РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – ГРАД ПЕРНИК

УТВЪРДИЛ:
АДМ.РЪКОВОДИТЕЛ-
ПРЕДСЕДАТЕЛ:
/М.Алексов/

РАЙОНЕН СЪД Република България Г.Р. ПЕРНИК

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В РАЙОНЕН СЪД - ПЕРНИК

Утвърдени със Заповед №578/25.08.2020г., изменени и допълнени със Заповед №1164/29.12.2022г. на Административен ръководител - Председател на РС – Перник

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 – Перник 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 – Перник, юридическо лице на бюджетна издръжка с адрес град Перник, ул. „Търговска“ №37, Булстат: 000386840.

(2) Като администратор на лични данни, при обработването на лични данни Районен съд – Перник 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 – Перник 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 – Перник, не изискват или вече не изискват идентифициране на субекта на данните, Районен съд – Перник 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 – Перник 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 – Перник 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 – Перник и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на Районен съд – Перник 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 от Регламент 2016/679, физическите лица, чиито лични данни се обработват от Районен съд – Перник, 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 – Перник, съобразно възложените им от закона правомощия и нормативно определените им функции, както и обработващи лични данни, на които Районен съд – Перник 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 и служба „Архив“ на Районен съд - Перник.

(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 - Перник. Учрежденският архив е оборудван с пожароизвестителна система и пожарогасител, със система за контрол на достъпа и задължително се заключва.

(3) Достъп до архивното помещение имат само съдебните архивари, и служители от общата администрация, на които са дадени специално права чрез магнитни карти.

(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 системния администратор, 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 длъжностно лице за орган по безопасност и здраве при работа.

Чл. 14./изм. и доп. Зап.№1164/29.12.2022г./ Процедура за докладване и управление на инциденти, в съответствие с чл.33 от Регламент 2016/679 и чл.67 от ЗЗЛД.

(1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, се извършват следните действия:

1.Служителят, констатирал нарушението/инцидента, незабавно докладва на длъжностното лице по защита на данните естеството на нарушението/инцидента и обстоятелствата, при които същото/същия е установен;

2.Длъжностното лице по защита на данните извършва проверка относно докладваното нарушение/инцидент и изяснява подробно в какво се състои нарушението (неразрешено разкриване или достъп до личните данни, унищожаване, загуба, промяна), датата и часа на нарушението, кой е извършителя (ако е възможно да се установи), колко са засегнатите физически лица, какви са възможните неблагоприятни последици и др. Работещите в Районен съд – Перник са задължени да съдействат на ДЛЗД при извършване на проверката;

3. След извършване на проверката ДЛЗД информира писмено административния ръководител за заключението от нея и предлага или предприема в рамките на своите правомощия мерки за прекратяване и/или ограничаване последиците от нарушението/инцидента (вкл. предлага или определя лица, отговарящи за прилагането им);

4. Когато нарушението на сигурността на личните данни има вероятност да доведе до риск за правата и свободите на субектите на данни, ДЛЗД изготвя уведомление съгл. чл. 67, ал. 3 от ЗЗЛД до надзорния орган, което изпраща по e-mail с обратна разписка за доставянето му, както и по пощата на хартиен носител, в срок от 72 часа от узнаването за нарушението/инцидента.

5. Когато нарушението на сигурността засяга лични данни на физически лица, които Районен съд – Перник обработва в контекста на правораздавателната си дейност, то на основание чл. 33 ОРЗД, във връзка с

чл. 17, ал. 1 ЗЗЛД уведомлението за нарушението, изготвено по образец (Приложение №5), се изпраща на компетентния надзорен орган в лицето на Инспектората на ВСС. Във всички останали случаи уведомлението се изпраща на Комисия за защита на личните данни.

6. Когато нарушението на сигурността на личните данни има вероятност да доведе до висок риск за правата и свободите на субектите на данни, ДЗЛД изготвя уведомление до съответните физически лица в срок не по-късно от 7 дни от установяването му. В уведомлението се посочва описание на нарушението и информацията и мерките по чл. 67, ал. 3, т. 2, 3 и 4 ЗЗЛД.

7. Действията по т. 7 не се прилагат, когато е приложена поне една от следните мерки:

- предприети са подходящи технически и организационни мерки за защита, които са приложени по отношение на личните данни, засегнати от нарушението, по начин, който прави личните данни неразбираеми за всяко лице, което няма право на достъп до тях като например криптиране.

