Основните ***организационни мерки за физическа защита*** в Административен съд – Сливен включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни,
3. определяне на организацията на физическия достъп;

 (2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения*, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи.

(4) *Организацията на физическия достъп до помещения*, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

*(5) Зони с контролиран достъп* са всички помещения на територията на Административен съд – Сливен, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни в Административен съд – Сливен са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

(8) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа.

**Чл. 20.** (1). Основните ***технически мерки******за физическа защита*** в Административен съд – Сливен включват:

1. използване на ключалки и заключващи механизми;
2. шкафове, метални каси
3. оборудване на помещенията с пожароизвестителни и пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в *шкафове, в кабинети, които се заключват,*  като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за кабинетите притежават съответните съдебни служители по силата на служебните им задължения и длъжностната характеристика.

(3) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: *ключалки* (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица и пожарогасителни средства.

(4) *Пожароизвестителните средства* и *пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

**Чл. 21.** (1). Основните ***мерки за персонална защита*** на личните данни, приложими в Административен съд – Сливен, са:

1. Лицата, обработващи лични данни са задължени да познават нормативната уредба в областта на защита на личните данни (Общия регламент относно защитата на данните (ЕС) 2016/679, настоящите Правила, Политиката за защита на лични данни прилагана в Адм.съд Сливен(утвърдена със Заповед № РД-13-234 от 22.10.2018 и Правилата за управление и контрол на информацията в Административен съд – Сливен, утвърдени от административния ръководител със Заповед № РД-13-215 от 10.11.2014 г.). Съдии и съдебни служители се запознават с настоящите Вътрешни правила след утвърждаването им, включително и при последващо актуализиране, както и при постъпване на работа, което се удостоверява с полагане на подпис в изричен списък;
2. Запознаване и осъзнаване на опасностите за личните данни, обработвани от Административен съд – Сливен;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между щатния състав и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

 (2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

**Чл. 22.** (1). Основните ***мерки за документална защита*** на личните данни, са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител* - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на Административен съд – Сливен, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на Административен съд – Сливен, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. *Регламентиране на достъпа до регистрите* *с лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;
4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. *Процедури за унищожаване* - документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на Административен съд – Сливен или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. *Контрол на достъпа до регистрите*, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;
2. ***Правила за размножаване и разпространение*,** които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

**Чл. 23.** (1) ***Защитата на автоматизираните информационни системи и/или мрежи***в Административен съд – Сливен включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. *Идентификация и автентификация* чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на Административен съд – Сливен. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае”;
2. *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;
3. Управление на *външни връзки и/или свързване*, включващо от своя страна:

3.1.Дефиниране на обхвата на вътрешната мрежа: Като *вътрешна мрежа* се разглежда локална жична мрежа и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на Административен съд – Сливен. Като *външна мрежа* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на Административен съд – Сливен.

3.2.Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено съдиите и служителите и/или специално упълномощени от административния ръководител на Административен съд – Сливен лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае“. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

3.3.Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на системния администратор. В отговорностите му са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Административен съд – Сливен.

3.4.Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на системния администратор. Той е задължен да предприеме адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на Административен съд – Сливен, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

1. *Защитата от зловреден софтуер* включва:

4.1.използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от системния администратор. Забранено е инсталирането на софтуерни продукти без изричното му одобрение.

4.2.използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от системния администратор или от оторизирани от ръководството на Административен съд – Сливен лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

4.3.активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

4.4.забрана за пренос на данни от външен носител – системният администратор проверява всеки външен носител преди да бъде използван във вътрешната мрежа.

4.5.при съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми системния администратор и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

1. Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

5.1.Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на Административен съд – Сливен.

5.2.Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

5.3.Отговорност за архивиране има системният администратор.

5.4.Срокът на архивиране следва да е съобразен с действащото законодателство.

5.5.Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

1. Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти и др. носители на информация, еднократно записваеми носители и др.)
2. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификатаи нуждите наАдминистративен съд – Сливен.
3. Данните, които вече не са необходими за целите на Административен съд – Сливен и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. *Организация на* *телекомуникационните връзки и отдалечения достъп* до вътрешните мрежи на Административен съд – Сливен:

1.1.Отдалечен достъп до вътрешната мрежа на Административен съд – Сливен не е предвиден. По изключение, и след изричната оторизация от ръководството на Административен съд – Сливен, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

1.2. На съдии и/или служители от Административен съд – Сливен може да бъде предоставен отдалечен достъп за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано със системния администратор за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и одобрено от ръководството на Административен съд – Сливен. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време след мотивирано становище от системния администратор, както и в случаите на заплаха за сигурността на данните.

