РЕПУБЛИКА БЪЛГАРИЯ
РАЙОНЕН СЪД – БЛАГОЕВГРАД

УТВЪРДИЛ:……..
ПРЕДСЕДАТЕЛ: ВЕРА КОЕВА

ВЪТРЕШНИ ПРАВИЛА ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В РАЙОНЕН СЪД – БЛАГОЕВГРАД в сила от 05.10.2020 г.

I. ОБЩИ ПОЛОЖЕНИЯ

Нормативни основания
Регламент /ЕС/2016/679 на Европейския парламент и на съвета от 27.06.2019 година 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/ЕО /Общ регламент относно защитата на данните/
Закон за защита на личните данни

Предмет
Тези Вътрешни правила уреждат условията и реда за обработване на лични данни, водене на регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, както и упражняването на контрол при обработването на лични данни

Понятия
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 оже 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 социалната идентичност на това лице;
2.“Обработване на лични дани“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.

Принципи на обработване на лични данни

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 се подходящи, свързани сас 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 целите на обработването;
5.Ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняването 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 или 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 данснси.

Условия за достъп до лични данни

Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача, налагат такъв достъп, при спазване на принципа „необходимо да се знае“ и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, до които са получили достъп при и по повод изпълнение на задълженията си.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Всяко физическо лице, чиите лични данни ще се обработват от администратора, следва да бъде уведомено за:

1.Данните, които идентифицират администратора;

2.Целите на обработването на личните данни и правното основание за обработването;

3.Категориите лични данни, отнасящи се до съответното физическо лице;

4.Получателите или категориите получатели, на които могат да бъдат разкрити данните;

5.Срока за съхранение на личните данни;

6.Информация за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент ЕС/2016/679 – Общия регламентп относно защита на данните/ОРЗД/;

7.Правото на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8.Правото на жалба до надзорен орган –КЗЛД;

9.Източните на данните;

10.Съществуване на автоматизирано вземане на решения, включително профилиране;

Горните изисквания не се прилагат когато обработването е за статистически, исторически или научни цели и предоставянето на данните е невъзможно или изисква прекомерни усилия; вписването или разкриването на данни са изрично предвидени в закон; физическото лице, за което се отнасят данните вече разполага с тазиинформация или е налице изрична забрана за това в закон.

Горната информация се обявява на леснодостъпно място на електронната страница на РС – Благоевград.

II.АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ

Администратор на лични данни е Районен съд – Благоевград със седалище, адрес на управление и адрес за кореспонденция: Благоевград, пл.“Васил Левски“ № 1, работно време от 8.30 до 17.00 часа и електронен адрес: blagoevgrad-rs@justice.bg

Районен съд – Благоевград обработва лични данни във връзка с изпълнението на законовите си правомощия, като сам определя целите и средствата за обработването им, при спазване на относимите нормативни актове.

Длъжностно лице по защита на данните

ОРЗД изключва органите на съдебната власт от задължителните хипотези, при които следва да се определи длъжностно лице по защита на данните. Основната функция на органите на съдебната власт е правораздавателната, а всички останали дейности са съпътстващи я. Именно поради това определянето на длъжностно лице по отношение на съпътстващите дейности на органите е в самостоятелната им преценка.

В случай, че администраторът на лични данни прецени, че е приложимо и необходимо, то определеното от него длъжоностно лице по защита на данните:
1.Информира и съветва администратора и служителите, които извършват обработване, за техните задължения по силата на ОРЗД и на други разпоредби за защита на данни на равнище ЕС или държава членка;
2.Наблюдава спазването на ОРЗД относно защитата на данните и на други разпоредби за защитата на данни на равнище ЕС или държава членка;
3.Наблюдава спазването на политиките на администратора по отношение на защитата на личните данни;
4.Допринася за повишаване осведомеността на служителите в РС – Благоевград, участващи в дейностите по обработване;
5.Извършва необходимите одити/проверки/ за прилагането на изискванията за защита на личните данни в РС – Благоевград.
6.При поискване предоставя съвети по отношение на оценката на въздействие върху защитата на данните и наблюдава нейното извършване;
7.Произнася се по постъпили искания за упражняване на права от субекти на данни;
8.Сътрудничи си с КЗД в качеството й на надзорен орган в РБ по всички въпроси, предвидени в ОРЗД или произтичащи от други правни актове на ЕС или от законодателството на РБ или по въпроси, инициирани от надзорен орган;
9.Действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в ОРЗД, и по целесъобразнот консултира по всякакви други въпроси;
10. В съответствие с чл.30 от ОРЗД води регистър на дейностите по обработване на лични данни в РС – Благоевград.
11.Води регистър за нарушенията на сигурността на данните;
12.Води регистър за искания от субекти на данни.

