РЕПУБЛИКА БЪЛГАРИЯ
Р А Й О Н Е Н С Ъ Д – П Л О В Д И В

УТВЪРЖДАВАМ:
ИВАН КАЛИБАЦЕВ
Административен ръководител –
Председател на Районен съд - Пловдив
дата: 18.11.2021 г.

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В РАЙОНЕН СЪД – ПЛОВДИВ

гр. Пловдив, бул. „Шести септември" № 167
тел.: 032/656 361, факс 032/656 375, e-mail: rsp@rs-plovdiv.com

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила са изготвени в съответствие с изискванията на Регламент /ЕС/ 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕД /Общ регламент относно защитата на данните/.

Чл. 2. Правилата определят реда, по който Районен съд – Пловдив събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.

Чл. 3. 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 Районен съд – Пловдив 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. 4. (1) Администратор на лични данни по смисъла на чл. 4, ал. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679 (Регламента) е Районен съд – Пловдив - юридическо лице на бюджетна издръжка с адрес гр. Пловдив, бул. „Шести септември" № 167, БУЛСТАТ: 000471778. Искания до съда в качеството му на администратор на данни могат да се изпращат по пощата, лично да бъдат подадени в Регистратурата на съда или да се отправят на електронен адрес: **rsp@rs-plovdiv.com.**

(2) Районен съд – Пловдив обработва личните данни самостоятелно или чрез възлагане на обработващ лични данни.

(3) Достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения /по закон и/или по длъжностна характеристика/ или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да

се знае". Тези лица – магистрати и съдебни служители, действат под ръководството и по указания на администратора и са длъжни да познават и прилагат нормативната уредба в областта на защитата на личните данни, настоящите правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в Районен съд – Пловдив.

Чл. 5. (1) Като юридическо лице, възникнало по силата на закон, Районен съд – Пловдив осъществява правораздавателна дейност, регламентирана в Конституцията на Република България, Закона за съдебната власт, Наказателно-процесуален кодекс, Гражданско-процесуален кодекс и др. нормативни актове, във връзка с която обработва лични данни и сам определя целите и средствата за обработването им. Осъществяването на надзор и осигуряване спазването на Регламент /ЕС/ 2016/679, на ЗЗЛД и на нормативните актове в областта на защитата на личните данни при обработването на лични данни от Районен съд – Пловдив при изпълнение на функциите му на орган на съдебната власт се осъществяват от Инспектората на Висшия съдебен съвет, съгласно Глава Трета от Закона за защита на личните данни (изм. и доп., ДВ бр. 17 от 26.02.2019 г.). По отношение на личните данни, обработвани в контекста на правораздавателната дейност на съда, правото на жалба се упражнява пред Инспектората на Висшия съдебен съвет, който е компетентен надзорен орган, съгласно чл. 17 ал. 1 от ЗЗЛД.

(2) Районен съд – Пловдив обработва лични данни и във връзка с трудово-правните отношения, финансово-счетоводната дейност и др. на работещите по щатно разписание в институцията. При изпълнение на тази си административна дейност, надзорът по прилагане на правилата за обработване на лични данни се осъществява от Комисията за защита на личните данни.

Чл. 6. (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. 7. (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 Районен съд – Пловдив, не изискват вече идентифициране на субекта на данните, администраторът на лични данни 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. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 8. (1) Длъжностното лице по защита на личните данни в Районен съд - Пловдив е съдебният служител на длъжност „Човешки ресурси", определено със заповед на Административния ръководител на съда. Връзка със служителя може да се осъществи на адрес :гр. Пловдив, бул. „Шести септември"№ 167, тел. 032/656-362, statistik@rs-plovdiv.bg; Длъжностното лице по защита на данните има следните задължения и правомощия:

1. Поддържа връзка и сътрудничи с Комисията за защита на личните данни и Инспектората към Висшия съдебен съвет;
2. При поискване предоставя съвети по отношение на оценка на въздействие върху защита на данните и да наблюдава извършването на оценката;
3. Осигурява организация по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
4. Следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
5. Осъществява контрол по спазване на изискванията за защита на регистрите;
6. Контролира спазването на правата на потребителите във връзка с регистрите и програмно- техническите ресурси за тяхната обработка;
7. Следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред на обработването;
8. Определя ред за съхраняване и унищожаване на информационни носители;
9. Определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
10. Определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;
11. Отчита рисковете свързани с операциите по обработване на личните данни;

12. Провежда периодичен контрол за спазване изискванията по защита на данните и при открити нередности предлага мерки за тяхното отстраняване.

13. Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

14. Води регистър на дейностите по обработване на лични данни в Районен съд – Пловдив - **/Приложение № 9/** и Регистър на нарушения на сигурността на личните данни **/Приложение № 10/.**

Чл. 9. Служителите на Районен съд - Пловдив са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да актуализират при необходимост регистрите на личните данни;

4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

6. да не допускат неоторизирани лица в помещенията, в които се съхраняват данните.

