РЕПУБЛИКА БЪЛГАРИЯ
АДМИНИСТРАТИВЕН СЪД - СМОЛЯН

УТВЪРДИЛ,

Административен ръководител – Председател

на Административен съд – Смолян:

Игнат Колчев

…13.06.24… год.

ВЪТРЕШНИ ПРАВИЛА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В

АДМИНИСТРАТИВЕН СЪД – СМОЛЯН

I. ОБЩИ ПОЛОЖЕНИЯ

1.Настоящите вътрешни правила се издават на основание Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 год. 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/, наричан по-нататък „Регламент (ЕС) 2016/679“ и Закона за защита на личните данни (ЗЗЛД) и имат за цел да регламентират механизмите за защита на личните данни, обработвани в Административен съд - Смолян.

2.В Административен съд - Смолян се прилагат организационни и технически мерки за защита, които да гарантират нормативно установените принципи на обработване на лични данни: законосъобразност, добросъвестност и прозрачност; ограничение на целите; свеждане на данните до минимум; точност; ограничение на съхранението; цялостност и поверителност; отчетност.

3.„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.

II. АДМИНИСТРАТОР И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

1.Административен съд – Смолян е **администратор на лични данни** (на основание чл. 4, т. 7 от Регламент (ЕС) 2016/679), които се обработват при или във връзка с осъществяване на възложените му от закона правомощия, по повод дейността на съда и за изпълнението на задължения по договори, по които съдът е страна.

Седалището на администратора и адресът на управление е: гр. Смолян, бул. "България" № 16, етаж 3. На този адрес може да се изпращат по пощата искания до Административен съд – Смолян като администратор на лични данни или лично да се подадат исканията в деловодството на съда – стая № 11 „Справки".

Исканията може да се отправят на e-mail: smolyan-adms@justice.bg или по факс: 0301/8 14 20.

2.Административен съд - Смолян може да обработва личните данни *самостоятелно* или *чрез възлагане на обработващ лични данни.* Обработване на личните 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.Достъпът и обработването на лични данни се осъществява само от лица, чиито служебни задължения (съгласно длъжностна характеристика) или конкретно възложена задача налагат такъв достъп, при спазване на принципа "Необходимост да се знае". Тези лица – магистрати и съдебни служители, действат под ръководството и по указания на администратора на лични данни и са длъжни да познават и прилагат нормативната уредба в областта на защитата на личните данни, настоящите Вътрешни правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в Административен съд - Смолян. Лицата под ръководството на администратора подписват декларация (Приложение № 2) или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при и по повод изпълнение на задълженията си.

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

5.Обработващ лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора – Административен съд - Смолян и е отделно, външно за структурата на администратора – Административен съд - Смолян, лице.

6.Длъжностно лице по защита на данните. Длъжностно лице по защита на данните се определя въз основа заповед за възлагане от административния ръководител на съда. Редът и изискванията за определяне на длъжностно лице по

защита на данните, задълженията и отговорностите му са уредени в чл. 37, чл. 38 и чл. 39 от Регламент (ЕС) 2016/679.

7.Личните данни, обработвани в Административен съд - Смолян се съхраняват съобразно сроковете, определени в Номенклатура на делата със срокове за съхранението им, образувани от дейността на Административен съд - Смолян.

III. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

1. Административен съд – Смолян поддържа в писмена форма, включително и в електронен формат, регистър на дейностите по обработване на лични данни (Приложение № 1), за които отговаря.

2. „Регистър с лични данни" представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител. Достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените лица, в съответствие с принципа на „Необходимост да знае", за да се изпълняват техни задължения.