III.РЕГИСТРИ НА ЛИЧНИ ДАННИ

1.Регистър „Деловодство – участници в съдебните производства“

В регистъра се обработват лични данни на страните по делата, образувани в РС – Благоевград с оглед използването им за служебни цели: за всички дейности, свързани с обработването на делата – изготвяне на документи по

тях/призовки, писма, съобщения и т.н./ и за установяване на връзка с лицата по телефон, на електронен адрес и за изпращане на пощенска кореспонденция.
В регистъра се обработват следните категории лични данни: физическа идентичност – имена, ЕГН, адреси, телефони, ел.адрес; здравен статус на физическите лица; гражданско състояние на физическите лица – семейно положение, данни за наследници и др.
Данните в регистъра се обработват на хартиен и на технически носител.
В деловодството се водят на хартиен носител следните книги: азбучни указатели, описни книги, книги за открити и закрити заседания, книги за привеждане в изпълнение на присъдите, книга за веществите доказателства, книга за получените и върнатите призовки, регистър на съдебните решения по чл.235, ал.5 от ГПК, книга за приемане и отказ от наследство, регистър на изпълнителните листа, регистър на актовете, с които преписката е върната, респ. производството е прекратено и върнато на първоинстнационния съд за поправка на очевидна фактическа грешка, допълване, изменение в частта за разноските на решението или отстраняване на нередовности и за администриране на жалбата.
Данните в регистъра се предоставят от физическите и юридическите лица при входиране на документите във входящия регистър и се въвеждат директно в деловодните програми.
Данните на хартиен носител се съхраняват в сроковете, определени в ПАС по отношение на делата и деловодните книги.
Базата данни от деловодната програма се архивира ежедневно на диск на сървъра на съда и на външен диск. Информацията на външния диск се съхранява при специални условия. Физически дисковете се съхраняват в метална каса, със собствен заключващ механизъм, а помещението в което се съхраняват дисковете е с решетки на прозорците и достъпът до него на външни лица става само в присъствието на работещите в помещението служители.
Администраторът на лични данни предоставя достъп – справки, извлечения, издава документи и извършва други услуги от съответния регистър с лични данни, само на законово основание.
Данните от регистъра се обработват от съдиите и съдебните служители и при спазване на принципа „необходимост да се знае“, като длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните задължения. Всеки служител при започване на работа подписва декларация, която се съхранява в личното му досие.
Оценка на въздействие на регистъра
Ниво на въздействие – поверителност - средно, цялостност - средно, наличност – средно, общо за регистъра – средно.

Оцеката на въздействие се извършва периодично на две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.
При оценка на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – страни по дела, чийто брой надхвърля 2.
В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Деловодство – участници в съдебни производства“ е средно.
Физическа защита – Личните данни се обработват в кабинетите и канцелариите на длъжностните лица и се съхраняват в същите помещения. Помещенията са защитени чрез заключване на вратите и пожарогасителни средства в коридора на сградата. Сградата се охранява от служители на ГД“Охрана“, чрез които се осъществява пропусквателния режим в съдебната палата. Всички помещения, находящи се на партера на съда са с поставени решетки на прозорците.
Външни лица нямат достъп до помещенията, в които се обработват лични данни от регистъра, с изключение на регистратурата и деловодствата, където има обособени входове и сектори за граждани и адвокати, отделени от помещенията на служителите с парапети. Външни лица нямат достъп до частта от помещенията, в които работят съдебните служители, а достъпът на външни лица в тези канцеларии дори само в обособените сектори за външните лица, става само в присъствието на служителите.
Персонална защита – Лицата, обработващи лични данни се запознават със ЗЗЛД, политиката за поверителност и настоящите вътрешни правила.
Споделянето на критична информация между служителите /идентификатори, пароли за достъп и други/ е забранено от политиката за информационна сигурност.
Документална защита - Личните данни се поддържат на хартиен и технически носител. Обработването се извършва от 8.30 до 17.00 часа, като достъп до регистъра имат само длъжностните лица. В извънредни случаи обработването на лични данни може да се извършва и в почивни и празнични дни при полагане на дежурства. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания. Достъпът е ограничен само за упълномощени лица в съответствие с принципа „необходимост да се знае“.
Сроковете за съхранение на документите на хартиен носител от този регистър са определени в ПАС.
Документи с лични данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежен ред от упълномощени лица.

