



РЕПУБЛИКА БЪЛГАРИЯ  
СОФИЙСКИ РАЙОНЕН СЪД

**ЗАПОВЕД**

**№ AC – 571**

*гр. София, 07.12.2021г.*

На основание чл.80, ал.1, т.1 от Закона за съдебната власт във връзка със задължението на Софийски районен съд да осигури организационна и техническа защита при обработване и съхраняване на лични данни и да гарантира правата на субектите на лични данни в съответствие с изискванията на 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/EО (Общ регламент относно защитата на данните), Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. 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 наказателни санкции и относно свободното движение на такива данни за отмяна на Рамково решение 2008/977/ПВР на Съвета и Закона за защита на личните данни,

**НАРЕЖДАМ:**

**1. УТВЪРЖДАВАМ „ПРАВИЛА за мерките и средствата за защита на личните данни, обработвани в Софийски районен съд“.**

**2. ВЪЗЛАГАМ** на системните администратори от отдел „Информационно обслужване“ да публикуват настоящата заповед и утвърдените с нея правила на интернет страницата на съда и на служебната страница на съда, раздел „Документи“ – „Вътрешни правила“.

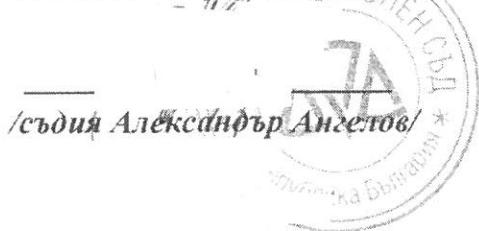
**3. ВЪЗЛАГАМ** контрола по изпълнение на заповедта на съдебния администратор на Софийски районен съд.

*Заповедта и приложените към нея Вътрешни правила да се сведе до знанието на всички съдии и служители в СРС чрез публикуването ѝ във вътрешната компютърна мрежа на съда.*

*Препис от заповедта и приложените към нея правила да се връчи срещу подпись на съдебния администратор, началник от дел „Информационно обслужване“, служителите в сектор „Правно обслужване“ – за сведение и изпълнение.*

*Председател на Софийски районен съд:*

*/съдия Александър Ангелов/*



# **ПРАВИЛА ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ОБРАБОТВАНИ В СОФИЙСКИ РАЙОНЕН СЪД**

## **РАЗДЕЛ I Общи положения**

### **Предмет**

**Чл.1.(1)** Настоящите 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, разпределението на дейностите и отговорностите на длъжностните лица, както и упражняването на контрол при обработването на лични данни в Софийския районен съд (CPC).

**(2)** В зависимост от конкретната ситуация, CPC може да обработва данни в качеството на администратор или на обработващ. Седалището на CPC е гр. София, бул. „Ген.М.Д.Скобелев“ № 23. Адресът за кореспонденция и контакт във връзка с администрирането и/или обработката на лични данни е:

град София, п. код 1612, бул. „Цар Борис III“ № 54,  
работно време: понеделник - петък, 09:00 часа - 17:00 часа,  
електронна поща: [srs@justice.bg](mailto:srs@justice.bg).

**(3)** Настоящите правила са изгответи в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. (Общ регламент относно защитата на данните, ОРЗД), Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. (Директивата) и Закона за защита на личните данни (ЗЗЛД).

**Чл.2.** Използваните при изготвяне на настоящите правила понятия имат значението по чл.4 ОРЗД, в частност и следното значение:

1. „длъжностно лице по защита на данните“ – съдебен служител на CPC, определен съобразно чл.37 и сл. ОРЗД;

2. „обработващ лични данни“ – магистрати и съдебни служители в CPC, които обработват лични данни, предоставени и/или изискани с цел изпълнение на чл.6, ал.1, б. „б-д“ ОРЗД;

3. „„обработване на данни“ – всяка дейност, извършвана с лични данни или набор от лични данни;

4. „псевдонимизиране“ – заместване на лични данни (информация), която идентифицира пряко или непряко субект на данни, с един или повече идентификатори („псевдоними“), така че лицето да не може да бъде идентифицирано без достъп до допълнителна информация, която се съхранява отделно и е предмет на технически и организационни мерки с цел гарантиране нейната поверителност.