Чл. 10. За неизпълнение на задълженията вменени на съответните длъжностни лица по ЗЗЛД се налагат дисциплинарни наказания по КТ, а когато неизпълнението на съответното задължение е констатирано и установено от компетентен орган, предвидено в ЗЗЛД и ОРЗД административно наказание – глоба. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

IV. ОТГОВОРНОСТИ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 11. Районен съд – Пловдив 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. 12. Районен съд – Пловдив 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. 13. (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 Районен съд – Пловдив и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на Районен съд – Пловдив 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. 14. 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 Районен съд – Пловдив, подписват декларация за съгласие по образец **(Приложение № 1).**

Чл. 15. (1) Право на достъп до регистрите с лични данни имат само магистрати и служители в Районен съд – Пловдив, съобразно възложените им от закона правомощия и нормативно определените им функции, както и обработващи лични данни, на които Районен

съд – Пловдив 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 на съда 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, за което задължително подписват декларация **/Приложение № 2/**, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител.

(4) При неспазването на ограниченията за достъп до личните данни и нарушаване на правилата за обработване на лични данни магистратите и съдебните служители носят дисциплинарна отговорност.

Чл. 16. (1) Документите, преписките и делата, по които работата е приключила, се предават за архивиране в служба „Архив“ на Районен съд - Пловдив.

(2) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в Служба „Архив“, за срокове, съобразени с действащото законодателство и Номенклатурата на делата и документите в Районен съд - Пловдив. Архивохранилището е оборудвано с пожароизвестителна система и пожарогасители, със система за контрол на достъпа и задължително се заключва.

(3) Достъп до архивното помещение на съда имат само съдебните архивари.

(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. 17. (1) Най-малко веднъж годишно се извършва проверка за състоянието и целостта на личните данни, съдържащи се в обработваните от Районен съд – Пловдив 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 Районен съд – Пловдив, която изготвя доклад за резултата от проверката. Докладът трябва да включва и преценка на необходимостта за обработка на личните данни или унищожаване.

Чл. 18. (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. Когато нарушението на сигурността засяга лични данни, които Районен съд – Пловдив обработва в контекста на правораздавателната си дейност, на основание чл. 33 от Регламент /ЕС/ 2016/679 във връзка с чл. 17 ал. 1 от ЗЗЛД, за него следва да бъде уведомен Инспекторатът към Висш съдебен съвет, а ако нарушението засяга лични данни, обработвани от съда за целите на чл. 42 ал. 1 от ЗЗЛД, то уведомяването се извършва на основание чл. 67 ал. 1 от ЗЗЛД, а именно: В случай на нарушение на сигурността на личните данни, което има вероятност да доведе до риск за правата и свободите на субектите на данни, администраторът без излишно забавяне, но не по-късно 72 часа след като е разбрал за нарушението, уведомява комисията, съответно Инспектората, за него. Когато уведомлението е подадено след посочения срок, в него се посочват причините за забавянето.
/Приложение № 3/

Чл. 19. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, Районен съд – Пловдив 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. 20.(1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от Районен съд – Пловдив регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове. **/Приложение № 4/**

(2) В случаите, в които се налага унищожаване на носител на лични данни, Районен съд – Пловдив прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване на 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.

Чл. 21. (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 **(Приложение № 5).** Страните по съдебни дела не подават заявление – Приложение № 5.

(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 предоставена под формата на:

1. устна справка;

2. писмена справка;

3. преглед на данните от самото лице;

4. предоставяне на исканата информация на технически носител;

5. по електронен път.

(4) Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни по образец **(Приложение № 6)**, включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

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

V. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 22. ***Физическата защита*** в Районен съд – Пловдив 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. 23. (1). Основните ***организационни мерки за физическа защита*** в Районен съд – Пловдив 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 или защитени шкафове*, 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. Последните нямат достъп до съхраняваните в електронен вид данни.

(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 Районен съд – Пловдив, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни в Районен съд – Пловдив 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 се знае", с оглед изпълнението на работните им задължения.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени 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. 24. (1). Основните ***технически мерки за физическа защита*** в Районен съд – Пловдив 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, които могат да се заключват*, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават съответните съдебни служители по силата на служебните им задължения.

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

(4) *Пожароизвестителните и пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба. С цел опазване на техническите и информационните ресурси при аварии, произшествия и бедствия /пожар, наводнение и др./ се провеждат съответните мероприятия: периодична проверка на изправността на контакти, ел. инсталациите, ел. таблата, нагревателните и отоплителните уреди в канцелариите и кабинетите на Съдебната палата; забрана за ползване на отоплителни уреди, освен при необходимост и определяне на отговорници в съответните помещения, когато такива се използват; съхраняване на информационните носители в каси или метални шкафове, когато има нормативни изисквания за това. Районен съд - Пловдив предприема превантивни действия при защита на личните данни в случай на природни бедствия. При настъпили критични ситуации правилото е спасяване на човешки живот и последващи действия за опазване и защита на личните данни.