3. Поддържаните от Административен съд – Смолян **регистри с лични данни са** за:

3.1. Дейности по обработване на лични данни при управлението на човешки ресурси – регистър „ПЕРСОНАЛ"

Цели на обработване:

Лични данни се обработват за индивидуализирането на трудовите правоотношения, при спазване на нормативните изисквания - чл. 6, пар. 1, б. „б" и „в" от Регламента, ЗСВ, ПАС, КТ, КСО, ЗЗБУТ и др.; за постигане на служебни цели; за внасянето на промени - изменения и прекратяване на трудовите правоотношения с лицата от персонала, за изготвянето на документи във връзка с трудовото правоотношение /допълнителни споразумения, декларации, документи удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др./, заповеди за назначаване, преназначаване и прекратяване на трудовото правоотношение, за повишаване ранга и/или индивидуалния размер на основната месечна заплата и други документи, необходими за представяне пред различни институции, по искане на служител или държавни институции; за установяване на връзка с лицата от персонала по телефон; за изпращане на кореспонденция във връзка с изпълнение на задължения по сключените със служителите трудови договори и/или допълнителни споразумения; издаване на служебни карти и др.

Категории субекти на данни:

При управлението на човешки ресурси се обработват лични данни на кандидати за работа и лицата от персонала – магистрати и съдебни служители.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, месторождение, телефон, подпис; с икономическата идентичност - имотно състояние, имущество и интереси; със социалната идентичност - образование, трудова дейност, данни за здравословното и психическото състояние (медицинско свидетелство, удостоверение за психическо състояние, болнични листове), данни за съдимост (свидетелство за съдимост), лични данни на служителите, свързани с гражданството (декларация), психологична пригодност (заключение), данни, свързани с деклариране на липса на несъвместимост (декларация), данни, свързани със семейно положение, родствени връзки, както и данни, свързани с политически неутралитет (декларация).

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни (Служба по трудова медицина), субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, съдебни изпълнители, ВСС, Инспектората към ВСС, НИП и др.

Данните от регистър „Персонал" са служебна информация. Документите на хартиен носител се съхраняват в пълен обем и се подреждат в досиетата на магистратите и съдебните служители. Досиетата на магистратите и на съдебните служители се съхраняват в специален метален, заключващ се шкаф в стая 15 „Административен секретар". Достъп до документите в специалния шкаф има административния секретар.

Документи, съдържащи лични данни, се съхраняват и на електронен носител - компютри, които са защитени с антивирусни програми. Защитата от нерегламентиран достъп до съхраняваните на технически носител лични данни се осъществява чрез индивидуални пароли и нива на достъп на служителите.

При необходимост от пренасяне на документи с лични данни от регистър „Персонал", те се запечатват в плик и се предават чрез:

-призовкари, които ги доставят на адресата срещу подпис;

-изпращане по пощата с препоръчано писмо с обратна разписка;

-куриерска фирма, която ги доставя на адресата срещу подпис.

Административен съд - Смолян, в качеството си на работодател и на администратор на лични данни, определя три годишен срок за съхранение на лични данни на участници в конкурс/процедура по кандидатстване съгласно чл. 343, ал. 2 от ЗСВ, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок. Всеки участник в конкурс/процедура по кандидатстване съгласно чл. 343, ал. 2 от ЗСВ попълва декларация по образец (Приложение № 5). След изтичането на този срок нарочно определена от Председателя на Административен съд - Смолян или оправомощено от него лице комисия изтрива или унищожава съхраняваните документи с лични данни, освен ако специален закон предвижда друго.

Когато в процедурата по набиране и подбор на персонала работодателят е изискал да се представят оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от окончателното приключване на процедурата по набиране и подбор да получи обратно представените документи, освен ако специален закон предвижда друго. Административен съд - Смолян връща документите, по начина, по който са подадени.

3.2. Дейности по обработване на лични данни при осъществяването на финансово-счетоводна дейност

Цели на обработване:

Лични данни се обработват за изпълнение на задълженията, свързани с воденето на счетоводна отчетност, изплащането на възнагражденията на лицата от персонала, на третите лица - изпълнители по договори за доставка на стоки и услуги, на вещи лица, преводачи, свидетели и др.