- предприети са мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни;

- направено е публично съобщение, с цел да се избегнат непропорционални усилия по уведомяване на множество лица, така че субектите на данни да са в еднаква степен ефективно информирани.

8. Длъжностното лице по защита на данните попълва Регистъра на нарушенията на сигурността на данните (Приложение №4).

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 – Перник 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 – Перник 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 и служба „Архив“.

(2) В случаите, в които се налага унищожаване на носител на лични данни, Районен съд – Перник 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. Всички документи, съдържащи лични данни, се унищожават по начин, непозволяващ тяхното възстановяване.

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 Искане за достъп до данни (Приложение №2) и след тяхното легитимиране. Страните по съдебни дела не подават искане – приложение №2.

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

Чл.18. Администратор, длъжностно лице по защита на данните и регистри с лични данни.

Индивидуализиране на администратора на лични данни, съгласно изискванията на чл.54 от ЗЗЛД.

(1) Администратор на лични данни е Районен съд - Перник, със седалище и адрес на управление: гр. Перник, ул.“Търговска“ №37.

(2) Районен съд - Перник обработва лични данни във връзка с изпълнението на законовите си правомощия, като определя сам целите и средствата за обработването им, при спазване на нормативните актове.

(3) Личните данни се обработват самостоятелно от администратора на лични данни и чрез възлагане на обработващи лични данни.

Чл.19. В качеството си на публичен орган Районен съд - Перник определя длъжностно лице по защита на данните.

(1) Длъжностно лице по защита на личните данни се определя със заповед на Административния ръководител – Председател на Районен съд – Перник.

Чл.20 Длъжностното лице по защита на данните изпълнява следните задачи:

1. информира и съветва администратора и служителите, които извършват обработване, за техните задължения по силата на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз;

2. наблюдава спазването на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз;

3. наблюдава спазването на политиките на администратора по отношение на защитата на личните данни;

4. допринася за повишаване на осведомеността на служителите на Районен съд - Перник, участващи в дейностите по обработване;

5. извършва необходимите проверки за прилагането на изискванията за защита на личните данни в Районен съд - Перник;

6. при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава нейното извършване;

7. произнася се по постъпили искания за упражняване на права от субекти на данни;

8. сътрудничи си с Комисията за защита на личните данни в качеството й на надзорен орган на Република България по всички въпроси, предвидени в Общия регламент относно защитата на данните или произтичащи от други правни актове на Европейския съюз или от законодателството на Република България или по въпроси, инициирани от надзорния орган;

10. в съответствие с чл. 30 от Общия регламент относно защитата на данните води регистър на дейностите по обработване на лични данни в Районен съд - Перник;

11. води регистър за нарушенията на сигурността на данните;

12. води регистър за искания от субекти на данни.

IV. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. Физическата защита в Районен съд – Перник 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. 20. (1). Основните **организационни мерки за физическа защита** в Районен съд – Перник 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 се изграждат прегради и се обособява затворено помещение, в което се извършват дейностите по обработване на лични данни, което е физически ограничено и достъпно

само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения, и преддверие, до което имат достъп външни лица и в което 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 – Перник, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни в Районен съд – Перник 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 се съхраняват в помещения с ограничен достъп, само за упълномощен персонал, а такива съдържащи чувствителни лични данни /като кадрови досиета и др./ се съхраняват в заключени метални шкафове, които също се намират 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. 21. (1). Основните **технически мерки за физическа защита** в Районен съд – Перник включват:

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

4. Видеонаблюдение.

(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. 22. (1). Основните **мерки за персонална защита** на личните данни, приложими в Районен съд – Перник, 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;
2. Запознаване и осъзнаване на опасностите за личните данни, обработвани от Районен съд – Перник;
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 такива обучения;
2. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква такава тренировка.

Чл. 23. (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 – Перник, 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 дейност на Районен съд – Перник, 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 се 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 – Перник 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).
6. *Изготвяне на Политика по сигурност на информацията* - внедряване на подходящи механизми за контрол, които включват политика, процеси, процедури, софтуерни и хардуерни функции.

(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 се 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. 24. (1) **Защитата на автоматизираните информационни системи и/или мрежи** в Районен съд – Перник 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 мрежи, обработващи лични данни, включват:

1. *Идентификация* чрез използване на уникални потребителски акаунти и пароли, както и КЕП за всяко лице, осъществяващо достъп до мрежата и ресурсите на Районен съд – Перник. 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 – Перник. 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 – Перник.