Конкретни действия:

1. Защита от пожари – при задействане на пожароизвестителната система и установяване на пожар, се започва незабавно гасене със собствени средства (пожарогасители) и уведомяване на съответните органи; евакуация на служители и посетители на сградата. Като превантивна мярка за опазване на лични данни, същите е необходимо да се съхраняват в метални шкафове.
2. Защита при наводнения – предприемат се незабавни действия по ограничаване на разпространението; евакуират се служители и посетители; Като превантивна мярка за опазване на лични данни, същите е необходимо да се съхраняват в метални шкафове.
3. При други възможни критични ситуации, служителите работещи с лични данни е необходимо да прилагат по-горе цитираните превантивни мерки.

Чл. 25. (1). Основните ***мерки за персонална защита*** на личните данни, приложими в Районен съд – Пловдив, 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 и настоящите правила. 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 Районен съд – Пловдив;

3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.) 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 такива **/Приложение № 7/**;

2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква такива **/Приложение № 8/** .

Чл. 26. (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 Районен съд – Пловдив, 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 дейността на Районен съд – Пловдив по сключени договори с контрагенти, 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 „Необходимост да се знае"; Регистрите съдържащи лични данни не се изнасят извън сградата на администратора. Никое длъжностно лице или трето лице няма право на достъп до регистрите на лични данни, освен ако данни от същите не са

изискани по надлежен път от органи на съдебната власт. В такива случаи достъпът е правомерен.

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. Личните данни на физически и юридически лица, получени за целите, за които се обработват, се съхраняват съгласно сроковете приети с Номенклатура на делата със срокове за тяхното съхранение в РС - Пловдив.

5. *Процедури за унищожаване* - документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на Районен съд – Пловдив 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), чрез изготвяне на актови протоколи.

(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. 27. (1) ***Защитата на автоматизираните информационни системи и/или мрежи*** в Районен съд – Пловдив 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 Районен съд – Пловдив. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да се 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 Районен съд – Пловдив. Като *външна мрежа* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на Районен съд – Пловдив.

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 Районен съд – Пловдив лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимост да се 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 Районен съд – Пловдив.

3.4.Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на системните администратори. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на

Районен съд – Пловдив, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. *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 системните администратори. Забранено е инсталирането на софтуерни продукти без изричното им одобрение.

4.2.използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от системните администратори или от оторизирани от ръководството на Районен съд – Пловдив 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 – системните администратори проверяват 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 системните администратори 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.

5. 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 Районен съд – Пловдив.

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 имат системните администратори.

5.4.Срокът за съхранение на архивите 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.

6. 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.)

7. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на Районен съд - Пловдив.

8. Данните, които вече не са необходими за целите на Районен съд – Пловдив 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 Районен съд – Пловдив:

1.1.Отдалечен достъп до вътрешната мрежа на Районен съд – Пловдив не е предвиден. По изключение, и след изричната оторизация от ръководството на Районен съд – Пловдив, 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 Районен съд – Пловдив 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 Районен съд – Пловдив. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време след мотивирано становище от

системните администратори, както и в случаите на заплаха за сигурността на данните.

1.3. Публикуването на служебна информация на интернет страницата на Районен съд – Пловдив или в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено от специалист „Информационни технологии“ и системните администратори или след писмена оторизация от Административния ръководител на Районен съд – Пловдив.

2. Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на Районен съд – Пловдив, включват:

2.1. Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на Районен съд – Пловдив 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 Районен съд – Пловдив, 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 оперираш 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. 28. (1) По отношение на личните 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 Районен съд – Пловдив по електронен път или на преносими носители.

Чл. 29. 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.

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

Чл. 30. (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, а работещите с Виртуални машини правят изход от сесия.

(2) 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.

(3) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от Районен съд – Пловдив период, не по-дълъг от 6 месеца, което се изисква от потребителя автоматично. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

Чл. 31. (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. 32. (1) В Районен съд – Пловдив 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 системните администратори. 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. 33. 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.

VII. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 34. (1) В Районен съд – Пловдив се обработват лични данни в следните регистри:

- Регистър „Участници в производства по граждански, административни и изпълнителни дела";
- Регистър „Участници в производства по наказателни дела";
- Регистър „Бюро съдимост";
- Регистър „Финансово-счетоводен";
- Регистър „Кадри";
- Регистър „Конкурси за назначаване на съдебни служители";
- Регистър „Контрагенти";
- Регистър „Възлагане на обществени поръчки по ЗОП";
- Регистър „Производствена практика с Национална търговска гимназия – гр. Пловдив";

- Регистър „Молби, сигнали, жалби и предложения на граждани и организации, извън правораздавателната дейност на Районен съд – Пловдив“;
- Регистър „Искания по ЗДОИ“;

(2) Общо описание на всеки регистър, категориите лични данни, основанието и целта на обработване, субектите на данните, средствата за обработване, лицата/институциите, на които се предоставят и срока за съхраняване се съдържат в Регистър на дейностите по обработване на лични данни в Районен съд – Пловдив.

Чл. 35. Длъжностното лице по защита на личните данни в Районен съд – Пловдив води регистъра на дейностите по обработване на личните данни и регистъра на нарушения на сигурността на личните данни, и го предоставя при поискване на контролните органи.