Категории субекти на данни:

Лица от персонала – магистрати и съдебни служители, трети лица – контрагенти, вещи лица, участници в административното и касационно административно-наказателното производство и др.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, информация за номер на банкова сметка.

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, съдебни изпълнители, ВСС, АДФИ, Сметната палата и др.

3.3 Дейности по обработване на лични данни при изпълнение на правомощията на съда във връзка с административни дела

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на правомощията на съда във връзка с нормативно установените функции и задължения на съда във връзка с производствата по административни дела /ЗСВ, АПК, ПАС и др./

Категории субекти на данни:

Лица по административни дела – жалбоподатели, ищци, ответници, заинтересовани страни, вещи лица, процесуални представители, свидетели и други участници по административните дела, предвидени в АПК и др.

Категории лични данни:

Категориите лични данни, които се обработват са: име; данни по лична карта/паспортни данни; ЕГН; месторождение; адрес; телефон; образование; трудова дейност; семейна идентичност, родствени връзки; данни отнасящи се до здравето, психическо здраве; психическо състояние; умствено състояние; имотно състояние; финансово състояние; участие и/или притежаване на дялове или ценни книжа в други дружества; културни интереси; социален произход; расов произход; етнически произход; политически, религиозни и/или философски убеждения.

Категориите получатели, пред които се разкриват личните данни:

Личните данни се разкриват на субектите на данни и лицата /орган на съдебната власт, физическо или юридическо лице, публичен орган, агенция или друга структура/, предвидени в нормативен акт.

3.4. Дейности по обработване на лични данни при изпълнение на правомощията на съда във връзка с касационни административно-наказателни дела

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на правомощията на съда във връзка с нормативно установените функции и задължения на съда във връзка с производствата по касационни административно-наказателни дела /ЗСВ, НПК, АПК, ЗИНС, ПАС и др./

Категории субекти на данни:

Лица по касационни административно-наказателни дела, участници в съдебното производство – касационни жалбоподатели, ответници, процесуални представители и други участници по касационно наказателно-административните дела, предвидени в АПК и др.

Категории лични данни:

Категориите лични данни, които се обработват са: име; данни по лична карта/паспортни данни; ЕГН; месторождение; адрес; телефон; образование; родствени връзки; трудова дейност; данни отнасящи се до здравето, психическо

здраве; психическо състояние; умствено състояние; имотно състояние; финансово състояние; участие и/или притежаване на дялове или ценни книжа в други дружества; културни интереси; социален произход; расов произход; етнически произход; политически, религиозни и/или философски убеждения.

Категориите получатели, пред които се разкриват личните данни:

Личните данни се разкриват на субектите на данни и лицата /орган на съдебната власт, разследващи органи, физическо или юридическо лице, публичен орган, агенция или друга структура/, предвидени в нормативен акт.

3.5. Регистър „Вещи лица, адвокати и свидетели“

Цели на обработване:

Лични данни се обработват за изпълнение на задълженията, свързани с изпълнението на правомощията на съда във връзка с нормативно установените функции и задължения на съда във връзка с производствата по дела.

Категории субекти на данни:

Лица участници в образуваните пред съда производства. Съхранява лични данни на вещи лица, адвокати и свидетели по делата.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, ЕГН, адрес, данни на лична карта, телефон, информация за номер на банкова сметка и др.

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт - НАП, НОИ, Инспекция по труда, ВСС, АДФИ, Сметната палата и др.

3.6. Регистър на нарушения на сигурността на данните

Регистърът служи за отразяване, описване на нарушенията на сигурността на данни. В регистъра се съдържат данни за: номер, дата и час на установяване на нарушението, описание на нарушението, засегнати субекти на данни – категория/брой, засегнати записи с лични данни (брой записи), възможни последици от нарушението, оценка на нивото на риск за правата и свободите на субектите на данни, предприети мерки, уведомление до надзорния орган (дата/час на изпращане на уведомлението), поетапно уведомяване (ако е приложимо)- дата/час, причини за забавяне изпращането на уведомлението до надзорния орган, съобщение до субектите на данни (ако е приложимо) – дата/час/начин на изпращане на съобщението, отговорно лице.

