

Утвърдени със Заповед № АЗ- 61/08.05.2019 г.

Председател

Радостин Радков

ВЪТРЕШНИ ПРАВИЛА
на АДМИНИСТРАТИВЕН СЪД СОФИЯ- ГРАД
за мерките за защита на личните данни съгласно Регламент 2016/679

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Правилата при обработване на лични данни в Административен съд София-град са изработени съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 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/, наричан по-нататък „Регламент (ЕС) 2016/679“, Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета, Закона за защита на личните данни.

(2) Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на съдиите, на служителите, включително и участниците в конкурсни процедури в Административен съд София-град /АССГ/, на контрагентите, на страните и техните процесуални представители, както и на всички други групи физически лица, които имат достъп до сградата и помещенията на съда, вкл. и не само с тези, в които АССГ, в качеството му на администратор на лични данни, влиза в отношения при осъществяването на правомощията и дейността си.

Чл. 2. За целите на настоящите правила се ползват следните определения, неизчерпателно изброени:

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“ 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) „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4) „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

5) „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

6) „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

7) „получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

8) „трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

9) „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

10) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба,

промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

Чл. 3 (1) АССГ е юридическо лице на бюджетна издръжка и орган на съдебната власт. АССГ е регистриран по Закона за регистър БУЛСТАТ с БУЛСТАТ: 175200279.

(2) Административен съд София - град е с адрес на седалище в гр. София, район „Възраждане“, ул. „Георг Вашингтон“ № 17.

(3) Административен съд София - град осъществява функциите на орган на съдебната власт, предвидени в Конституцията на Република България, Закона за съдебната власт, Административнопроцесуалния кодекс, Граждански процесуален кодекс, Наказателно-процесуален кодекс и други нормативни актове.

(4) Административен съд София-град, в качеството си на администратор по смисъла на чл. 4, 7) от Регламент (ЕС) 2016/679, обработва лични данни във връзка със своята основна функция – да осъществява правораздавателна дейност, както и във всички останали случаи, в които е страна по възникнали гражданскоправни и публичноправни отношения.

Чл. 5. Административен съд София-град спазва следните принципи, свързани с обработването на лични данни, разписани в глава 2, чл.5 от Регламент (ЕС) 2016/679 - „законосъобразност, добросъвестност и прозрачност“; „ограничение на целите“; „свеждане на данните до минимум“; „точност“; „ограничение на съхранението“; „цялостност и поверителност“; „отчетност“.

Чл. 6. Административен съд София-град организира и предприема мерки за защита на личните данни от нарушения на тяхната сигурност. Предприетите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно, но не и по начин, несъвместим с тези цели.

(2) Личните данни се съхраняват на хартиен и електронен носител, така че да се идентифицира субектът на данните за период, не по-дълъг от необходимото за целите, за които се обработват те – осъществяване на правораздавателните функции на АССГ, сключване на договори в качеството му на работодател и възлагането на обществени поръчки, при взаимоотношения с органи на съдебната, изпълнителната и законодателната власт на Република България, както и всички останали случаи ad hoc или възникнали по силата на закон.

(3) Обработваните лични данни се съхраняват в нормативно определените срокове за всеки вид лични данни и според целта, поради която се обработват, след което се унищожават по ред и правила, разписани по-долу. Личните данни могат да се съхраняват и за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че бъдат приложени подходящите технически и организационни мерки,

предвидени с цел да бъдат гарантирани правата и свободите на субекта на данните.

(4) Обработването на лични данни в регистрите на АССГ по смисъла на чл. 4, 2) от Регламент (ЕС) 2016/679 се извършва в предварително обособени помещения съобразно предвидените мерки за защита и оценката на подходящото ниво на сигурност, така че да се предотвратят или преустановят евентуални нарушения и да се гарантират правата на лицата, чиито данни са обработвани.

Чл. 8. Когато не са налице хипотезите на чл. 6, § 1, б. „б“ – „е“ от Регламент (ЕС) 2016/679, физическите лица, чиито лични данни се обработват от АССГ, подписват декларация за съгласие по образец (**Приложение № 1**).