### **Субекти на данни и категории лични данни**

**Чл.3.(1)** Софийски районен съд събира и обработва лични данни, необходими за осъществяване на своите права и задължения като работодател, както и като орган на съдебната власт, в изпълнение на функции, възложени му със закон. Обработваните лични данни се групират в следните категории:

- „Управление на човешки ресурси“;
- „Правораздавателна дейност“;
- „Доставчици на услуги, контагенти“;
- „Бюро съдимост“;
- „Лица, подали молби, жалби, предложения, сигнали и искания до председателя на CPC“.

**(2)** В изпълнение на законовото си задължение относно лицата, полагащи трудова дейност в СРС (съдии, съдии по вписванията, съдебни изпълнители и съдебни служители) и кандидатите за работа, се събират и обработват следните лични данни:

а) физическа идентичност: имена, ЕГН, номер на лична карта/паспорт, дата и място на издаване, постоянен и/или настоящ адрес, телефон, електронна поща и други;

б) социална идентичност: данни относно образование, трудов опит, професионална и лична квалификация, умения;

в) семейна идентичност: данни относно семейното положение на лицата (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години);

г) икономическа идентичност: данни относно имотното и финансово състояние на лицата;

д) лични данни относно съдебното минало (наличие на осъждане за престъпление и/или административно нарушение) на лицата: свидетелство за съдимост;

е) данни за здравословното състояние на лицата: медицинско свидетелство, удостоверение за психично състояние, болнични листове, експертни решения на ТЕЛК и всяка прилежаща към тях документация;

ж) други данни, чието обработване е необходимо за изпълнение на правата и задълженията на СРС като работодател.

**(3)** Относно лицата, участници в съдебните производства или явяващи се по дела, в т.ч. веществите лица, съдебните заседатели, особените представители, свидетелите по делата, с оглед естеството на участиято им се събират и обработват данни, свързани с физическата идентичност, икономическата идентичност, социална идентичност, семейна идентичност, данни за съдебното минало и/или данни относно здравословното състояние.

**(4)** Относно доставчиците на услуги и контрагентите на СРС, в т.ч. по обществени поръчки и тръжни процедури, се събират, обработват и съхраняват лични данни, необходими за провеждането на процедурите, сключването и изпълнението на договорите, свързани с физическата идентичност. Специални категории данни (лични данни относно наличие на осъждане за престъпление и/или административно нарушение, социална идентичност и др.) се събират, обработват и съхраняват само доколкото е необходимо за сключването и изпълнението на процедурата/сделката.

**(5)** Относно регистър „Бюро съдимост“, обработването на лични данни, свързани с наличие на осъждане за престъпление и/или административно нарушение, се обработват по искане на лицата, по отношение на които е постановена присъда или акт за извършено нарушение или по искане на орган, компетентен по силата на нормативен акт.

**(6)** Относно лицата, подали молби, жалби, предложения, сигнали и искания до председателя на СРС, се обработват и съхраняват лични данни, които самите лица са преценили, че следва да представят. Данните се обработват с цел изпълнение на законови задължения на СРС, като използването им е ограничено само за служебни цели. Обработката и предоставянето на информация във връзка с отправени заявления по Закона за достъп по обществена информация се извършва само и доколкото тя отговаря на целите на ЗДОИ.

### **Цели и принципи на обработване на личните данни**

**Чл.4.(1)** Софийски районен съд събира, обработва и съхранява лични данни със следните цели:

1. управление на човешките ресурси, изплащане на трудовите възнаграждения и свързаните с това задължения на работодателя за удържане и плащане на осигуровки,

данъци, осъществяване на връзка с лицата, както и изпълнение на други права и задължения като работодател;

2. обезпечаване на съдопроизводствената дейност на съда;
3. осигуряване на икономическите, социални и битови потребности на магистратите, служителите и посетителите в СРС;
4. изготвяне на свидетелства за съдимост;
5. предприемане на действия и изготвяне на отговори във връзка с получени молби, жалби, предложения, сигнали и искания до председателя на СРС.