Относно „Дата и час на установяване на нарушението“ се посочва времето на установяване на нарушението, служителя/служителите, които са установили инцидента и начина на установяването. В случай, че това е възможно, се посочва и времето, в което нарушението е станало факт.

Относно „Описание на нарушението“ се посочва освен описание на инцидента, включващо посочване на това в какво се състои нарушението (унищожаване, загуба, промяна, неразрешено разкриване или достъп до данните) се посочват и лицата (административните звена), които извършват съответните операции и дейности по обработване на данни. Посочва се извършителя/причината, ако е известен/известна.

Относно „Възможни последици от нарушението“ се посочват неблагоприятните последици за физическите лица, които може да породят физически, материални или нематериални вреди, като например: загуба на контрол

върху личните им данни, ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизация, накърняване на репутацията и нарушаване на поверителността на лични данни, защитени от професионална тайна и др.

3.7. Регистър „Декларации по ЗПК"

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на задължението за подаване на декларациите по чл. 49, ал. 1, т. 2 от Закона за противодействие на корупцията (ЗПК) от лицата по § 2, ал. 1, т. 1 от ДР на ЗПК, на които орган по назначаването е Председател на Административен съд - Смолян.

Регистърът се води на основание чл. 56, ал. 1 от ЗПК и § 2, ал. 3 от ДР на ЗПК и съдържа лични данни за служителите в Административен съд - Смолян.

Категории субекти на данни: Лицата по § 2, ал. 1, т. 1 от ДР на ЗПК (служителите в администрацията на органите на съдебната власт, с изключение на служителите, които заемат технически длъжности), на които орган по назначаването е Председател на Административен съд - Смолян.

Категории лични данни:

Лични данни свързани с: физическа идентичност - имена на лицето, единен граждански номер, постоянен адрес, данни от лична карта, телефон; семейна идентичност - имена и единен граждански номер на съпруг/съпруга, на лицето, с което декларatорът се намира във фактическо съжителство, на съпружески начала; данни за ненавършилите пълнолетие деца на декларатора (имена, единен граждански номер, гражданство); данни относно имущественото и финансовото състояние на декларатора; размер на задължения към финансови и кредитни институции; информация за свързани лица и др. Личните данни в регистър „Декларации по ЗПК" се набират чрез подаване на декларации по чл. 49 от ЗПК на хартиен и на електронен носител.

Категориите получатели, пред които се разкриват личните данни:

Обработващи лични данни, субектите на данни, лица, предвидени в нормативен акт.

Регистърът се води на хартиен и на електронен носител.

Хартиените носители на лични данни са поместени в класьори, които се съхраняват от административния секретар в специален метален, заключващ се шкаф в стая 15 „Административен секретар". Достъп до документите в специалния шкаф има административния секретар.

Достъп до хартиените и техническите носители имат лицата, на които Председател на Административен съд - Смолян е възложил воденето на регистрите, приемането и съхраняването на декларации по чл. 49 от ЗПК, както и проверката на съдържанието им.

3.8. Регистър „Инициативи"

Цели на обработване:

Обработването на лични данни е свързано с изпълнението на задължението за участието на съда в реализацията на инициативата на ВСС - Образователната програма „Съдебната власт – информиран избор и гражданско доверие. Отворени съдилища и прокуратури", с цел повишаване правната култура на учениците, както и други провеждани мероприятия или инициативи с участието на представители на съда. Участието на децата в

Образователната програма е доброволно и има съгласие от родителите/настойници, скрепено с попълнени декларации личните данни на децата да бъдат обработвани, използвани и съхранявани от администратора на данни АССм.

Категории субекти на данни:

Лица участници в Образователната програма - провежданите лекции, възстановки, симулативни процеси, които пресъздават работните процеси в съда, както и други участници в провеждани мероприятия или инициативи от съда.