След изтичане на сроковете за съхранение, определени в ПАС и Номенклатурата на делата и документите, съдебните дела, документите и регистрите, съдържащи лични данни се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив, ако не подлежат на предаване в Държавен архив по реда на Закона за държавния архивен фонд.
Защита на автоматизирани информационни системи и мрежи – При работа с данни от регистъра се използва софтуерен продукт - деловодна програма. Данните се въвеждат в база данни и се съхраняват на сървър. Прави се архив на друг твърд диск на същия сървър, като архивите са защитени с пароли. Всеки служител има личен профил /потребителско име и парола/, с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.
Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства /UPS/.
Организационни мерки за гарантиране нивото на сигурност:
Денонощна охрана на сградата от служители на ГД“Охрана“ и видеонаблюдение от служителите на същата дирекция.
Работните конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица.
При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.
Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.
Актовете на съда се публикуват ежедневно на интернет страницата на съда и в ЦУБИПСА, при спазване на ЗЗЛД и ЗЗКИ, като се обезличават личните данни на физическите лица, упоменати в актове.
Действия за защита при аварии, произшествия и бедствия /пожар, наводнение и т.н./ - При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.
Предоставяне на лични данни на трети лица - Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативни задължения / МВР, Прокуратура, следствени органи и други/ при спазване на ЗЗЛД и ЗЗКИ.

2.Регистър „Бюро Съдимост“

Работата на бюрата за съдимост е нормативно регламентирана от Наредба № 8 от 26.02.2008 година за функциите и организацията на дейността на Бюрата за съдимост /Наредбата/.
В регистъра се обработват данни на осъдените лица в съдебните процеси и на техните възходящи – родители, като се обработват лични данни за физическа идентичност – имена, ЕГН, адрес, имена на родители.
Данните от този регистър се използват за служебни цели – за всички дейности, свързани с движението и обработването на делата, изготвяне на справки за съдимост при направени искания от компетентните органи и за издаване на свидетелства за съдимост лично от лицата или от техен пълномощник.
Данните от регистъра се обработват на хартиен и технически носител посредством софтуерен продукт АИС“Бюро съдимост“.
Данните в регистъра се предоставят от съдилищата /бюлетини за съдимост, определения за кумулация, реабилитация и други/ и се въвеждат директно в програмата, посредством която се извършват справките за съдимост и се издават свидетелствата за съдимост.
Данните в регистъра се съхраняват в сроковете, определени в Наредбата.
Администраторът на лични данни предоставя достъп, справки, издава свидетелства за съдимост и други документи, само на законово основание и на упълномощени лица.
За обработка на данните в регистъра се използва софтуерен продукт АИС“Бюро съдимост“, разработен от „Индекс-България- ЛирексБГ“ ООД, който осъществява и следгаранционното обслужване, поддържката и актуализацията на програмата.
Данните се въвеждат в програмата и се съхраняват на сървър. Прави се архив на друг твърд диск на същия сървър, като архивите са защитени с парола. Всеки упълномощен служител има личен профил /потребителско име и парола, с определени съобразно задълженията му права на достъп.Дефинирани са и уникални поребителски имена и пароли за стартиране на операционната система на всеки един компютър.

Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства /UPS/.
Обработването на данните в регистъра се извършва само от съдебните служители, за които е подадена информация в МП, че ще обработват данните от регистъра за съответната календарна година и достъп се предоставя само на тях.
Лицата, обработващи личните данни в Базата на Бюро „Съдимост“ задължително подписват декларация за неразпространение на лични данни, станали им известни по повод изпълнението на служебните им задължения, която се съхранява в личното досие.
Помещението, в което се съхраняват данните от регистъра на хартиен носител /картотека на бюлетините за съдимост/се заключва и е защитено и с метални решетки на прозорците.
Бюлетините за съдимост се съхраняват в метални шкафове – картотеки, с осигурено самостоятелно заключване.
Работните компютърни конфигурации, както и цялата IT инфраструктура, включително достъпът до интернет, се използват само за служебни цели.
При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервиз се извършва без устройствата, на които се съхраняват данните.
Не се разрешава осъществяването на отдалечен достъп до данните в регистъра.
Сроковете за съхранение на данните са определени в Наредбата.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.
Данни от регистъра се предоставят на държавни институции с оглед изпълнение на нормативно задължение / съдилища, прокуратури, органи