Чл. 9. При обработването на лични данни лицата имат възможност да реализират следните свои права:

- право на достъп до личните данни, които се обработват от администратора /чл. 15 от Регламент (ЕС) 2016/679/;
- право на коригиране, когато личните данни са непълни или неточни /чл. 16 от Регламент (ЕС) 2016/679/;
- право на изтриване /“право да бъдеш забравен“/, приложимо на някои от посочените по-долу основания: личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин; субектът на данните оттегля своето съгласие и няма друго правно основание за обработването; субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество /чл. 21, § 1 от Регламент (ЕС) 2016/679/; личните данни са били обработвани незаконосъобразно; при спазване на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора и други /чл. 17 от Регламент (ЕС) 2016/679/. Следва да се има предвид, че приоритет пред правото на изтриване има обработването на лични данни, когато е необходимо за упражняване на правото на свобода на изразяването и правото на информация; за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора; по причини от обществен интерес в областта на общественото здраве в съответствие с член 9, § 2, букви з) и и), както и член 9, § 3 от Регламент (ЕС) 2016/679; за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1 от Регламент (ЕС) 2016/679, доколкото съществува вероятност правото да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции;
- право на ограничаване на обработката на личните данни по смисъла на чл. 18 от Регламент (ЕС) 2016/679, изразяващо се във възможността същите да бъдат единствено съхранявани от администратора. Следва да се има предвид изключението по § 2 от този член, че при упражнено право на ограничаване на обработката на личните данни, те могат да бъдат обработени в следните случаи - само със съгласието на субекта на данните; за установяването,

упражняването или защитата на правни претенции; за защита на правата на друго физическо лице; поради важни основания от обществен интерес за Съюза или държава членка;

- право на преносимост на данните, изразяващо се във възможността субектът на данните да получи тези, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и пригоден за машинно четене формат, както и да ги прехвърли на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато: а) обработването е основано на съгласие в съответствие с член 6, параграф 1, буква а) или член 9, параграф 2, буква а) или на договорно задължение съгласно член 6, параграф 1, буква б); и обработването се извършва по автоматизиран начин /чл. 20 от Регламент (ЕС) 2016/679/;
- право на възражение - чл. 21 от Регламент (ЕС) 2016/679;

(2) Администраторът на лични данни може да откаже пълно или частично упражняването на правата на субектите на данни, когато то би създадо риск за: националната сигурност; отбраната; обществения ред и сигурност; предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществения ред и сигурност; други важни цели от широк обществен интерес и по-специално важен икономически или финансов интерес, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност; защитата на независимостта на съдебната власт и съдебните производства; предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регулираните професии; защитата на субекта на данните или на правата и свободите на други лица; изпълнението по гражданскоправни искове.

(3) Субектът на данни упражнява правата си по ал. 1 чрез писмено заявление до администратора на лични данни или по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация, за което е безплатно за субекта. Заявлението съдържа: 1. име, адрес, единен граждански номер или личен номер на чужденец или друг аналогичен идентификатор, или други идентификационни данни на физическото лице, определени от администратора, във връзка с извършваната от него дейност; 2. описание на искането; 3. предпочитана форма за получаване на информация /устна справка; писмена справка; преглед на данните от самото лице; предоставяне на исканата информация на електронен носител/ подпис, дата на подаване на заявлението и адрес за кореспонденция. При подаването на заявление от упълномощено лице към заявлението се прилага и пълномощното.

(4) Решението, с което се удовлетворява или отказва упражняването на правата на лицето, чиито лични данни се обработват, се съобщава в 1-месечен срок от подаване на заявлението в посочената като предпочитана форма за получаване на информация. Във всички случаи на предоставяне на информацията, с изключение „под формата на писмена справка“, следва да бъде съставен протокол, отразяващ извършваните действия, между лицето,

което предоставя исканата информация, или оправомощено от Председателя лице, и лицето, което е упражнило правото си на заявление по ал. 3.

(5) Достъп до обработваните от АССГ лични данни имат при наличие на законово основание следните трети страни – Висш съдебен съвет и Инспектората към него, съд, прокуратура, Национална агенция по приходите, Национален осигурителен институт, Висш адвокатски съвет, Национално бюро за правна помощ, Главна дирекция „Изпълнение на наказанията“, Комисия за противодействие на корупцията и за отнемане на незаконно придобитото имущество, банки и др.

(6) Ако субектът на данни счита, че обработването на лични данни, отнасящи се до него, нарушава правата му по Регламент (ЕС) 2016/679 и по ЗЗЛД, има право да сезира КЗЛД или Инспектората към ВСС или да обжалва актовете и действията на администратора по реда на чл. 38-40 ЗЗЛД.