Категории лични данни:

Лични данни, свързани с физическата идентичност - име, адрес и биометрични данни.

Категориите получатели, пред които се разкриват личните данни:

Получените лични данни (биометрични) от направеното аудио и видео заснемане на участниците в Образователната програма са с цел реализирането й в обществен интерес, за популяризиране правораздавателната дейност на съдилищата и повишаване правната култура на учениците.

IV. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ:

1. При събиране на лични данни, администраторът на лични данни предоставя информация на субектите на лични данни в момента на тяхното получаване:

1.1.Данните, които идентифицират администратора и координатите за връзка с него;

1.2.Координатите за връзка с длъжностното лице по защита на данните;

1.3. Целите на обработването, за което личните данни са предназначени, както и правното основание за обработването им;

1.4. Получателите или категориите получатели на личните данни;

1.5. Срока, за който ще се съхраняват личните данни;

1.6. Правото на субекта на данни да изиска достъп, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни или правото да се прави възражение срещу обработването, както и правото на преносимост на данните;

1.7.Правото на субекта на данни да подаде жалба до КЗЛД или до ИВСС;

1.8.Дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключване на договор, както и дали субектът на данните е длъжен да предостави личните си данни или да декларира съгласие за обработването им и евентуалните последствия, ако тези данни или декларацията не бъдат предоставени.

Информация се предоставя в обобщена, кратка и разбираема форма на интернет сайта на Административен съд – Смолян: https://smolyan-adms.justice.bg, раздел „Политика за защита на лични данни“.

2.В случай на нарушение на сигурността на личните данни администратора на лични данни, без излишно забавяне, но не по-късно от 72 часа след като е разбрал за нарушението, е длъжен да уведоми:

- Инспектората към Висшия съдебен съвет за нарушението на сигурността на личните данни при дейностите по обработване на личните данни, свързани с изпълнение на функциите на съда, като орган на съдебната власт - само в пряката, същинска правораздавателна дейност, съгласно чл.17, ал.1 от ЗЗЛД;
- Във всички останали случай при нарушение на сигурността на личните данни уведомява Комисията за защита на личните данни.

Уведомлението до надзорния орган - Инспектората към Висшия съдебен съвет, респективно Комисията за защита на личните данни, трябва да съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

2.1.В уведомлението трябва да се съдържа следното:

а) описание на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните, от което може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

2.2.Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

2.3.Администраторът трябва да документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

3.Жалба от физическо лице срещу администратора на лични данни Административен съд - Смолян, с които съдът има сключени трудови договори и/или допълнителни споразумения за нарушение се подава до Комисията за защита на личните данни.

4.Когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическите лица, администратора на лични данни уведомява и субекта на данните за нарушението на сигурността на личните данни не по-късно от 7 /седем/ дни от установяването му, освен когато:

- са предприети подходящи технически и организационни мерки за защита и тези мерки са приложени по отношение на личните данни, засегнати от нарушението. По-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях - криптиране;
- са взети впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни;
- уведомяването би довело до непропорционални усилия. В този случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да са в еднаква степен ефективно информирани.

5. В уведомлението администратора на лични данни на ясен и разбираем език посочва съгласно чл. 67, ал. 3 от ЗЗЛД най-малко:

- описание на нарушението на сигурността на личните данни, включително когато е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;
- името и координатите за връзка на длъжностното лице по защита на данните или на друго звено за контакт, от което може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

V. ОЦЕНКА НА РИСКА И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ

Оценката на риска се извършва на основата на: естеството, обхвата, контекста и целите на обработването, възможните рискове за правата и свободите на физическите лица и тяхната вероятност и тежест, последиците за правата и свободите на физическите лица.