VIII.АНАЛИЗ НА РИСКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 36. (1) Анализът на риска относно защитата на личните данни се извършва на основание чл. 32, пар.2 от Регламента (ЕС) 2016/679 по отношение на личните данни, обработвани в контекста на правораздавателната дейност, и на основание чл. 66, ал.1 от Закона за защита на личните данни, по отношение на личните данни, които съдът обработва за целите на чл. 42, ал.1 от ЗЗЛД.

(2) Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

(3) Оценка на въздействието е необходимо при:

1. Първоначалното въвеждане на нови технологии;
2. Автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;
3. Обработване на чувствителни лични данни в голям мащаб;
4. Мащабно, систематично наблюдение на публично обществена зона;
5. Други операции по обработване, съдържащи се в списък на надзорния орган по чл. 35, пар. 4 от Регламент (ЕС) 2016/679.

(2) Оценката на риска съдържа най-малко:

1. Системен опис на предвидените операции по обработване и

целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

2. Оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

3. Оценка на рисковете за правата и свободите на субектите на данни;

4.Мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(5) При извършването на оценката на въздействието се иска становището на длъжностното лице по защита на личните данни.

(6)Ако извършената оценката на въздействието покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска, следва да се извърши консултация с Комисия по защита на личните данни преди планираното обработване.

(7) При оценката на въздействието се отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение, която се основава на автоматизирано обработване и на чието основание се вземат мерки, които пораждат правни последици за лицето или го засягат в значителна степен;

2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;

3. лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;

4. лични данни в широко мащабни регистри на лични данни;

5. данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

(8) Определят се следните нива на въздействие:

1. "Изключително високо" - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. "Високо" - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. "Средно" - в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. "Ниско" - в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 37. (1) В зависимост от нивото на въздействие се определя и съответно ниво на защита.

(2) Нивото на защита представлява съвкупност от технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, както и криптографска защита на личните данни.

(3) Нивата на защита са, както следва:

1. при ниско ниво на въздействие - ниско ниво на защита;

2. при средно ниво на въздействие - средно ниво на защита;

3. при високо ниво на въздействие - високо ниво на защита;

4. при изключително високо ниво на въздействие - изключително високо ниво на защита.

Чл. 38. (1) Минималното ниво на технически и организационни мерки, които следва да осигури администраторът е, както следва:

1. при ниско ниво на защита – следните мерки: определяне на помещенията, в които ще се обработват лични данни; определяне на помещенията, в които ще се разполагат елементите на

комуникационно-информационните системи за обработване на лични данни; определяне на организацията на физическия достъп; ключалки; шкафове; оборудване на помещенията; пожарогасителни средства; познаване на нормативната уредба в областта на защитата на личните данни; знания за опасностите за личните данни, обработвани от администратора; съгласие за поемане на задължение за неразпространение на личните данни;определяне на регистрите, които ще се поддържат на хартиен носител;определяне на условията за обработване на лични данни;регламентиране на достъпа до регистрите; определяне на срокове за съхранение; процедури за унищожаване; идентификация и автентификация; управление на регистрите; външни връзки/свързване; защита от вируси; копия/резервни копия за възстановяване; носители на информация; персонална защита; определяне на срокове за съхранение на личните данни;процедури за унищожаване/заличаване/изтриване на носители.

2. при средно ниво на защита - следните мерки: определяне на помещенията, в които ще се обработват лични данни; определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; определяне на организацията на физическия достъп; ключалки; шкафове; оборудване на помещенията; пожарогасителни средства; познаване на нормативната уредба в областта на защитата на личните данни; знания за опасностите за личните данни, обработвани от администратора; съгласие за поемане на задължение за неразпространение на личните данни;определяне на регистрите, които ще се поддържат на хартиен носител;определяне на условията за обработване на лични данни; регламентиране на достъпа до регистрите; определяне на срокове за съхранение; процедури за унищожаване; идентификация и автентификация; управление на регистрите; външни връзки/свързване; защита от вируси; копия/резервни копия за възстановяване; носители на информация; персонална защита; определяне на срокове за съхранение на личните данни;процедури за унищожаване/заличаване/изтриване на носители. определяне на зоните с контролиран достъп; определяне на използваните технически средства за физическа защита; познаване на политиката и ръководствата за защита на личните данни; споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.); обучение; тренировка на персонала за реакция при събития, застрашаващи сигурността на данните. контрол на достъпа до регистрите; правила за размножаване и разпространение; телекомуникации и отдалечен достъп; поддържане/експлоатация; физическа среда/обкръжение; стандартните криптографски възможности на операционните

системи; стандартните криптографски възможности на системите за управление на бази данни; стандартните криптографски възможности на комуникационното оборудване;

3. при високо ниво на защита - мерките по т. 2, както и следните мерки: определяне на режима на посещения; определяне на екип за реагиране при нарушения; оборудване на зоните с контролиран достъп; устройства за контрол на физическия достъп; охрана и/или система за сигурност; средства за защита на периметъра; пожароизвестителни и пожарогасителни системи; детектори за субстанции (метали, взривни вещества и др.); процедури за проверка и контрол на обработването; политика за защита на личните данни, ръководства по защита и стандартни операционни процедури; определяне на роли и отговорности; контроли на сесията; наблюдение; планиране на случайността/непредвидените случаи; управление на конфигурацията; тренировка на персонала за реакция при събития, застрашаващи сигурността на данните; системи за разпределение и управление на криптографските ключове; нормативно определените системи за електронен подпис.