1.3. Публикуването на служебна информация на интернет страницата на Административен съд – Сливен или в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено от съдебния администратор или системния администратор, или след писмена оторизация от административния ръководител на Административен съд – Сливен.

1. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на Административен съд – Сливен, включват:

2.1. Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на Административен съд – Сливен от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

2.2. Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на Административен съд – Сливен, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър.

2.3. Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (магнитни карти за контрол на достъпа, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

**Чл. 24.** (1) По отношениеналичните данни се прилагат и мерки, свързани с ***криптографска защита на данните*** чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване.

(2) Криптирането се използва и за защита на личните данни, които се предават от Административен съд – Сливен по електронен път или на преносими носители.

**Чл. 25.** Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.) - При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощено лице вписва в дневника последствията от инцидента и мерките, които са предприети за отстраняването им. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

# V. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

**Чл. 26.** (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) Административен съд – Сливен прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

**Чл. 27.** (1)Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

**Чл. 28.** (1) В Административен съд – Сливен се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от системния администратор. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни, предварително се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

**Чл. 29.** Съдии и служители, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

# VI. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

**Чл. 30.** Поддържаните от Административен съд – Сливен регистри с лични данни са:

1. регистър „Персонал”

2. регистър „Вещи лица и свидетели“

3. регистър „Деловодство“

4. регистър „Заявления за достъп до обществена информация”

 5. регистър „Трудови възнаграждения и социално-осигурителни плащания”

6.регистър „Контрагенти“

7.регистър по ЗЗКИ

РЕГИСТЪР „ПЕРСОНАЛ”

Чл.31. В регистъра се обработват лични данни на магистрати и съдебни служители, с оглед:

1. индивидуализиране на трудови правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив, Закона за съдебната власт, Правилника за администрацията в съдилищата и др.;

3. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите правоотношения;

- за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови договори;

Чл.32. В регистъра се обработват категории лични данни на следните основания:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. икономическа идентичност: данни относно имотното и финансово състояние на физическото лице, участието и/или притежаването на дялове или ценни книжа на дружества и др.;

5. лични данни относно гражданско-правния статус на лицата (напр. свидетелства за съдимост), необходима предпоставка за започване на работа в съдебната система за всички длъжности;

6. лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство за започване на работа, експертни лекарски решения и др.

Чл. 34. (1) Данните от регистъра се обработват от административния секретар, който изпълнява длъжността „личен състав“ и съдебни служители, чиито задължения включват обработване на данните на персонала, при спазване на принципа „Необходимост да се знае”. Лицата, обработващи личните данни в регистър „Личен състав“ се определят със заповед на административния ръководител.

(2) Право на достъп до регистъра има само упълномощени лица.

(3) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

(4) Административния секретар трябва да извършва ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението – за заличаването им.

РЕГИСТЪР „ВЕЩИ ЛИЦА И СВИДЕТЕЛИ”

Чл.35.(1) В регистъра се обработват лични данни на физически лица, явяващи се в качеството си на вещо лице/експерт, свидетел и др. в съдебния процес.

(2) Личните данни се обработват, с оглед на:

1. индивидуализиране на граждански правоотношения;

2. изпълнение на нормативните изисквания на Закона за съдебната власт, Правилника за администрацията на съдилища, Наредба за възнагражденията на вещите лица, Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив, и др.;

3. използване на събраните данни за съответните лица за служебни цели:

- за изготвяне на всякакви документи на лицата в тази връзка (договори, анекси, документи, служебни бележки, справки за изплатени суми, удостоверения и др. подобни);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по граждански договори;

- за водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица.

Чл.37. В регистъра се обработват категории лични данни на следните основания:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография (за вещи лица само);

3. лични данни, които се отнасят до здравето: данните се съдържат в експертни лекарски решения и др.

Чл. 39. Данните от регистъра се обработват от съдебни служители, чиито задължения включват обработване на данните на вещите лица, при спазване на принципа „Необходимост да се знае”. Лицата, обработващи личните данни в регистър „Вещи лица “ се определят със заповед на административния ръководител.

2. Право на достъп до регистъра има само упълномощени лица.

3. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

РЕГИСТЪР „ДЕЛОВОДСТВО”

Чл.39. В регистъра се обработват лични данни на физически лица, участници в съдебния процес, с оглед на:

1. изпълнение на нормативните изисквания на Закона за съдебната власт, Правилника за администрацията в районните, окръжните, административните, военните и апелативните съдилища, АПК и др.;

2. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съдебния процес – призоваване, връчване на решения, съобщения и др. съдебни книжа и други дейности;

- за изготвяне на всякакви документи на лицата в тази връзка (удостоверения, изпълнителни листове, служебни бележки, справки, и др. подобни);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до участието му в съдебния процес;

Чл.40. В регистъра се обработват категории лични данни на следните основания:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години), както и родствени връзки;

4. лични данни относно гражданско-правния статус на лицата, необходими при протичането на съдебния процес (напр. свидетелства за съдимост);

5. лични данни, които се отнасят до членство в политически партии и организации;

6. лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство, медицински експертизи, експертни лекарски решения и др.

 Чл.41.Данните от регистъра се обработват от съдебни служители в Административен съд – Сливен, определени със заповед на административния ръководител.

2. Право на достъп до регистъра имат само определените със заповедта на административния ръководител лица.

3. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

РЕГИСТЪР „ТРУДОВИ ВЪЗНАГРАЖДЕНИЯ И СОЦИАЛНО-ОСИГУРИТЕЛНИ ПЛАЩАНИЯ”

Чл.42. В регистъра се обработват лични данни на магистрати и съдебни служители, с оглед:

1. индивидуализиране на трудови правоотношения;

2. изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив, Закона за съдебната власт, Правилника за администрацията в съдилищата и др.;

3. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите правоотношения;

- за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови договори;

- за водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица по трудови правоотношения.

Чл.43. В регистъра се обработват категории лични данни на следните основания:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.);

2. социална идентичност: данни относно образование и допълнителни квалификации (вид на образованието, място, номер и дата на издаване на дипломата), както и трудова дейност и професионална биография;

3. семейна идентичност: данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

4. лични данни, които се отнасят до здравето: данните се съдържат в медицинско свидетелство за започване на работа, експертни лекарски решения и др.

Чл. 44. Данните от регистъра се обработват от главния счетоводите

и съдебни служители, чиито задължения включват обработване на данните на персонала, при спазване на принципа „Необходимост да се знае”.

1.Лицата, обработващи личните данни в регистър „Трудови възнаграждения и социално-осигурителни плащания“ се определят със заповед на административния ръководител.

2. Право на достъп до регистъра има само упълномощени лица.

3. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

РЕГИСТЪР „ЗАЯВЛЕНИЯ ЗА ДОСТЪП ДО ОБЩЕСТВЕНА ИНФОРМАЦИЯ”

Чл. 45. В регистърът се обработват лични данни на физически или юридически лица в качеството им на заявители. По изискване на ПАС, този регистър се води на хартиен носител. Личните данни на тези лица се обработват от, с оглед използването им за служебни цели свързани с изготвяне на справки и удостоверения:

Чл. 46. В регистърът се обработват следните категории лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, адрес, телефони за връзка и др.);

Данните в регистъра се предоставят от физическите лица при подаване на заявления пред Административен съд – Сливен. Данните се въвеждат в регистъра за достъп до обществена информация, кореспонденция и др.

Чл. 47. Данните от регистъра се обработват от съдебни служители в Административен съд – Сливен, определени със заповед на административния ръководител.

1. Право на достъп до регистъра имат само определените със заповедта на административния ръководител лица.

2. Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

 РЕГИСТЪРЪТ “КОНТРАГЕНТИ”

Чл.48 В регистъра се обработват и съхраняват лични данни на физически и юридически лица, нормативно регламентирани във връзка с извършването на дейности, както пряко свързани с основната дейност на регистратора, така и във връзка с допълнителни дейности- възлагане на обществени поръчки, изпълнение на текущи и аварийни ремонти и др.