Чл. 10. (1) Всяко лице, действащо под ръководството на администратора, което има достъп до личните данни, обработва тези данни във връзка със своите служебни функции и не следва да ги разпространява на трети лица. Във връзка с осигуряването на мерки за защита на личните данни Администраторът или оправомощено от него лице провежда първоначален или инцидентен инструктаж на съдиите и служителите на АССГ за запознаване с настоящите правила /протокол, който се подписва собственоръчно от лицето, което ще има достъп до личните данни, и лицето, извършило инструктажа – Приложение № 2/. След прекратяване на правоотношенията с АССГ лицето с достъп до лични данни попълва декларация за конфиденциалност относно обработените от него лични данни, станали му известни при и по повод изпълнение на служебните функции /Приложение № 3, което се подписва собственоръчно от лицето, имало достъп до личните данни/. Декларацията се попълва към датата на прекратяване на правоотношенията и е със срок на действие не по-малко от 2 /две/ години.

(2) Съдиите и служителите от състава на АССГ 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 е основание за налагане на дисциплинарни наказания по отношение на съответните служители.

(3) При обработването на личните данни съдиите от състава на АССГ спазват Кодекса за етично поведение на българските магистрати, а съдебните служители - Етичния кодекс на съдебните служители.

Чл. 11. (1) АССГ, чрез общата и специализираната администрация, поддържа регистри на дейностите по обработване, за които отговоря, в писмена форма и/или в електронен формат,

(2) АССГ поддържа следните регистри:

1. „Счетоводен регистър“, „Счетоводен архив“ и „СБКО“ – чрез звено „Финансова дейност и снабдяване“;

2. регистър „Стопанисване и управление на съдебното имущество“ – чрез звено „Стопанисване и управление на съдебното имущество“;

3. регистър „Човешки ресурси“, съдържащ информация относно трудовите правоотношения на съдиите и съдебните служители и участниците в конкурсни процедури – чрез звено „Човешки ресурси“;

4. регистри „Класифицирана информация“ – чрез служба „Регистратура за класифицирана информация“ в съответствие с изискванията на ЗЗКИ, ППЗЗКИ и други подзаконовни актове в областта на защита на класифицираната информация- чрез регистратура „Класифицирана информация“;

5. регистри и книги, водени от служба „Регистратура“ - входящ дневник; изходящ дневник; разносна книга; регистър на заявленията за достъп до обществена информация; книга по чл. 251, ал. 3 АПК;

6. регистри и книги, водени от служби „Съдебно деловодство“ и „Съдебни секретари“ съобразно изрично разписаните им функции в чл. 37-56 от ПАС - азбучен указател за образуваните административни дела и касационни дела; описна книга; книга за открити заседания; книга за закрити и разпоредителни заседания; регистър на съдебните решения; регистър на изпълнителни листове, издадени за държавни такси и суми, присъдени в полза на съдебната власт; архивна книга.

7. регистър „Архив“ – чрез служба „Архив“ съобразно функциите, посочени в глава X, Част Четвърта от ПАС и Вътрешните правила за дейността на архива в АССГ, утвърдени от Председателя на АССГ;

8. книга за получени и върнати призовки и съдебни книжа- чрез звено „Връчване на призовки и съдебни книжа“;

9. Регистър на декларациите, попълвани от съдебните служители съгласно § 2, т. 1 от ДР на ЗПКОНПИ- чрез звено „Човешки ресурси“;

10. „Видеонаблюдение“, осигурявано от Главна дирекция „Охрана“ към Министъра на правосъдието, достъп до който се осъществява по реда и условията на чл. 12, ал. 3 от настоящите правила.

Забележка: Редът и условията за съхраняването и архивирането на всички документи и книжа, както и сроковете за това, са регламентирани в глава X, Част Четвърта от ПАС, Вътрешните правила за дейността на архива в АССГ, Номенклатурата на делата със срокове за съхраняване в АССГ, при спазването на специалните за това закони и подзаконовни нормативни актове. Обработването на лични данни за целите на Националния архивен фонд на Република България е обработване в обществен интерес, като в тези случаи не се прилагат чл. 15, 16, 18, 19, 20 и 21 от Регламент (ЕС) 2016/679.