(2) При изключително високо ниво на защита администраторът предприема мерките по т. 3, както и мерки, произтичащи от международни политики за сигурност или актове с международен характер.

Чл. 39. (1) Оценката на въздействието се извърши по критериите „поверителност", „цялостност" и „наличност".

- при нарушаване/неизпълнение на критерий „поверителност", (т.е. при евентуално разкриване на лични данни на неоторизирани лица в процеса на тяхното обработване), това би могло да застраши неприкосновеността на личността и личния живот (ниво „ниско"), както и да засегне интереси, разкриващи здравословното състояние на един или група служители (ниво „средно"). Общото ниво на въздействие за критерий „поверителност" е средно.

- при нарушаване/неизпълнение на критерий „цялостност", (т.е. при евентуална промяна по неоторизиран начин на личните данни в процеса на обработването им и/или изменение или използване на неразрешени манипулации на функциите при обработване на личните данни), това би могло да застраши неприкосновеността на личността и личния живот (ниво „ниско"), както и да засегне интереси, разкриващи здравословното състояние на един или група служители (ниво „средно"). Общото ниво на въздействие за критерий „цялостност" е средно.

- при нарушаване/неизпълнение на критерий „наличност", (т.е. при евентуална невъзможност оторизираните лица да обработват

личните данни и/или невъзможност за бързото им възстановяване при евентуален срив), това би могло да застраши неприкосновеността на личността и личния живот (ниво „ниско“), както и да засегне интереси, разкриващи здравословното състояние на един или група служители (ниво „средно“). Общото ниво на въздействие за критерий „наличност“ е средно.

(2) След извършването на оценка на въздействието върху защитата на личните данни обработващи се в Районен съд – Пловдив се установиха следните нива:

№	Регистър	Ниво на въздействие
1	Регистър „Участници в производства по граждански, административни и изпълнителни дела“	средно
2	Регистър „Участници в производства по наказателни дела”	средно
3	Регистър „Бюро съдимост“	средно
4	Регистър „Финансово-счетоводен“;	средно
5	Регистър „Контрагенти“	средно
6	Регистър „Кадри“	средно
7	Регистър „Конкурси за назначаване на съдебни служители“	средно
8	Регистър „Възлагане на обществени поръчки по ЗОП“	средно
9	Регистър „Производствена практика с Национална търговска гимназия – гр. Пловдив“	средно
10	Регистър „Молби, сигнали, жалби и предложения на граждани и организации извън правораздавателната дейност на Районен съд – Пловдив“	средно
11	Регистър „Искания по ЗДОИ“	средно

(3) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(4) Анализът на риска се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

IX. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 40. Всички съдии и служители в Районен съд – Пловдив 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. 41. Контрол по прилагане на мерките за физическа, персонална и документална защита на личните данни осъществява длъжностното лице по защита на лични данни в Районен съд - Пловдив, а контролът по криптографската защита и защита на автоматизирани информационни системи и мрежи – от системните администратори.

Чл. 42. Надзор и осигуряване спазването на Регламент (ЕС) 2016/679 и Закон за защита на личните данни при обработване на лични данни в Районен съд - Пловдив 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.

Чл. 43. Комисията за защита на личните данни е органът, който наблюдава и осигурява прилагането на правилата за обработване на лични данни от съдилищата в качеството им на „обикновени" администратори (административна дейност), като например: обработването на данни на работещите по щатно разписание на съда, във връзка с трудовите им правоотношения, сключване на договори с контрагенти, провеждане на конкурси за назначаване, финансово-счетоводна дейност.

Чл. 44. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Закона за защита на личните данни, 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 „Декларация за конфиденциалност"

-Приложение № 3 „Уведомление до КЗЛД за нарушаване сигурността на лични данни"

-Приложение № 4 „Протокол за унищожаване на лични данни"

-Приложение № 5 „Искане за достъп до лични данни“

-Приложение № 6 „Споразумение относно условията за обработване на лични данни“

-Приложение № 7 „Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите в РС – Пловдив Вътрешни правила за мерките за защита на личните данни“

-Приложение № 8 „Протокол за проведен инструктаж по противопожарна охрана и безопасност“

-Приложение № 9 – Образец на Регистър на дейностите по обработване на лични данни

-Приложение № 10 – Образец на Регистър на нарушения на сигурността на личните данни

Приложение № 1

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ ОТ СУБЕКТА НА ДАННИТЕ

Долуподписаният/ата....., с адрес: ....., с настоящото декларирам, че давам съгласието си Районен съд – Пловдив да обработва моите лични данни за целите на:

.....

със средства, съобразени с разпоредбите на Общия регламент относно защитата на данните /ЕС/ 2016/679, приложимото право на Европейския съюз и законодателство на Република България относно защитата на личните данни.

Съзнавам, че мога да оттегля моето съгласие по всяко време.

Съзнавам, че оттеглянето на съгласието ми по-късно няма да засегне законосъобразността на обработването, основано на даденото от мен сега съгласие.