на МВР, следствие и т.н./, както и на физически лица, чрез издаване на свидетелства за съдимост.
След изтичане сроковете за съхранение, бюлетините за съдимост и бюлетините по чл.78а НК се унищожават от нарочна комисия по определения в Наредбата начин и след разрешение на ТО "Държавен архив".

3.Регистър „Човешки ресурси"

В регистъра се обработват лични данни на магистрати и съдебни служители, работещи в Районен съд – Благоевград по правоотношения възникнали по силата на ЗСВ /за магистратите/ и по трудови правоотношения /за съдебните служители/.
Събраните данни се използват за служебни цели – за всякакви дейности, свързани със съществуване, изменение или прекратяване на трудовите парвоотношения и на правоотношенията на магистратите по ЗСВ; за изготвяне на всякакви документи на лицата в тази връзка /договори, заповеди, допълнителни споразумения, УП, служебни бележки, удостоверения и други/, за връзка по телефон и изпращане на пощенска кореспонденция; за водене на счетоводна отчетност относно възнагражденията и осигурителните плащания на лицата.
В регистъра се обработват следните категории лични данни: за физическа идентичност – имена, данни от лична карта, ЕГН, адрес, телефон и др.; социална идентичност – данни за образование, квалификации, за трудова дейност и професионална биография; за семейна идентичност – данни за семейно положение – брак, развод, деца и т.н; гражданско правен статус – свидетелства за съдимост; лични данни, свързани със здравето на лицата – медицинско свидителство за започване на работа, решения на ТЕЛК и други.
Данните се обработват на хартиен и технически носител. Автоматизираната обработка се осъществява посредством ПП"Конто" за счетоводството и ПП"Аладин" за човешките ресурси.
Данните се предоставят от физическите лица при започване на работа и се въвеждат в ПП"Аладин", а на хартиен носител се съхраняват в кадровите досиета на съдиите и служителите.
Данните от регистъра се съхраняват в срок от 50 години / кадрови досиета и електронен архив/.
Събраните в регистъра данни се ползват само за дейностите по управление на човешките ресурси, изискуеми се по силата на нормативната уредба, регламентираща трудовите и служебните правоотношения, данъчно-осигурителните правоотношения, счетоводното отчитане, безопасните и здравословни условия на труд, както и социалните въпроси.

Данните се предоставят лично на лицата или на други институции само случаите, когато това е предвидено в закон /НОИ, НАП, Инспекция по труда, ИВСС, СБУТ и други/.
Данните в регистъра се обработват от съдебни служители, в зависимост от длъжностната им характеристика и при спазване на принципа „необходимост да се знае“
Оценка на въздействие на регистъра
Ниво на въздействие – поверителност - средно, цялостност - средно, наличност – средно, общо за регистъра – средно.
За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица, се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва периодично на всеки две години или при промяна в характера на обработваните лични данни и броя на засегнатите физически лица. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – магистрати и съдебни служители, чийто брой надхвърля2.
В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Човешки ресурси“ е средно.
Физически достъп се преодставя само на служителите, чиито служебни задължения включват обработване на този вид лични данни. Данните се обработват в канцелариите на служителите, като данните на хартиен носител /кадровите досиета, ведомости и други/ се съхраняват в метални шкафове /картотеки/ с осигурено самостоятелно заключване, допълнително осигурено постоянно заключване на помещенията, а външни лица имат достъп до тези помещения само в присъствие на служителите. Помещенията, находящи се на партерния етаж се оборудвани с решетки на прозорците, а всички канцеларии в съда се охраняват денонощно от служители на ГД“Охрана“. В коридорите на съда са осигурени пожарогасители.
Лицата, обработващи лични данни на съдиите и съдебните служители се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.
Споделянето на критична информация между служителите /пароли за достъп, идентификатори и други/ е забранено от политиките за информационна сигурност.