1. Когато в обхвата на оценката на въздействието попада проблем, при който съществува несигурност свързана с настъпването на сериозни негативни резултати, следва да се направи оценка на риска. Тя е необходима, когато:

1.1. не е налице нулева вероятност, че определено нежелано събитие или развитие ще се прояви;

1.2. не е възможно да се предвиди кои лица или групи ще са засегнати или най-тежко засегнати;

1.3. негативните последици за определени лица, групи, сектори или региони ще бъдат много сериозни и необратими.

2. Оценката на риска включва три стъпки:

2.1.идентифициране на релевантните рискове, при което се прави ясно описание на произхода на риска и естеството на последиците, които той може да има с точното представяне кой и какво би било негативно засегнато, при какви обстоятелства и по какъв начин;

2.2.определяне на вероятността от настъпване и степента на вредите.

2.3.описание на алтернативните начини за ограничаване на идентифицираните рискове.

Оценката на риска се извършва преди започване обработването на данни. Резултатите от оценката на риска се степенуват като нисък, среден и висок риск за съхранението на данните.

При съответната оценка на риска, администратор на лични данни приема една или повече от техническите и организационни мерки на защита, след прилагането на които се извършва нова оценка на риска.

3.Оценката на въздействието е процес, чиято цел е да опише обработването на личните данни, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, като ги оцени и определи мерки за справяне с тези рискове.

VI. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

1.Административен съд – Смолян като администраторът на лични данни осигурява необходимите финансови, технически и човешки ресурси за определянето и въвеждането на подходящи организационни и технически мерки, съответстващи на рисковете с различна вероятност и тежест за правата и свободите на физическите лица.

2.Административен съд - Смолян като администратор на лични данни осигурява подходящи технически и организационни мерки за осигуряване на ниво на сигурност, съобразено с рисковете за правата и свободите на физическите лица.

3.Подходящите технически и организационни мерки се въвеждат към момента на определяне на средствата за обработване и към момента на самото обработване. Задължението за въвеждане на подходящи мерки се отнася до обема на събраните

лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност.

4.Физическа защита:

4.1.Физическата защита в Административен съд - Смолян 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.

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

4.3.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.

4.4.Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в помещения с подходящи мерки за контрол на достъпа до тях само за оправомощени лица.

4.5.Помещенията, в които деловодно се обработват лични данни са оборудвани със заключващи се врати.

4.6.Достъп до помещенията, в които се обработват лични данни, имат определените за целта лица. Външни лица се допускат след прилагане на допълнителни мерки за защита на личните данни.

5. Персонална защита.

5.1.Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае".

5.2.Всички служители са длъжни да спазват ограниченията за достъп до личните данни, и са персонално отговорни пред администратора на лични данни за нарушаването на принципите за „поверителност", „цялостност" и „наличност" на личните данни.

5.3.Лицата, обработващи лични данни под ръководството на администратора, при постъпване на работа се запознават с нормативната уредба в областта на защита на личните данни и актовете по нейното прилагане; опасностите за личните данни, обработвани от администратора; настоящите правила.

5.4.Провеждане на специализирани обучения за работа и опазване на лични данни, в случай, че спецификата на служебните задължения изисква подобно.

5.5.Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай, че спецификата на служебните задължения изисква подобно мероприятие.

5.6.Лицата, обработващи лични данни под ръководството на администратора, задължително подписват декларация (Приложение № 2), с която поемат задължение за неразпространение на лични данни станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител. Подписването на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето.

5.7.Магистратите и съдебните служителите, които имат служебен квалифициран електронен подпис (КЕП) и на които е възложено да подписват документи с КЕП, нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

6. Документална защита

6.1.Документите, съдържащи лични данни, се съхраняват само в помещения с ограничен достъп.

6.2.Обработването на лични данни на хартиен носител се извършва само в работно време, по изключение в извън работно време след разпореждане на административния ръководител.

6.3.Достъп до регистрите с лични данни е ограничен и се предоставя на упълномощени служители, в съответствие с принципа „Необходимост да се знае".

6.4.Контрол на достъпа до регистрите се упражнява от административния ръководител или определено от него длъжностно лице.

