Р Е П У Б Л И К А Б Ъ Л Г А Р И Я

Р А Й О Н Е Н С Ъ Д – Р А Д О М И Р

УТВЪРДИЛ:
АДМ.РЪКОВОДИТЕЛ- /п/
ПРЕДСЕДАТЕЛ:
/И. Павлова/

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В РАЙОНЕН СЪД - РАДОМИР

Утвърдени със Заповед № 104 /18.04.2019 г. на Административен ръководител-Председател на Районен съд - Радомир

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 Районен съд – Радомир 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 Районен съд – Радомир, юридическо лице на бюджетна издръжка с адрес град Радомир, ул. „Кирил и Методий“ №22, Булстат: 000386858.

(2) Като администратор на лични данни, при обработването на лични данни Районен съд – Радомир 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, Районен съд – Радомир осъществява правораздавателна дейност,

регламентирана в Конституцията на Република България, Закона за съдебната власт, НК, НПК, ГПК 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 Районен съд – Радомир, не изискват или вече не изискват идентифициране на субекта на данните, Районен съд – Радомир 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. Районен съд – Радомир 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. Районен съд – Радомир 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 Районен съд – Радомир и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на Районен съд – Радомир 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 Районен съд – Радомир, 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 Районен съд – Радомир, съобразно възложените им от закона правомощия и нормативно определените им функции, както и обработващи лични данни, на които Районен съд – Радомир 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) Документите, преписките и делата, по които работата е приключила, се предават за архивиране по реда на Вътрешните правила за дейността на учрежденския архив на Районен съд - Радомир.

(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 Районен съд - Радомир. 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. 12. 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 №88/27.04.2016 г.) длъжностно лице.

Чл. 13. (1) Най-малко веднъж годишно се извършва проверка за състоянието и целостта на личните данни, съдържащи се в обработваните от Районен съд – Радомир 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 – Радомир, която изготвя доклад за резултата от проверката. Докладът трябва да включва и преценка на необходимостта за обработка на личните данни или унищожаване.

Чл. 14. (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. 15. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, Районен съд – Радомир 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. 16. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните Районен съд – Радомир 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, Районен съд – Радомир 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.

Чл. 17. (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. Заявлението се вписва в Регистър на исканията (Приложение №2). Страните по съдебни дела не подават заявление – приложение №2.

(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 и/или електронен носител.

(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 №3), 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 – Радомир, 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 Районен съд – Радомир 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 Районен съд – Радомир 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 – Радомир, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни в Районен съд – Радомир 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 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. 20. (1). Основните ***технически мерки за физическа защита*** в Районен съд – Радомир 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 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; заключваеми шкафове 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 Районен съд – Радомир, 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 и Вътрешни правила за използване на информацията и компютърното оборудване в Районен съд – Радомир, утвърдени Заповед № 322/12.11.2018г. на Административния ръководител – Председател на РдРС). 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 – Радомир;
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 Районен съд – Радомир, 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 Районен съд – Радомир, 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 Районен съд – Радомир 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 Районен съд – Радомир 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 – Радомир. 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 Районен съд – Радомир. 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 – Радомир.

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 – Радомир 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 Районен съд – Радомир.

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 Районен съд – Радомир, 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 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 Районен съд – Радомир 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.

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 – Радомир.

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.

6. Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сториджсистема),

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

1.1.Отдалечен достъп до вътрешната мрежа на Районен съд – Радомир не е предвиден. По изключение, и след изричната оторизация от ръководството на Районен съд – Радомир, 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 – Радомир 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 – Радомир. 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 Районен съд – Радомир или в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено от системния администратор или след писмена оторизация от административния ръководител на Районен съд – Радомир.

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

2.1. Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на Районен съд – Радомир 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 – Радомир, 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 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 – Радомир 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) Районен съд – Радомир прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, физическа локация, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност повече от 30 секунди), 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) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от Районен съд – Радомир период, не по-дълъг от 6 месеца. 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 Районен съд – Радомир 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 Районен съд – Радомир регистри с лични данни са:

1. Регистър „Персонал”
2. Регистър „Деловодство”
3. Регистър „Вещи лица и съдебни заседатели“
4. Регистър „Бюро съдимост”
5. Регистър „Входяща и изходяща поща”

VII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 31. Всички съдии и служители в Районен съд – Радомир 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 лицето по защита на лични данни, определено със заповед №103/18.04.2019 г. на Адм.ръководител – Председател на Районен съд гр.Радомир, 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 Районен съд - Радомир 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 „Искане за предоставяне на достъп до лични данни“

Чл. 35. Вътрешните правила са изготвени на 17.04.2019 г. Утвърждават със заповед на Административния ръководител– Председател

на Районен съд – Радомир и се актуализират по реда на тяхното утвърждаване.

Приложение № 1 към чл. 9 от Правилата

ДЕКЛАРАЦИЯ
ЗА
СЪГЛАСИЕ ЗА СЪБИРАНЕ, ИЗПОЛЗВАНЕ И ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Долуподписаният/ата…….....……
…....…..... ЕГН……ЛК №…….издадена на
….....……...от.....…..…....…….....

ДЕКЛАРИРАМ:

Съгласен/а съм **Районен съд – Радомир**, в качеството му на *администратор на лични данни* да събира, съхранява и обработва личните ми данни, които предоставям във връзка с
……..
…….

Запознат/а съм с :

- Целта и средствата на обработка на личните ми данни
- Доброволния характер на предоставяне на данните и последиците от отказа за предоставянето им
- Правото на достъп и коригиране на събраните данни
- Наименованието и адреса на институцията, както и името и длъжността на обработващия данните служител, определени със Заповед на административния ръководител – председател на Районен съд – Радомир

С настоящата декларация декларирам съгласие за съхранение и обработка на личните ми данни при спазване на разпоредбите на Закона за защита на личните данни.

дата: Декларатор:
гр. /подпис/

Приложение № 2 към чл.17, ал.1 от Правилата

ДО
РАЙОНЕН СЪД – РАДОМИР
като администратор на лични данни

ИСКАНЕ ЗА
ДОСТЪП ДО 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, Районен съд гр.Радомир, като администратор на лични данни:

1. На основание чл. 15 от Регламента **да ми предостави достъп** до следните лични данни:….....……..
……
……

2. На основание чл. 16 от Регламента да коригира следните неточни данни / да попълни следните непълни данни:.....
.....
.....

3. На основание чл. 17 от Регламента **да изтрие** следните лични данни:
……
……
……

4. На основание чл. 18 от Регламента **да ограничи обработването** на следните лични данни:……...…….
……...……
……...……

5. На основание чл. 20 от Регламента **да ми предоставите за пренос при друг администратор** следните лични данни:…….....
.....
.....

6. На основание чл. 21 от Регламента **възразявам срещу обработване** на следните лични данни:.....
.....
.....

(Посочват се конкретните основания за искането и данните, за които се отнася)

Дата: ..... Заявител: .....

/имена и подпис/