Информиран съм, че имам право на информация за събираните от мен данни, за правото на достъп до тях, да искам данните ми да бъдат коригирани или изтрити, да искам обработването на данните ми да бъде ограничено и да възразя срещу определен начин на обработване на личните ми данни.

Дата: .....

Декларатор: .....

/...../

Приложение № 2

Д Е К Л А Р А Ц И Я

Подписаният/та/...../

/трите имена/

на длъжност .....

в Районен съд – Пловдив,

Д Е К Л А Р И Р А М, Ч Е:

1. Ще пазя в тайна личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения, няма да ги разпространявам и няма да ги използвам за други цели, освен за прякото изпълнение на служебните ми задължения.

2. Запознат/а/ съм с нормативната уредба, политиката и ръководствата в областта на защитата на личните данни, Вътрешните правила и Инструкция за мерките и средствата за защита на личните данни, обработвани в Районен съд – Пловдив.

3. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни нося дисциплинарна отговорност по Кодекса на труда, административно – наказателна отговорност по Закона за защита на личните данни и наказателна отговорност, ако деянието осъществява състава на чл. 284 и/или на чл. 319 д от Наказателния кодекс.

Дата..... Декларатор:.....

Приложение № 3

УВЕДОМЛЕНИЕ

до КЗЛД за нарушение на сигурността на личните данни в Районен съд – Пловдив

Описание на естеството на нарушението на сигурността на личните данни /засегнати категории данни, брой на засегнатите субекти, количество засегнати записи/.....
.....
.....
.....

Посочване на името и координатите за връзка на длъжностното лице по защита на данните:

.....
.....

Описание на евентуалните последици от нарушението на сигурността на личните данни:

.....
.....

Описание на предприетите или предложените мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици:

.....
.....

Служител, отговорен за защита на личните данни:.....

/три имена и подпис/

ПРИЛОЖЕНИЕ №4

П Р О Т О К О Л

за унищожаване на лични данни

Днес, ...2019 г., подписаният/ата ..... служител на длъжност:....., упълномощен на основание чл. 20 от Вътрешните правила на Районен съд – Пловдив за мерките за защита на личните данни и/или Заповед на Председателя на РС – Пловдив № ....., да извърша унищожаване на лични данни и носители на лични данни с изтекъл срок на съхранение, част от Регистър с лични данни „.....“, съставих настоящия протокол за унищожаването на лични данни с изтекъл срок за съхранение, включително и резервни копия от тях, както следва:

1. Данни съхранявани на магнитни носители за многократен запис, чрез **трайно изтриване, вкл. презаписването на носителите.**

2. Данни съхранявани на хартиен носител, чрез: **нарязване.**

3. Данни съхранявани на оптични носители за еднократен запис, чрез **физическо унищожаване на носителите:**

Унищожените данни:

Не са обработвани чрез облачни услуги.

Служител:.....

/...../

Приложение № 5

ДО

РАЙОНЕН СЪД - ПЛОВДИВ, като администратор на лични данни

ИСКАНЕ ЗА
ДОСТЪП ДО ЛИЧНИ ДАННИ

От

....., ЕГН/ЛНЧ: ....., с адрес: ....., Личен номер: ....., други идентификационни данни: ....., телефон: ....., електронен адрес: .....

(попълват се толкова данни, колкото са необходими за еднозначно разпознаване на лицето)

Моля, да ми бъде предоставена информация относно личните ми данни, съхранявани в Районен съд – Пловдив, а именно.....
.....
.....
.....
.....
.....
.....

Желая да получа исканата от мен информация в следната форма /желаното се подчертава/:

- преглед на информация;
- устна справка;
- писмена справка;
- копия на технически носител;
- по електронен път.

Дата: .....

Заявител: .....

/имена и подпис/

ПРИЛОЖЕНИЕ № 6

СПОРАЗУМЕНИЕ

относно условията за обработване на лични данни

Днес,..... г., в гр. Пловдив, между:

1. Районен съд - Пловдив, БУЛСТАТ 000471778, с адрес гр. Пловдив, бул. „Шести септември" № 167, представлявано от Иван Георгиев Калибацев – Административен ръководител – Председател и Румяна Иванова Калоферова – главен счетоводител, **като ВЪЗЛОЖИТЕЛ по Договор от.....**, **и**

2..... ....., БУЛСТАТ..... , със седалище и адрес на управление:.....,п редставлявано от.....,к ато **ИЗПЪЛНИТЕЛ** по **Договор от** .....; **наричани заедно „Страните"**

Като взеха предвид, че

1. На .....страните са сключили Договор от..... (Договора), с който ВЪЗЛОЖИТЕЛЯТ е възложил на ИЗПЪЛНИТЕЛЯ извършване на дейности, представляващи дейности по обработване на данни , като обработването се извършва за осъществяване на дефинираните от ВЪЗЛОЖИТЕЛЯ цели:.....