6.5.Сроковете за съхранение на данните са определени поотделно за всяка дейност по обработване съгласно Номенклатурата на делата със срокове за съхранение на Административен съд – Смолян.

6.6.За унищожаване на лични данни административният ръководител назначава комисия. Документите, съдържащи лични данни се унищожават по начин, непозволяващ тяхното възстановяване. След унищожаването на документите се съставя протокол, който се представя на председателя за утвърждаване.

6.7.Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители, само ако е необходимо за изпълнение на служебни задължения или ако са изискани по надлежния ред от упълномощени лица.

7.Защита на автоматизирани информационни системи и/или мрежи (АИС/М).

7.1.Личните данни, обработвани в Административен съд - Смолян, подлежат на електронна обработка.

7.2.Електронната обработка се реализира с помощта на специализирани приложни софтуерни продукти и чрез стандартни средства за текстообработка, електронни таблици и др.

7.3.При електронната обработка се използват само лицензирани системни и приложни софтуерни продукти или компютърни програми и бази данни, създадени в

рамките на трудово правоотношение по реда на Закона за авторското право и сродните му права.

7.4.Служителите, обработващи лични данни, задължително трябва да притежават необходимата компютърна грамотност и умение за работа с използваните специализирани софтуерни продукти.

7.5.Всеки упълномощен потребител на АИС/М има личен профил с определени потребителски акаунти и пароли, съобразни с неговите задължения с цел да се регламентират нива на достъп съобразен с принципа „Необходимост да се знае".

7.6.Идентификацията и автентификацията на потребителите се реализира със средствата на операционната система и на използваните специализирани софтуерни продукти чрез потребителско име и парола.

7.7.Сроковете за съхранение на данните са определени съобразно съответната дейност по обработване и в съответствие с утвърдената Номенклатура.

7.8.Заличаването на личните данните в електронен вид се осъществява чрез стандартните средства на операционната система или със средствата на специализираните софтуерни продукти.

7.9.В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията, система за ограничаване на достъпа.

7.10.Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

7.11.Забранено е използването на преносими носители на данни за лични нужди.

7.12.За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

7.13.За поддържането на АИС/М е определен системния администратор на Административен съд – Смолян.

8. Криптографска защита

За криптографска защита се използват стандартните криптографски възможности на операционната система, на системите за управление на бази данни, на комуникационното оборудване, както и квалифицирани електронни подписи (КЕП).

VII. ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.)

1.При възникване и установяване на инцидент, веднага се докладва на административният ръководител и в зависимост от обстоятелства, се уведомяват съответните институции.

2.С наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, ако това е възможно.

3.За инцидентите се води дневник, в който задължително се вписват: пореден номер, 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.

4.В предвидените в Регламента и ЗЗЛД случаи за инцидента се уведомява надзорния орган – Комисията за защита на личните данни.

VIII.ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

1.Лични данни, обработвани от администратора на лични данни, се предоставят на чужди държавни органи единствено в изпълнение на задължения по нормативни актове – изпълнение на съдебна поръчка, договор за правна защита и др. При необходимост от такова предоставяне се спазват разпоредбите на Регламента и настоящите Правила.

2.Данни, обработвани при осъществяване на дейност по управление на човешки ресурси, могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (НОИ, НАП, МВР и др.).

3.В качеството си на работодател, в случаите и по ред, предвидени в закон, административният ръководител предоставят лични данни на персонала и на определени кредитни институции (например банки), във връзка с изплащането на дължимите възнаграждения на магистрати и на съдебни служители, изпълнители по граждански договори, кредитни задължения и др.

IX. ИЗИСКВАНИЯ В ОТНОШЕНИЯТА С ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ (чл.28 от Регламент (ЕС) 2016/679)

1. В случай, че обработването на лични данни се извършва от името на администратора, администраторът на лични данни използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки, с оглед обработване в съответствие с Регламента и при осигуряване на защита на правата на субектите на данни.