След изтичане на сроковете за съхранение, кадровите досиета, ведомостите и други, съдържащи лични данни се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив.
Автоматизираната обработка на данните от този регистър се извършва посредством ПП“Аладин“ и ПП“Конто“. Данните се въвеждат в база данни и се съхраняват на работните компютри, на които се обработват личните данни. Служителите имат лични профили /потребителски имена и пароли/. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки компютър. ПП“Конто“ е инсталирана на сървър на ВСС.
Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система и мрежовите устройства. За защита на данните е инсталирана антивирусна програма. Ежемесечно информацията се архивира и се съхранява на твърдия диск. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства /UPS/.
Работните конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица.
При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервиз се извършва без устройствата, на които се съхраняват данните.
Не се разрешава осъществяването на отдалечен достъп до данните в регистъра за ПП“Аладин“.
Сроковете за съхранение на данните от регистъра е определен в Закона за счетоводството – 50 години.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.
Данните се предоставят лично на лицата или на други институции само случаите, когато това е предвидено в закон /НОИ, НАП, Инспекция по труда, ИВСС, СБУТ, застрахователи, банкови институции и други/.

4. Регистър „Контрагенти“

В регистъра се обработват лични данни на физически и юридически лица, във връзка с дейности, пряко свързани с основната дейност на администратора или във връзка с допълнителни дейности – възлагане на обществени поръчки, сключване на договори за ремонти и т.н. Данните са необходими за изпълнението на сключените договори по реда на ЗЗД, ЗОП, ТЗ и други.

В регистъра се съхраняват само минимални лични данни за индивидуализиране на субектите за сключване на договорите – имена, адреси и телефони.

Данните се предоставят от физическите и юридическите лица и съхраняват само на хартиен носител, като сроковете за съхранение са 5 години от изтичане на договорите и са определени в Номенклатурата за делата със сроковете за съхранение в РС – Благоевград.

Достъп до тази информация имат служителите, отговорни за изпълнение на процедурите по сключване и изпълнение на договорите, при спазване на принципа „необходимост да се знае“ и тези данни се предоставят на трети лица само на законово основание.

Данните се съхраняват в помещение с осигурено постоянно заключване и външни лица имат достъп до помещението само в присъствие на служителите.

Ниво на въздействие: поверителност – средно, цялостност – средно, наличност – средно, общо за регистъра – средно.

Лицата, обработващи лични данни на физически лица – контрагенти, се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.

5.Регистър „Вещи лица, съдебни заседатели, служебни защитници, особени представители, преводачи и други“

В регистъра се обработват лични данни на участници в съдебните производства, извън страните по делата /вещи лица, съдебни заседатели, особени представители, служебни защитници, преводачи и други/, като данните се събират на законово основание за нуждите на счетоводната отчетност и данъчно-осигурителните плащания във връзка с изплатените им възнаграждения.

Данните се предоставят от физическите лица при изплащане на възнагражденията и се въвеждат в ПП“Конто“ и ПП“Аладин“.

В регистъра се събират данни за физическа идентичност на лицата, ЕГН, документ за самоличност, адрес и други.

Данните от регистъра се обработват на хартиен и технически носител.
Данните се съхраняват в сроковете, определени в Закона за счетоводството и след извършен финансов одит.
Администраторът предоставя достъп, справки, извлечения, издаване на документи и други услуги от регистъра лично на лицата или на законово основание.
Данните се обработват от служителите в счетоводството съгласно длъжностната им характеристика и при спазване на принципа „необходимост да се знае“.
Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.
Оценката на нивото на въздействие: поверителност – средно, цялостност – средно, наличност – средно, общо за регистъра – средно.
За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица, се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва периодично на всеки две години или при промяна в характера на обработваните лични данни и броя на засегнатите физически лица. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – вещи лица, съдебни заседатели и други, чийто брой надхвърля 2.
В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Вещи лица, съдебни заседатели, служебни защитници, особени представители, преводачи и други“ е средно.
Личните данни от този регистър се обработват само от упълномощените лица. Всички документи на хартиен носител се съхраняват в стаята на упълномощените лица. За помещението е осигурено постоянно заключване, на прозорците са поставени решетки, в коридора има поставен пожарогасител. Външни лица имат достъп до помещението само в присъствието на упълномощените служители.
Лицата, обработващи лични данни на вещите лица, съдебните заседатели и други участници в съдебния процес, се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.
Споделянето на критична информация / пароли за достъп, идентификатори и други/ е забранено от политиките за информационна сигурност.