2. Действията по изпълнение на сключения договор представляват дейности по обработка на данни по смисъла на *Общия регламент относно защитата на данните (ЕС) 2016/679*, като в тези отношения ВЪЗЛОЖИТЕЛЯТ има качеството администратор на лични данни, а ИЗПЪЛНИТЕЛЯТ - на обработващ лични данни, и

3. За да уредят помежду си условията за обработване на лични данни и спазване изискванията на *Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателство на Република България относно защитата на личните данни* (за краткост законодателството за защита на личните данни),

Страните се споразумяха за следното:

1. Страните констатират, че по повод извършените до момента действия и действията, които ще бъдат извършвани по сключения между тях Договор от..... , ВЪЗЛОЖИТЕЛЯТ е администратор на лични данни по смисъла на регламент 2016/679, които е предоставил на ИЗПЪЛНИТЕЛЯ за обработка, а

ИЗПЪЛНИТЕЛЯТ е обработващ лични данни по смисъла на Регламент 2016/679 по отношение на данните, предоставени му от ВЪЗЛОЖИТЕЛЯ по силата на договора, относно следните категории субекти на данни:

1.1. Съдии при Районен съд - Пловдив;
1.2. Съдебни служители при Районен съд – Пловдив.

2. Във връзка с обработването на личните данни, предоставени от ВЪЗЛОЖИТЕЛЯ на ИЗПЪЛНИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ, като обработващ данни по смисъла на Регламент 2016/678, има задълженията по чл. 28, пар. 3 от Регламента, като се задължава:

2.1.Да обработва личните данни само по документирано нареждане на АДМИНИСТРАТОРА и единствено за целите, определени от АДМИНИСТРАТОРА.

2.2.Да предприеме и поддържа необходимите технически и организационни мерки за защита срещу неразрешено или незаконосъобразно обработване на личните данни, срещу случайна загуба, унищожаване или повреждане на лични данни, взимайки предвид съвременните технически постижения и разходите за такива мерки, необходими за осигуряването защита, съответстваща на вредите, които такова обработване, загуба, унищожаване или повреждане могат да нанесат и естеството на защитаваните лични данни;

2.3.Да предприеме и поддържа необходимите технически и организационни мерки за осигуряване правата на субектите на лични данни, гарантирани им от законодателството за защита на личните данни;

2.4.В случай на действително или потенциално нарушение на защитата на личните данни да уведоми ВЪЗЛОЖИТЕЛЯ и да предостави цялата информация, необходима на ВЪЗЛОЖИТЕЛЯ за изпълнение на задълженията му за уведомяване на компетентните надзорни органи и засегнатия(те) субект(и) на данни, незабавно, но при всички случаи не по-късно от 24 часа, след като ИЗПЪЛНИТЕЛЯТ е узнал или следва да е узнал за нарушението на защитата на личните данни;

2.5.Да гарантира, че служителите и подизпълнителите, които извършват обработването на лични данни от името на ИЗПЪЛНИТЕЛЯ, са обвързани със задължение за поверителност по отношение на обработването на лични данни и че са преминали необходимото обучение за спазване изискванията на законодателството за защита на личните данни;

2.6.Да поддържа досиета и да съхранява документация за обработените лични данни, категориите извършени дейности по обработване, както и за всяко потенциално посегателство върху лични данни, предоставени по т. 1;

2.7.Да не предава на трети страни лични данни, предоставени по т. 1, без предварително писмено съгласие от

ВЪЗЛОЖИТЕЛЯ/АДМИНИСТРАТОР. Предаването на лични данни на трети страни ще се осъществява само въз основа на писмено споразумение с третата страна, което вменява на последната същите задължения по отношение защитата на личните данни, каквито имат страните по настоящия договор.

2.8.Да не прехвърля извън Европейското икономическо пространство (ЕИП), предоставените й от другата страна лични данни, без предварително писмено съгласие от предоставилата ги страна. В случай на получено съгласие, да гарантира, че прехвърлянето на лични данни извън ЕИП е извършено съобразно законодателството за защита на личните данни;

2.9.След приключване на услугите по обработване да върне на ВЪЗЛОЖИТЕЛЯ/АДМИНИСТРАТОР личните данни:, получени по т. 1, и да заличи съществуващите при себе си копия на данните, освен ако законодателството за защита на личните данни не изисква тяхното съхранение и от ОБРАБОТВАЩИЯ в определен срок след прекратяване на договора;

2.10. Всяка от страните се задължава да информира другата страна за постъпило искане от субект на данни да упражни свои права, съгласно законодателството за защита на личните данни, във връзка с личните данни предадени по т. 1;

3. ОБРАБОТВАЩИЯТ се задължава по всяко време да осигурява достъп на АДМИНИСТРАТОРА до цялата информация, необходима за доказване изпълнението на задълженията на ОБРАБОТВАЩИЯ по законодателството за защита на личните данни във връзка с данните, предоставени по т. 1.

4. По молба на ВЪЗЛОЖИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ се задължава да представи писмени доказателства относно мерките, предприети за спазване на задълженията по настоящото Споразумение и Регламент 2016/679.

5. Отговорност на ИЗПЪЛНИТЕЛЯ/ОБРАБОТВАЩ.