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 – Перник 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 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 – Перник.

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 – Перник, 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 – Перник 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 програми. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират антивирусните програми.

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 – Перник.

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

1.1.Отдалечен достъп до вътрешната мрежа на Районен съд – Перник е предвиден след изричната оторизация от ръководството на Районен съд – Перник, 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.

1.3. Публикуването на служебна информация на интернет страницата на Районен съд – Перник или в интернет пространството, независимо под каква форма и на каква платформа, се извършва единствено от системния администратор или от административния ръководител на Районен съд – Перник.

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

2.1. Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на Районен съд – Перник 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 – Перник, 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. 25. (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.

Чл. 26. 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.

V. Оценка на въздействието върху защитата на данните

Чл. 27. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) 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.

(3) При извършването на оценката на въздействието се иска становището на длъжностното лице по защита на данните.

(4) Оценката на риска съдържа:

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;

(5) 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.

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

Чл. 28. (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 – Перник 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, КЕП, 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 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. 29. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на устойчивост, 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. 30. (1) В Районен съд – Перник 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. 31. 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. 32. Поддържаните от Районен съд – Перник регистри с лични данни са:

1. Регистър „Кадри”- В регистъра се обработват лични данни във връзка с възникване и прекратяване на трудовите правоотношения, при спазване на нормативните изисквания – чл.6, пар.1,б. „б“ и „в“ от ОРЗД (Общ регламент относно защита на личните данни), ЗСВ, ПАС, КТ, КСО, Здравословни и безопасни условия на труд и др.: за постигане на служебни цели; за изготвянето на документи във връзка с трудовото правоотношение (допълнителни споразумения, документи удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др.), документи за прекратяване на трудовите правоотношения с лицата от персонала, заповеди за назначаване, преназначаване и прекратяване на трудовото правоотношение, за повишаване размера на основната месечна заплата, за повишаване на ранга и други документи, необходими за представяне пред различни институции, по искане на служител или държавни институции; за изпращане на кореспонденция във връзка с изпълнение на задължения по сключените със служителите договори, издаване на служебни карти; телефони за връзка с лицата от персонала, данни за здравословното състояние на лицата и други.

1.1. Субектите на лични данни са кандидати за работа, които прилагат към документите си Декларация – съгласие за обработване на лични данни, съгласно Регламент /ЕС/2016/679, както и лицата от персонала: магистрати, държавни съдебни изпълнители, съдии по вписванията и съдебни служители.

1.2. Получатели на личните данни от този регистър са: Държавни органи в съответствие с техните правомощия - органи на съдебната власт, Национална агенция за приходите, Национален осигурителен институт, министерства и други; банки, с оглед изплащане на дължимите възнаграждения на служителите на съда, вещи лица, съдебни заседатели, преводачи и други участници в съдебните дела и на лицата, с които съдът е сключил договор, при изпращане и адресиране на кореспонденция-доставчици на пощенски и куриерски услуги, СТМ.

2. Регистър „Финансово-счетоводна дейност"- В регистъра се обработват лични данни с цел изпълнение на произтичащите законови задължения във връзка с постигане на финансова отчетност. Лични данни се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на лицата от персонала, на трети лица- изпълнители по договори за доставка на стоки и услуги, на вещи лица, преводачи, съдебни заседатели, свидетели и други.

2.1. Субектите на лични данни са лица, работещи в Районен съд- Перник - магистрати, държавни съдебни изпълнители, съдии по вписванията, съдебни служители, трети лица- контрагенти, вещи лица, участници в съдебното производство, съдебни заседатели и други. Лични данни, свързани с физическата идентичност- име, ЕГН, адрес, данни на лична карта, телефон, информация за номер на банкова сметка.

2.2. Получатели на личните данни от този регистър са: лица, предвидени в нормативен акт- различни институции – банки, ВСС, МП, НАП, НОИ, Инспекция по труда и др.