(2) В сградите на Софийски районен съд се извършва видеонаблюдение от Главна дирекция „Охрана“ към Министъра на правосъдието, която обработва получените лични данни по реда и условията на чл.391-394 ЗСВ. Целта на събирането на лични данни е идентифициране на физическите лица, посещаващи сградата на съда и помещенията в нея за контрол за достъп. Записите от видеонаблюдението се съхраняват за срок от 1 месец. Достъп до данните имат определени служители в рамките на изпълняваните от тях служебни задължения.

Чл.5.(1) При обработката на личните данни Софийски районен съд спазва принципите, разписани в глава 2, чл.5 ОРЗД, съобразно дадените им в Регламента понятия и обем, а именно:

1. законност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхранението;
6. цялостност и поверителност;
7. отчетност.

(2) Законосъобразно обработване на лични данни е налице, когато обработването е необходимо за спазването на законово задължение, което се прилага спрямо СРС. Извън хипотезите на чл.6, §1, б. „б“-„е“ ОРЗД, физическите лица, чиито данни се обработват от СРС, подписват декларация за съгласие – Приложение №1.

(3) Когато лични данни са предоставени от субекта на данни на Софийски районен съд без правно основание или в противоречие с принципите за тяхното законосъобразно обработване, в едномесечен срок 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 документира с протокол от комисия, нарочно определена за това от административния ръководител на СРС или оправомощено от него лице.

#### **Лица, отговарящи за събирането, обработката и съхранението на личните данни и достъп до лични данни**

Чл.6.(1) Събирането, обработката, съхранението и защитата на личните данни се извършва само от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

(2) В качеството си на публичен орган Софийски районен съд определя длъжностно лице по защита на данните.

(3) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

1. информира и съветва администратора и служителите, които извършват обработване, за техните задължения по силата на ОРЗД, на други разпоредби за защитата на данни на равнище ЕС или приложимото българско законодателство;
2. наблюдава спазването на настоящите правила и на приложимото

законодателство относно защитата на личните данни;

3. допринася за повишаване на осведомеността на служителите в СРС, участващи в дейностите по обработване;

4. извършва необходимите одити (проверки) за прилагането на изискванията за защита на личните данни в СРС;

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

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

7. сътрудничи си с Комисията за защита на личните данни в качеството ѝ на надзорен орган на Република България по всички въпроси, предвидени в ОРЗД или произтичащи от други правни актове на Европейския съюз или от законодателството на Република България или по въпроси, инициирани от надзорния орган;

8. действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в чл.36 ОРЗД и по целесъобразност се консултира по всякакви други въпроси;

9. в съответствие с чл.30 ОРЗД води регистър на дейностите по обработване на лични данни във Софийски районен съд;

10. води регистър за нарушенията на сигурността на данните;

11. води регистър за искания от субекти на данни.

**(4)** Данните за контакт с длъжностното лице по защита на данните се обявяват на леснодостъпно място на електронната страница на Софийски районен съд и се съобщават на Комисията за защита на личните данни съгласно чл.37, §7 ОРЗД.

**(5)** Всяко лице, действащо под ръководството на администратора, което има достъп до личните данни и/или обработва тези данни във връзка със своите служебни функции, не следва да ги разпространява на трети лица. При назначаване на съдебен служител в СРС, лицето по изречение първо попълва и собстворъчно подписва декларация за конфиденциалност относно обработваните от него лични данни, станали му известни при и по повод изпълнение на служебните функции (Приложение № 2). Декларацията е със срок на действие не по-малко от 5 (пет) години от прекратяване на трудовото правоотношение със СРС.

**(6)** Магистратите и служителите 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.

**(7)** При обработването на личните данни магистратите спазват Кодекса за етично поведение на българските магистрати, а съдебните служители - Етичния кодекс на съдебните служители.

### **Процедури по обработване на личните данни**

**Чл.7.(1)** Процедурата по обработване на личните данни на магистрати, съдебни служители и кандидати за работа в СРС обхваща обработването и съхранението на лични данни, събрани при и по повод набиране на персонал.

1. Данните се съхраняват в лични трудови или кадрови досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси се съхраняват на хартиен носител.