5.1. Ако поради нарушение от страна на ИЗПЪЛНИТЕЛЯ на задълженията му да обработва данните в съответствие с чл. 28, пар. 3 от Регламент 2016/679 и настоящото Споразумение, на ВЪЗЛОЖИТЕЛЯ/АДМИНИСТРАТОР бъде потърсена отговорност и му бъде наложена санкция или ВЪЗЛОЖИТЕЛЯТ/АДМИНИСТРАТОР понесе вреди или бъде осъден да заплати обезщетения на трети лица, ИЗПЪЛНИТЕЛЯТ дължи на ВЪЗЛОЖИТЕЛЯ възстановяване на всички суми, които последният е бил осъден да заплати.

5.2. Всяко нарушение на изискванията за законосъобразно обработване на личните данни в съответствие с настоящото споразумение, е основание за едностранно прекратяване на сключения Договор от .....от страна на ВЪЗЛОЖИТЕЛЯ без предизвестие.

6. Настоящето споразумение е в сила докато ИЗПЪЛНИТЕЛЯТ/ОБРАБОТВАЩ обработва лични данни, получени в изпълнение на Договора по чл.1., независимо дали срокът на договора е изтекъл или не.

ЗА.....: ЗА РС – ПЛОВДИВ:.....

/...../ /...../

ПРИЛОЖЕНИЕ № 7

П Р О Т О К О Л

за преминато обучение по защита на личните данни и инструктаж за приложимите в Районен съд - Пловдив

Вътрешни правила за мерките за защита на личните данни съгласно Регламент 2016/679

Днес,.....2019 г., подписаният/ата/.....
....., с адрес.....
.....,ЕГН.....,
на длъжност.....в Районен съд – Пловдив,

ДЕКЛАРИРАМ, ЧЕ:

1. Ми беше проведено обучение по законодателството по защита на данните и бях запознат с Вътрешните правила на Районен съд - Пловдив за мерките за защита на личните данни, съгласно Регламент 2016/679.

2. Ми беше проведен инструктаж относно правилата за сигурност при обработването на лични данни и съм запознат с прилаганите от Районен съд - Пловдив мерки за физическа, персонална, документална, криптографска защита на личните данни и защитата на автоматизирани информационни системи и мрежи по отношение на регистрите с лични данни, до които имам достъп при осъществяване на трудовата ми функция.

Длъжностно лице
по защита на данните:

/...../

Декларатор:

/...../

ПРИЛОЖЕНИЕ № 8

П Р О Т О К О Л

за проведен инструктаж по противопожарна охрана и безопасност на служителите в РАЙОНЕН СЪД – ПЛОВДИВ, с цел защита на хартиените, техническите и информационните ресурси

Днес, ... 2019 г., подписаният/ата ..... , с адрес: .....,на длъжност.....

ДЕКЛАРИРАМ, ЧЕ:

ми беше проведен инструктаж и съм запознат с прилаганите от Районен съд – Пловдив мерки за противопожарна охрана във връзка с защита на хартиените, техническите и информационните ресурси, съдържащи лични данни, обработвани от Районен съд - Пловдив.

Длъжностно лице
по защита на данните : .....

Декларатор:

Приложение № 9

Администратор на лични данни

РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

на основание чл.30 от Общия регламент относно защитата на данните

Администратор на личните данни:.....

(наименование)

Координати за връзка с администратора:.....

(адрес, електронен адрес)

Длъжностно лице по защита на данните:.....

(име, длъжност, контакти)

Открит на..... г.

Дата	Регистър с лични данни	Цели на обработване	Правно основание	Категории субекти	Категории лични данни	Категории получатели	Предаване в трети държави	Дейности на обработване	Срокове за изтриване	Общо описание на мерките
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)

Приложение № 10

РЕГИСТЪР НА НАРУШЕНИЯ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

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

Образец на декларация за участие в конкурсна процедура

Д Е К Л А Р А Ц И Я

Долуподписаният/та/.....

/трите имена/

Д Е К Л А Р И Р А М:

Съгласен/на съм Районен съд – Пловдив да съхранява и обработва личните ми данни, съгласно изискванията и при спазване на разпоредбите на Закона за защита на личните данни и във връзка с Регламент (ЕС) 2016/679, които предоставям във връзка с подаване на документи за участие в конкурсна процедура.

Известно ми е, че:

- моите лични данни, които съм представил/а на Районен съд - Пловдив в рамките на процедурата по кандидатстване за длъжността....., се обработват от Районен съд – Пловдив за целите на конкурсната процедура.
- информиран/а съм, че Районен съд – Пловдив може да обработва моите лични данни само докато и доколкото това е необходимо във връзка с конкурсната процедура. За обработката извън тези рамки (напр. след приключване на конкурсната процедура) Районен съд – Пловдив се нуждае от моето допълнително съгласие в съответствие с разпоредбите за защита на личните данни.
- заявлението и всички приложени към него документи се съхраняват в Районен съд – Пловдив за срок от шест месеца, считано от момента на приключване на конкурсната процедура;
- при желание, всеки кандидат може да получи обратно комплекта си с документи, преди изтичането на горепосочения срок.

Дата..... Декларатор:.....

гр.....