(3) Видовете данни, които се обработват от АССГ, са следните /неизчерпателно изброени в зависимост от целта, за която се обработват/:

- физическа идентичност: имена, ЕГН, личен номер на чужденец, данни по документ за самоличност, адрес, телефон, електронен адрес, образ и др.;

- семейна идентичност – членове на семейството, трите имена, ЕГН, адрес и др.;

- социална идентичност: информация за образование, документ за придобито образование, професионална квалификация, за придобита юридическа правоспособност, за владееене на чужди езици, трудов стаж, включително юридически стаж, професионална биография и др.;

- лични данни относно съдебното минало: свидетелство за съдимост и др.;

- данни за здравословно състояние: медицински свидетелства, болнични листове, решения на ТЕЛК/НЕЛК, трудови злополуки и др.;

- икономическа идентичност: възнаграждения и обезщетения, данни относно имотното и финансово състояние на лицето, участието и/или притежаването на дялове или ценни книжа на дружества, данни за банкови сметки и други, изискуеми с оглед преценка на изискванията за съвместимост на заеманата длъжност, вкл. и с цел противодействие с корупцията и др.;

- основни работни данни – длъжност, длъжностна характеристика, месторабота, снимка, работно време, условия за работа и наемане на работа, данни за отпуск и други;

- данни за набиране/подбор при участие в конкурсни процедури - например всички лични данни, съдържащи се в автобиография или резюме, формуляр за кандидатстване, бележки за интервю, документация за проверка и подбор;

- мониторингови данни – данни за пристигане и напускане на сградата на АССГ и на данни за активността в ползваните мрежи и информационни системи от съдиите и служителите от състава на АССГ.

(4) Личните данни от регистрите се обработват с цел изпълнението различни законови задължения на администратора, неизчерпателно изброени:

- управление на човешки ресурси и кадрова обезпеченост на АССГ;
- финансово-счетоводна дейност;
- осигуряване на материално-техническата база и управление на имуществото на съда;
- идентифициране на лицата, които имат достъп до сградата и помещенията в нея, в частност – страните по делата или техни представители;
- осъществяване на правораздавателната дейност;
- осигуряване на достъп до обществена информация по ЗДОИ;
- осигуряване защита на класифицираната информация;
- ефективно противодействие на корупцията и създаване на гаранции, че лицата по § 2, т. 1 ДР на ЗПКОНПИ изпълняват правомощията или задълженията си честно и почтено при спазване на Конституцията и законите;
- охранителна цел.

(5) Право на достъп до водените книги и регистри с лични данни имат съобразно възложените им от закон правомощия служителите на АССГ въз основа на длъжностната им характеристика или чрез изричен акт на Председателя на АССГ, както и всички съдии от състава на АССГ, при спазване на принципа „Необходимост да знае”.

(6) При поискване АССГ осигурява достъп до поддържаните регистри на съответните надзорни органи – Комисията за защита на личните данни и

Инспектората към Висшия съдебен съвет, като се отчете спецификата на осъществявания надзор.

Чл. 12. Особени случаи на обработване на лични данни:

(1) Когато лични данни са предоставени от субекта на данни на АССГ без правно основание или в противоречие с принципите за тяхното законосъобразно обработване, в срок един месец от узнаването администраторът на лични данни ги връща, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването и унищожаването се документират с протокол от нарочно определена от Председателя на АССГ или оправомощено от него лице за това комисия.

(2) В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни КЗЛД или ИВСС, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица по реда и условията на чл. 33 Регламент (ЕС) 2016/679;

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на тяхната сигурност по реда и условията на чл. 34 от Регламент (ЕС) 2016/679;

(3) В сградата на АССГ се осъществява видеонаблюдение от Главна дирекция „Охрана“ към Министъра на правосъдието, която обработва получените лични данни по реда и условията на чл. 391-394 от ЗСВ. Целта на събирането на лични данни е идентифициране на физическите лица, посещаващи сградата на съда и помещения в нея за контрол за достъп.

Записите от техническите средства за видеонаблюдение се съхраняват в регистър „Видеонаблюдение“ в срок от тридесет дни след изготвянето им. Достъп до данните имат определени служители в рамките на изпълняваните от тях служебни функции.

(4) АССГ, в качеството си на работодател и на администратор на лични данни, определя 6-месечен срок за съхранение на лични данни на участници в процедури по набиране и подбор на персонала, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок в декларация по образец /Приложение № 4/. След изтичането на този срок нарочно определена от Председателя на АССГ 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, той връща тези документи на субекта на данни, който не е одобрен за назначаване,

в 6-месечен срок от окончателното приключване на процедурата, освен ако специален закон предвижда друго.