Сроковете за съхранение на информацията са определени в Закона за счетоводството и при извършен финансов одит.
Данни от регистъра се предоставят на други институции на законово основание за нуждите на данъчните и осигурителните плащания / НОИ, НАП и други/.
След изтичане на сроковете за съхранение, документите се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив.
Автоматизираното обработване на данните от този регистър се извършва посредством ПП“Конто“ и ПП“Аладин“. Данните се въвеждат в база данни и се съхраняват на работните компютри, където се обработват данните. Упълномощените служители имат лични профили /потребителски имена и пароли/. Дефинирани са и уникално потребителско име и парола за стартиране на операционната система на компютъра. ПП“Конто“ е инсталирана на сървър на ВСС.
Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства.За защита на данните е инсталирана антивирусна програма. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства /UPS/.
Работните компютри, както и цялата IT инфраструктура, включително достъпът до интернет, се използват единствено за служебни цели.
При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервиз се извършва без устройствата, на които се съхраняват данните.
Не се разрешава осъществяването на отдалечен достъп до данните в регистъра до ПП“Аладин“.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.

Данни от регистъра могат да бъдат предоставяни на държавни институции за изпълнение на законови задължения / НАП, НОИ и др./

6.Регистър „Кандидати за работа“.

В регистъра се съхраняват данни на лица, участващи в процедурите по подбор на персонала. Данните се предоставят от физическите лица – кандидати за работа с документите за участие в обявените конкурси.

В регистъра се обработват следните категории лични данни: за физическа идентичност – имена, данни от лична карта, ЕГН, адрес, телефон и др.; социална идентичност – данни за образование, квалификации, за трудова дейност и професионална биография; гражданско правен статус – свидетелства за съдимост; лични данни, свързани със здравето на лицата – медицинско свидителство за започване на работа и други.

Когато в процедурата по подбор се изисква представяне на оригинален документ или нотариално заверени копия на документи, удостоверяващи физическа или психическа годност на кандидата, необходима квалификационна степен и стаж за заеманата длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от приключване на процедурата да получи обратно представените документи. РС – Благоевград връща документите по начина, по който са подадени.

Данните се съхраняват и обработват само на хартиен носител.

Личните данни на всички останали кандидати за работа се съхраняват в сроковете, определени в Номенклатурата на делата със сроковете за съхранение в РС – Благоевград.

След изтичане на сроковете за съхранение, документите на кандидатите за работа се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив.

Администраторът на лични данни предоставя достъп и справки само лично на лицата или на техните пълномощници и не предоставя данни на други лица или институции.

Данните от регистъра се обработват от съдебни служители в зависимост от длъжностните им характеристики и при спазване на принципа „необходимост да се знае“.

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

Документите се съхраняват в хранилището на съда до изтичане на срока за съхранение. За помещението е осигурено постоянно заключване и в същото има пожарогасител. До помещението нямат достъп външни лица.

Оценката на нивото на въздействие: поверителност – средно, цялостност – средно, наличност – средно, общо за регистъра – средно.

За определяне на адекватното ниво на организационните мерки и допустимия вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица, се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва периодично на всеки две години или при промяна в характера на обработваните лични данни и броя на засегнатите физически лица. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – кандидати за работа, чийто брой надхвърля 2.
В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Кандидати за работа“ е средно.
Лицата, обработващи лични данни на кандидатите за работа, се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.

7. Регистър „Искания по ЗДОИ“

В този регистър се обработват лични данни на физически и юридически лица, подали до съда заявления за достъп до обществена информация.
Личните данни са в минимален обем – за физическа идентичност – име, адрес, телефон или електронен адрес за връзка и се предоставят от самите лица.
Данните се обработват от съдебни служители, на които в зависимост от длъжностната характеристика е възложено обработването на заявленията по ЗДОИ, при спазване на принципа „необходимост да се знае“.
Администраторът на лични данни не предоставя тези лични данни на трети лица, освен когато тя отговоря на целите на ЗДОИ.