2. Личните и кадрови досиета се подреждат и съхраняват в специални картотечни шкафове със заключване, находящи се в кабинета на служителите „Човешки ресурси“. Данните на кандидатите за работа се съхраняват в нарочни

шкафове в кабинета на служителите „Човешки ресурси“.

3. Достъпът до досиета се предоставя само на лица, които във връзка с изпълняването на служебните си задължения и по длъжностна характеристика могат да имат достъп до тях.

4. Лицата, оправомощени да обработват лични данни, приемат всички организационно-технически мерки за съхраняването и опазването на личните досиета и класорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

5. Досиетата на съдиите и служителите, както и данните на кандидатите за работа не се изнасят извън сградата на съда, в която се помещава кабинета на служителите „Човешки ресурси“.

(2) Процедурата по обработване на лични данни, отнасящи се до всички лица, съдебни преводачи, съдебни заседатели, особени и процесуални представители и други лица, участващи в съдебния процес обхваща обработването и съхранението на лични данни събрани по повод участиято им в съдебните процеси във връзка с тяхното индивидуализиране в процеса, изпълнение на нормативни права и задължения на СРС, за установяване на връзка с тези лица, за водене на счетоводна отчетност относно дължимите и/или изплатени възнаграждения и разноски на тези лица.

1. Личните данни се обработват както от съдиите, така и от съдебни служители от специализираната администрация относно обезпечаване на съдопроизводствената дейност по делата, както и от служители в звено „Счетоводство“ във връзка с изплащането на полагащите се възнаграждения и счетоводната отчетност.

2. Данните се съхраняват на хартия по делата, образувани в СРС и в електронен вид – в електронните папки на делата, при въвеждане на същите в деловодната програма, използвана от СРС. В частта на счетоводните данни, същите се съхраняват на хартиен носител в помещенията, заемани от служителите в звено „Счетоводство“ и в електронен вид – в ползваните от СРС специализирани счетоводни продукти.

(3) Процедурата по обработване на лични данни, отнасящи се до доставчици на услуги и други контрагенти, обхваща обработването и съхранението на лични данни, необходими за провеждането на процедурите, склучването и изпълнението на договорите.

1. Личните данни във връзка с изпълнение на задължения по ЗОП, СРС съхранява на хартиен носител – в отделни досиета за всяка обществена поръчка, които досиета се съхраняват в шкафове и помещения с ограничен достъп. Личните данни на участниците в обявени от СРС обществени поръчки в ЦАИС „ЕОП“ се съхраняват в електронната система, в профила на СРС, като достъпът до тях е ограничен.

2. Личните данни във връзка със счетоводната отчетност се обработват от служителите в звено „Счетоводство“ и се съхраняват на електронен и/или на хартиен носител. Достъпът до даниите е ограничен.

(4) Процедурата по обработване на лични данни, отнасящи се до съдимостта на лицата и данните за извършени от тях нарушения (свидетелства съдимост и справки съдимост) обхваща обработването и съхранението им от служителите в бюрото „Съдимост“ към СРС. Личните данни се въвеждат в специализиран деловоден продукт. Бюлетините за съдимост се съхраняват в електронен вид и на хартиен носител. Хартиените носители се съхраняват в помещения с ограничен достъп.

(5) Процедурата по обработване на лични данни на лица, подали молби, жалби, предложения, сигнали и искания до председателя на СРС, обхваща обработката им в обема, предоставен от лицата. Обработката се извършва от служителите в административна служба „Регистратура“, като за целта се води специализиран електронен регистър за документооборота, свързан с административната дейност на

съда. Достъп до този регистър е предоставен на определени от административния ръководител на СРС лица.

#### **Документиране на обработката на лични данни**

**Чл.8.(1)** Личните данни се събират за конкретни, точно определени цели и се обработват законосъобразно, добросъвестно, съобразно определените цели и при спазване на принципа на отчетност.

**(2)** Личните данни се съхраняват на хартиен и/или електронен носител, така че да се идентифицира субектът на данните за период, не по-дълъг от необходимото за целите, за които се обработват те. 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 е налице съгласие за това от субекта на данните или данните ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие че ще бъдат приложени подходящите технически и организационни мерки, предвидени с цел да бъдат гарантиирани правата и свободите на субекта на данните.