3. Регистър „Управление на граждански, наказателни и изпълнители дела" - В регистъра се обработват лични данни на следните субекти на данни: ищци, ответници, подсъдими, жалбоподатели, тъжители, нарушители по УБДХ, молители в делата по реабилитация, в производствата във връзка с изпълнение на наказанията и искания до съда в досъдебното производство, лицата, по отношение на които се иска прилагане на принудителна медицинска мярка и други участници в съдебния процес. Взискател, длъжник и други участници в изпълнителния процес. Личните данни, които се обработват са: име, данни от лична карта, ЕГН, месторождение, адрес, телефон, образование, трудова дейност, умствено и психическо състояние, имотно състояние, финансово състояние, притежаване на дялове или ценни книжа в други дружества, културни интереси, социален произход, расов произход, етнически произход, политически, религиозни, философски убеждения, информация за номер на банкова сметка на взискателя.

3.1. Получатели на личните данни от този регистър са: лица участници в съдебния процес, ОСВ, разследващи органи, учреждения и ведомства, които по закон имат право да получават такава информация, лица, участващи в изпълнителния процес, НАП, Регистър на банковите сметки и сейфове.

4. Регистър „Съдебни заседатели, вещи лица, адвокати и свидетели“ - Личните данни в този регистър се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на вещи лица, съдебни заседатели, свидетели и други.

4.1. Субектите на лични данни са вещи лица, участници в съдебното производство, съдебни заседатели и други. Личните данни са свързани с физическата идентичност- име, ЕГН, адрес, данни на лична карта, телефон, информация за номер на банкова сметка.

4.2. Получатели на личните данни от този регистър са: служители, работещи в Районен съд – Перник, обработващи лични данни.

5. Регистър „Бюро съдимост” - Личните данни в този регистър се съхраняват в бюлетини за съдимост, обработването им е свързано с наложени на лицата присъди и наказания, при спазване на нормативните изисквания на Наредба №8 за функциите и организацията на дейността на бюрата за съдимост, НПК, НК.

5.1. Субектите на лични данни са лица, родени в района на съда, които са осъдени от български съдилища, освободени от наказателна отговорност от български съдилища, осъдени от чуждестранни съдилища с влязъл в сила съдебен акт. Личните данни са свързани с физическата идентичност- име, ЕГН, месторождение, гражданство, собствено, бащино и фамилно име на майката и бащата на осъденото лице.

5.2. Получатели на личните данни от този регистър са: Съдилища, прокуратура, разследващи органи, органите по ЗЗКИ, учреждения и ведомства, които по закон имат право да получават такива сведения, централен орган за предаване или приемане на информация за съдимост от страна членка на ЕС или съдебни органи на друга държава, по които това е предвидено в международен договор, по който РБ е страна.

VIII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 33. Всички съдии и служители в Районен съд – Перник 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. 34. Контрол по прилагане на мерките за физическа, персонална и документална защита на личните данни осъществява лицето по защита на лични данни, определено със заповед №578/25.08.2020 г. на Адм.ръководител – Председател на Районен съд гр. Перник, а контролът по криптографската защита и защита на автоматизирани информационни системи и мрежи – от системния администратор.

Чл. 35. Надзор и осигуряване спазването на Регламент (ЕС) 2016/679 и Закон за защита на личните данни при обработване на лични данни в Районен съд - Перник 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. 36. 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, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

Чл. 37. Приложения 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“;

- /**изм.Зап.№1164/29.12.2022г.**/ Приложение №3 „Регистър на дейностите по обработване на лични данни в Районен съд – Перник, на основание чл.30 от ОРЗД, респективно чл.62, ал.1 от ЗЗЛД;

- /**нов.Зап.№1164/29.12.2022г.**/ Приложение №4 „Регистър на нарушенията на сигурността на личните данни в Районен съд - Перник;

- /**нов.Зап.№1164/29.12.2022г.**/ Приложение №5 „Уведомление за нарушение сигурността на лични данни съгласно чл. 67, във вр. с чл. 17, ал. 1 ЗЗЛД;

- Политика по сигурност на информацията в Районен съд – Перник;

- Процедура за извършване на оценка на въздействието върху защитата на данните в Районен съд – Перник;

- Информация по чл.54 от Закона за защита на личните данни;

- Въпросник относно дейностите по обработване в РС-Перник на лични данни при управление на човешките ресурси;

- Въпросник относно дейностите по обработване в РС-Перник на лични данни по направление финансово-стопански дейности;

- Въпросник относно дейностите по обработване в РС-Перник на лични данни, свързани с правораздавателната дейност.

Чл. 38. Вътрешните правила са утвърдени със Заповед №578/25.08.2020г., изм.и допълнени със Заповед №1164/29.12.2022г. на Административния ръководител– Председател на Районен съд – Перник.