Данните се събират и обработват само на хартиен носител.
Личните данни се съхраняват в нормативно определените срокове, след което се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив.
Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.
Документите се съхраняват в регистратурата на съда до изтичане на срока за съхранение, съгласно Номенклатурата на делата със сроковете за съхрнение в РС - Благоевград. За помещението е осигурено постоянно заключване и в коридора има пожарогасител. Достъпът на външни лица в помещението се осъществява само в присъствие на служителите.
Оценката на нивото на въздействие: поверителност – средно, цялостност – средно, наличност – средно, общо за регистъра – средно.
За определяне на адекватното ниво на организационните мерки и допустимия вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица, се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва периодично на всеки две години или при промяна в характера на обработваните лични данни и броя на засегнатите физически лица. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – кандидати за работа, чийто брой надхвърля 2.
В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Заявления по ЗДОИ“ е средно.
Лицата, обработващи лични данни на заявителите по ЗДОИ се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител

или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.

8. Регистър „Жалби, сигнали и други искания“

В този регистър се обработват лични данни на физически и юридически лица, подали до съда сигнали, жалби, оплаквания и други в тази насока.

Личните данни са в минимален обем – за физическа идентичност – име, адрес, телефон или електронен адрес за връзка и се предоставят от самите лица.

Данните се обработват от съдебни служители, на които в зависимост от длъжностната характеристика е възложено обработването на тези документи, при спазване на принципа „необходимост да се знае“.

Администраторът на лични данни не предоставя тези лични данни на трети лица, освен ако това не е предвидено в закон.

Данните се събират и обработват само на хартиен носител.

Личните данни се съхраняват в срокевете, определени в Номенклатурата на делата със сроковете за съхранение в РС - Благоевград , след което се унищожават чрез преработка от специализирани фирми и след дадено разрешение от Държавен архив.

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

Документите се съхраняват в общата канцелария на съда до изтичане на срока за съхранение. За помещението е осигурено постоянно заключване и в коридора има пожарогасител. Достъпът на външни лица в помещението се осъществява само в присъствие на служителите.

Оценката на нивото на въздействие: поверителност – средно, цялостност – средно, наличност – средно, общо за регистъра – средно.

За определяне на адекватното ниво на организационните мерки и допустимия вид защита, администраторът извършва оценка на въздействието върху обработваните лични данни. При определяне нивото на въздействие върху конкретно физическо лице или група физически лица, се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва периодично на всеки две години или при промяна в характера на обработваните лични данни и броя на засегнатите физически лица. При оценката на въздействието администраторът отчита характера на обработваните лични данни, които се отнасят до физическата идентичност на група физически лица – кандидати за работа, чийто брой надхвърля 2.

В зависимост от определеното ниско ниво на въздействие, нивото на защита на регистър „Жалби, сигнали и други искания“ е средно.

Лицата, обработващи тези данни се запознават със ЗЗЛД, настоящите правила и други и задължително подписват декларация, с която поемат

задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларациите се съхраняват в досиетата на служителите.
При възникване и установяване на инцидент, незабавно се уведомява административния ръководител или лицето, отговорно за защита на данните, ако е определено такова.
За инцидентите се води дневник, в който се описват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, упълномощеното 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 административния ръководител или лицето по защитата на личните данни, ако е определено такова, като това се отразява в дневника по архивиране и възстановяване на данни.

IV.ПОЛУЧАТЕЛИ НА ЛИЧНИ ДАННИ, ИЗВЪН СТРУКТУРАТА НА РАЙОНЕН СЪД – БЛАГОЕВГРАД

Районен съд - Благоевград разкрива лични данни на физически лица извън собствената си структура, единствено ако има законово основание за това. Категориите получатели на личните данни се определят за всеки конкретен случай според законовото им основание да получат данните, като могат да бъдат:
- държавни органи в съответствие с техните правомощия (например Националната агенция за приходите, Националният осигурителен институт, Висш съдебен съвет, Министерство на правосъдието и други);
- банки с оглед изплащане на дължимите възнаграждения на служителите и др.
- за пощенски и куриерски услуги при адресиране на кореспонденция до физически лица. Документи на хартиен носител се изпращат чрез пощенска услуга, предоставяна на лицензиран пощенски оператор или куриерска служба на собствената администрация.

V.ОБЩИ РАЗПОРЕДБИ

За неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните /ЕС/2016/679, приложимото право на ЕС и законодателството на Република България относно защитата на личните данни – Закона за защита на личните данни и нормативните актове, свързни с прилагането му.