2.Отношенията с обработващия лични данни се уреждат с писмен договор или с друг правен акт, задължителен за обработващия, със следните реквизити: предмет и срок на действие на обработването, естество и цел на обработването, вид на личните данни и категории субекти на данни, задължения и права на администратора на лични данни, изисквания при включване на други обработващи лични данни, задължения на обработващия.

X. ПРАВО НА ДОСТЪП

1.Всяко физическо лице има право на безплатен достъп до отнасящи се за него лични данни на основание и по реда на Регламент (ЕС) 2016/679 или на ЗЗЛД в зависимост от целите на обработването.

2.Правото на достъп се осъществява с писмено заявление до Административния ръководител – Председател на Административен съд - Смолян (Приложение № 3). Заявлението се подава лично или от изрично упълномощено лице, чрез нотариално заверено пълномощно, което се прилага към заявлението. Заявление може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронните удостоверителни услуги (ЗЕДЕУС).

3.Информацията може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице. Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по

електронен път, освен в случаите, когато това е забранено от закон. Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

4.Администраторът на лични данни разглежда заявлението за предоставяне на пълна или частична информация, и се произнася в съответните срокове, произтичащи от Регламент (ЕС) 2016/679 или ЗЗЛД според целта на обработването.

5.Администраторът на лични данни отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон или когато са налице други нормативни ограничения.

6.В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът на лични данни е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

XI. РЕД ЗА УНИЩОЖАВАНЕ ИЛИ ЗАЛИЧАВАНЕ НА ЛИЧНИ ДАННИ СЛЕД ПОСТИГАНЕ НА ЦЕЛИТЕ НА ОБРАБОТВАНЕТО

1.Физическото лице има право по всяко време да поиска от администратора на лични данни да изтрие (правото *„да бъдеш забравен"*) или коригира/допълни негови лични данни (Приложение №4), обработването на които не отговарят на изискванията на Регламента, като подаде писмено заявление до Административния ръководител – Председател на Административен съд - Смолян.

2.Когато информацията, съдържа данни, представляващи класифицирана информация, се прилага редът по ЗЗКИ.

3.Унищожаването на личните данни се извършва от комисия, определена по заповед на административния ръководител на съда. За извършените действия комисията съставя протокол и изготвя Акт за унищожаване.

4.Унищожаване на личните данни, образувани от основната дейност на съда по правораздаване се извършва по ред и в сроковете, посочени в нормативните и поднормативните актове уреждащи дейността на съдилищата /ЗСВ, ПАС и др./ и при съблюдаване на разпоредбите на утвърдената Номенклатура на делата със срокове за съхраняването им, образувани от дейността на Административен съд - Смолян, уреждаща процедурата за унищожаване на данните след изтичане на срока за съхранение и контрола за нейното спазване.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1.Контрол по изпълнението на настоящите Вътрешни правила се осъществява от административния ръководител на съда.

§2.Настоящите вътрешни правила отменят Вътрешните правила за защита на личните данни в Административен съд – Смолян, утвърдени със Заповед № 131 от 12.07.2021 год. на Председателя на Административен съд – Смолян, в сила от 12.07.2021 год.

§3.Вътрешните правила за защита на личните данни в Административен съд – Смолян могат да бъдат изменяни и допълвани.

§4.Всички съдебни служители 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.

§5.Вътрешните правила да се публикуват на сайта на съда и във вътрешна мрежова папка „AC-SMOLIAN“ достъпна за всички магистрати и съдебни служители в съда.

Неразделна част от настоящите правила са:

Приложение № 1 - Регистър на дейностите по обработване на лични данни

Приложение № 2 - Декларация

Приложение № 3 - Заявление за достъп до лични дънни

Приложение № 4 - Заявление за допълване/коригиране на лични данни

Приложение № 5 - Декларация за участие в конкурс/процедура по кандидатстване съгласно чл. 343, ал. 2 от ЗСВ

Приложение № 6 - Регистър на нарушения на сигурността на данните