Чл. 13. АССГ прилага защита на личните данни, която включва:

1. Физическа защита – с цел предотвратяване на нерегламентиран достъп и защита на сградата и помещенията в нея, в които се извършват дейности по обработване на лични данни, като се използват сигнално-охранителна система, видеонаблюдение, използване на заключващи механизми, шкафове, метални каси, оборудване с пожароизвестителни и пожарогасителни средства;

2. Персонална защита – по смисъла на чл. 10 от настоящите вътрешни правила;

3. Документална защита – чрез определяне на условията за обработване на лични данни; чрез определяне на регистрите, които ще се поддържат; регламентиране на достъпа до регистрите с лични данни; чрез определяне на срокове за съхранение; процедури за унищожаване;

4. Защита на автоматизирани информационни системи и мрежи – чрез автентикация, използване на уникални потребителски акаунти и пароли; администриране на достъпа до мрежите; защита от зловреден софтуер.

Чл. 14. (1) АССГ въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламент (ЕС) 2016/679, като се отчита най-вече разпоредбата на чл. 25 от Регламент (ЕС) 2016/679 и се вземат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, при извършване на оценка на въздействието дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679.

(2) При обработването на личните данни в АССГ се прилагат следните технически и организационни мерки за осигуряване на съответното ниво на сигурност:

- документите на хартиен носител/електронен носител се съхраняват в кабинетите на Председателя на АССГ, на Заместник-председателите, Съдебния администратор, съдиите, съответните звена или служби от администрацията на АССГ според вида на изпълняваната от тях дейност;
- документи, съставени от служителите на съда се съхраняват на специализирани сървъри, компютърни системи, а в случаи на предоставени от страни по дела външни електронни носители на информация, същите се съхраняват по делата.
- допуска се размножаване и разпространение на лични данни /чрез копиране на хартиен/електронен носител/ в случаите, предвидени в закон или подзаконов нормативен акт, на лица при изпълнение на служебните им или трудови функции /НОИ, НАП и други трети страни/, както и на страните по делата или упълномощени от тях лица;
- комуникационно-информационните системи, използвани за обработка на лични данни, физически се разполагат в специални защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители,

които за изпълнение на служебните си функции се нуждаят от такъв достъп, както и трети лица, натоварени със служебни ангажменти за поддръжката на нормалното функциониране на тези системи, които не са от състава на АССГ;

- помещенията, в които се регистрират, обработват и съхраняват лични данни, не се оставят без надзор, а при излизане на служителите от тях – същите се заключват;
- достъпът до помещенията, в които се регистрират, обработват и съхраняват лични данни, е физически ограничен и контролиран - само за съдии и служители с оглед изпълнение на служебните им функции 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 и съдии, на които е необходимо да имат достъп с оглед изпълнението на служебните им функции, и „публична част“ – до която имат достъп външни лица /страни по водените дела; вещи лица; куриери; участници в конкурси/обществени поръчки; страни по договори и други/ и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител;
- създават се зони с контролиран достъп чрез заключване и/или код, обхващащи ет. 1 /съдебни зали/, ет. 2 и ет. 3 от сградата /работни кабинети/;
- допуска се оторизиран достъп до съответните регистри и книги, съдържащи лични данни, както и до поддържаните информационни системи;
- служителите, на които е възложено да подписват документи с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица;
- създаване на индивидуални акаунти и използване на персонални пароли от съдиите и служителите от състава на АССГ за достъп до служебния компютър, като паролите подлежат на задължителна промяна на всеки шест месеца, както и в случай на нерегламентиран достъп – в момента на установяването.
- в случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват /вкл. и чрез деактивиране или изтриване на акаунта/;
- забранява се предоставянето на персоналните пароли на трети лица, с изключение на случаите на принципа „необходимост да се знае“;
- достъпът до локално споделено /персонално/ пространство се осъществява от съдиите и служителите на АССГ, като модифицирането на данни в него е възможно само от персоналния компютър и от лицето, предоставило достъп до тези данни;
- определя се ниво на достъп до следните WEB базирани системи – Система за случайно разпределение на дела и Система за изчисляване на натовареността на съдиите чрез персонални профили и пароли и КЕП за лицата, на които е разрешен достъпът до тях;