1. индивидуализиране на данни, свързани със сключване на договори;

2. използване на събраните данни за съответните лица за служебни цели:

- за всички дейности, свързани с осъществяване на основната дейност- правораздаване и допълнителни дейности

 -изпълнение на нормативните изисквания на Кодекса на труда,
Кодекса за социално осигуряване, Закона за съдебната власт, Закона за счетоводството, Закона за държавния архив и др.;

Чл.49. Събраните данни за съответните физически и юридически лица се използват за служебни цели:

 -за изготвяне на всякакви документи на лицата в тази връзка (договори, анекси, служебни бележки, справки, удостоверения и др. подобни);

 - за установяване на връзка с лицето по телефон, за изпращане на

кореспонденция, отнасяща се до изпълнение на задълженията му по

сключени договори;

 -за водене на счетоводна отчетност относно разплащането с
посочените по-горе физически и юридически лица;

Чл.50**.** В регистъра се обработват следните категории лични данни:

- физическа идентичност: имена, ЕГН, номер, дата и място на издаване на документи за самоличност, постоянен и настоящ адрес и др.;

**-** трудова дейност: месторабота и заемана длъжност, професионален опит.

Чл.51. Данните от регистъра се обработват от Съдебния администратор, Главния счетоводител, Административния секретар и служителите, в чиито длъжностни характеристика е определено задължение за обработване на данните на външни лица - представители на фирми, извършващи външни услуги и при спазване на принципа „Необходимост да се знае”.

1. Право на достъп до регистъра имат само лицата, които обработват данните.

2. Длъжностните лице нямат право да разпространява информация за личните данни, станали му известни при изпълнение на служебните му задължения.

РЕГИСТЪР ПО ЗЗКИ

Чл.52. Регистърът “ЗЗКИ” набира и съхранява лични данни на участниците в съдебния процес в съда по време на процес с оглед:

* индивидуализиране на страните и участниците в процеса;

 - изпълнение на нормативните изисквания на процесуалните кодекси, ЗЗКИ и Правилника за администрацията в съдилища и др.;

Чл.53. Събраните данни за съответните лица се използват за служебни цели:

* за всички дейности, свързани със съществуване, изменение и
прекратяване на участието им в процеса - за изготвяне на
всякакви документи на лицата в тази връзка (служебни бележки,
справки, удостоверения и др. подобни);
* за установяване на връзка с лицето по телефон, за изпращане на
кореспонденция, отнасяща се до изпълнение на задълженията му като страна/ участник в процеса;
* за водене на счетоводна отчетност относно дължимите плащания от и на посочените по-горе лица за държавни такси и разноски по делата ;

Чл.54. В регистъра се обработват следните категории лични данни:

- за физическа идентичност: имена, ЕГН, адреси, телефони за връзка дата и място на издаване на документи за самоличност, постоянен и настоящ адрес и др.;

- здравен статус на физически лица

-гражданско състояние на физически лица- семейно положение, данни за наследници.

**-** трудова дейност: месторабота и размер на трудовото възнаграждение.

- социално-икономическа идентичност: имотно и финансово състояние, участие в сдружения и /или притежаване на дялове или ценни книжа на дружества и др.

Чл.55. Данните от регистъра се обработват от Адм. ръководител – Председател, съдиите и служителите с достъп до класифицирана информация

- Право на достъп до регистъра посочените по-горе лица

- Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

# VІI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

**Чл. 31.** Всички съдии и служители в Административен съд – Сливен са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

**Чл. 32.** Контрол по прилагане на мерките за физическа, персонална и документална защита на личните данни осъществява ……………, определен със Заповед на председателя на Административен съд – Сливен, а контролът по криптографската защита и защита на автоматизирани информационни системи и мрежи – от системния администратор.

**Чл. 33**. Надзор и осигуряване спазването на Регламент (ЕС) 2016/679 и Закон за защита на личните данни при обработване на лични данни в Административен съд - Сливен във връзка с изпълнение на функциите му на орган на съдебната власт осъществява Инспектората към Висшия съдебен съвет съгласно Глава Трета от Закона за защита на личните данни (изм. и доп., ДВ бр. 17 от 26.02.2019 г.).

**Чл. 34.** (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Закона за защита на личните данни (изм. и доп., ДВ бр. 17 от 26.02.2019 г.), Общия регламент относно защитата на данните (ЕС) 2016/679 и приложимото право на Европейския съюз.

 (2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- Приложение №1 „Декларация за съгласие“

- Приложение №2 „Протокол за инструктаж“

- Приложение №3 „Декларация за конфиденциалност“

-Приложение № 4 „Протокол за унищожаване на носители на лични данни“

**Чл. 35.** Вътрешните правила са Утвърдени със Заповед ……………………. на административния ръководител-председател на Административен съд – Сливен и се актуализират по реда на тяхното утвърждаване.

Изготвил:Съдебен администратор……………

 /М.Едрева/