- определя се ниво на достъп до вътрешна Автоматизирана система за управление на делата чрез персонални профили и пароли за лицата, на които е разрешен достъпът до нея;
- предоставена и администрирана безжична мрежа от интернет доставчик , която е напълно отделена от вътрешната мрежа на съда и с регламентиран достъп до нея чрез въвеждане на парола за служителите на АССГ и свободен за посетителите в сградата на съда.
- в зависимост от възложените функции, ограничава се достъпът до външни мрежови ресурси - интернет връзки с трети страни, сегменти на хостинг системи на трети страни.
- администрирането и контролът на мрежи включва контрол на инсталиране на всички устройства и софтуер, включително мрежови устройства и интернет връзки към външни мрежи и други устройства и системи, които могат да позволят достъп до мрежите на Администратора;
- извършване на периодична профилактика на сървърните и персонални компютърни системи, на локалната мрежа, включваща и проверка за зловреден софтуер, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данните, актуализиране на системния софтуер и др.;
- забранено е инсталирането на софтуерни продукти, различни от предвидените за изпълнение на служебните функции.
- забранено е ползване на хардуерни и/или софтуерни инструменти от съдиите и служителите на АССГ, които биха могли да послужат, за да се компрометира сигурността на информационните системи;
- в АССГ се използва единствено софтуер с уредени авторски права, инсталиран от оторизирано за това лице;
- при съмнение или установяване на компрометирана компютърна система работещият с нея е задължен да уведоми оторизираните от АССГ лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразеня компютър /чрез външни носители, електронна поща и/или други способности за електронна обмяна на информация/;
- отдалечен достъп до автоматизираната система за управление на дела не е предвиден да се осигурява, с изключение на случаите на принципа „необходимост да се знае“;
- възможност за установяване лицето, имало неразрешен достъп до регистрите и книгите;
- при регистриране на неправилен достъп до информационните масиви, съдържащи лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, лицето, констатирало това нарушение/инцидент, незабавно докладва за това в писмен вид на председателя или оправомощено от него лице за предприемане на мерките по чл. 33 от Регламент (ЕС) 2016/679;
- въведени са процедури за създаване на архивни копия /ежедневно/ и за възстановяване на данни в състоянието, в което са били преди изгубването или унищожаването;

- архивните копия за възстановяване на данни се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните;
- при въвеждане, промяна или предаване на лични данни да се съхранява информация съобразно вида на данните и начина им на обработване относно: времето (дата и час) на въвеждане, промяна или предаване на личните данни; лицата, извършващи въвеждането, промяната или предаването на личните данни; лицата, на които са предоставени личните данни;
- достъпът до информацията, която се обработва чрез интернет страницата на АССГ, се осъществява съгласно декларацията за поверителност, която е поместена на нея;
- публикуването на съдебните актове в интернет страницата на АССГ се извършва на основание чл. 64 от Закона за съдебната власт, при спазване на изискванията на ЗЗЛД, ЗЗКИ, настоящите вътрешни правила и Правилата за обявяване и публикуване на съдебните актове в АССГ;
- публикуването на информация във връзка с провежданите от АССГ обществени поръчки се осъществява при спазване на изискванията, сроковете и условията на ЗОП, ЗЗЛД, настоящите вътрешни правила, като съдържащите се лични данни на физическите лица се заличават;
- след постигане целта на обработване на личните данни, съдържащи се в поддържаните от АССГ регистри, личните данни, съобразно вида, в който се съхраняват, и след изтичане на сроковете за тяхното архивиране, както и ако не подлежат на такова, следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите вътрешни правила /изтриване и/или физическо унищожаване на носителя на данни/
- извършват се периодични проверки относно спазването на правилата за обработване на лични данни и предприемането на мерки за отстраняване на евентуални нарушения;
- предприемане на специални мерки в случай на аварии, произшествия и бедствия /пожар, наводнения и др./;
- всички съдии и служители на АССГ са длъжни да спазват програмата за начален инструктаж, правилата за осигуряване на здравословни и безопасни условия на труд, вкл. и за противопожарна безопасност и безопасна работа на неелектрическия персонал при експлоатация на електрически уреди, машини, апарати и съоръжения до 1000W, за което преминават съответния инструктаж съобразно утвърдени от Председателя на АССГ вътрешни правила и инструкции.

VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. Всички съдии и служители от състава на АССГ са длъжни спазват ежедневно при изпълняване на заеманата от тях длъжност и възложените им служебни функции и настоящите вътрешни правила.

Чл. 35. За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

Приложения:

- **Приложение № 1** – декларация за съгласие;
- **Приложение № 2** – протокол;
- **Приложение № 3** – декларация за конфиденциалност;
- **Приложение № 4** – декларация на участниците в конкурсни процедури.

Настоящите вътрешни правила са утвърдени със заповед на Председателя на Административен съд София-град на основание чл. 25и от Закона за защита на личните данни.

Настоящите вътрешни правила отменят Правила за минималното ниво на технически и организационни мерки за сигурност, които са задължителни за магистратите и служителите, оторизирани с достъп до регистри с лични данни в Административен съд София-град, влезли в сила от 30.12.2008 г.