**(3)** Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:

1. цели на обработването;
2. категории лични данни и категориите субекти на данни;
3. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;
4. предаването на лични данни на трета държава;
5. когато е възможно, предвидените срокове за изтриване на различните категории данни;
6. общо описание на техническите и организационните мерки за сигурност

**(4)** Протоколите се изготвят от лицата, които извършват съответната обработка на данни по указания от административния ръководител или от оправомощено от него лице.

**(5)** Съвкупността от всички протоколи, съдържащи гореописаната информация, съставлява регистъра на дейностите по обработването, съгласно чл.30 ОРЗД.

#### **Технически и организационни мерки за защита на данните**

**Чл.9.(1)** Всички помещения, в които се съхраняват и обработват лични данни, са под контрол на достъпа. Възможните технически средства за контрол на достъп са:

1. охрана на сградата;
2. устройства за разпознаване чрез магнитна карта или ключ;
3. наблюдение с видеокамери в коридорите, където е изградена система за видеонаблюдение.

**(2)** Персоналната защита на личните данни се осъществява при спазване на следните мерки:

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“;

2. споделянето на критична информация между служителите (като

индификатори, пароли за достъп и др.) е забранено;

3. външни лица имат достъп до помещението, в които се обработват лични данни, само в присъствието на оправомощени служители.

(3) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:

1. 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. Декларацията се съхранява в кадровото досие на всеки служител;

2. се запознават с приложимата нормативна база и вътрешни правила и политики относно защитата на личните данни;

3. се запознават с опасностите за субектите на личните данни, обработвани от администратора.

(4) Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. достъпът до операционната система, съдържаща файлове с лични данни, се осъществява от оправомощени служители чрез създадените им лични профили (потребителско име и парола), с определени съобразно задълженията права и нива на достъп;

2. електронните бази данни са защитени чрез стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства, инсталрирана антивирусна програма, периодично извършване на профилактика на софтуера и системните файлове;

3. въвеждане на пароли на файлове, които съдържат лични данни;

4. в помещението, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещението, система за ограничаване на достъпа, сигнално-охранителна система;

5. архивиране на данните на технически носител се извършва периодично с оглед съхранение на информацията.

**Чл.10.(1)** Съдът установява процедури по обработване на лични данни, както в тези правила, така и във вътрешните правила на СРС и в длъжностните характеристики на служителите.

(2) Съдът провежда периодични обучения на магистратите и служителите, за да се гарантира познаване на нормативната уредба, настоящите правила, потенциалните рискове за сигурността на данните и мерките за намаляването им.

(3) Съдът прилага следните организационни мерки за гарантиране нивото на сигурност:

1. охрана на сградата на СРС е депонощна и се осъществява от Главна дирекция „Охрана“;

2. работните компютърни конфигурации, както и цялата ГГ инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

3. при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни;

4. отдалечен достъп до данни от регистрите се осъществява само от обработващи лични данни, с които СРС има склучен договор.

(4) Софийски районен съд не осъществява автоматизирано вземане на решения, включително профилиране.

(5) Длъжностното лице по защита на личните данни докладва периодично на ръководството на СРС предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

## **Нарушения на сигурността**

**Чл.11.(1)** Магистрат или служител от състава на СРС, идентифицирал признания на нарушение на сигурността на данните, е длъжен да докладва незабавно на дължностното лице по защита на данните, като му предостави цялата налична информация. Уведомяването се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му.

**(2)** Дължностното лице по защита на данните извършва своевременно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

**(3)** Дължностното лице по защита на данните докладва незабавно на административния ръководител на съда наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяване, вида на щетите, предприетите мерки за ограничаване на щетите.

**(4)** След уведомяването по ал. 3 администраторът заедно с дължностното лице по защита на данните предприемат необходимите мерки за предотвратяване или намаляване на последиците от неправомерния достъп/нарушението на сигурността, както и възможните мерки за възстановяване на данните.

**(5)** При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, дължностното лице по защита на данните може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай, дължностното лице уведомява незабавно ръководството за предприетите мерки и съобразява последващите действия с получените инструкции.

**Чл.12.(1)** В случай, че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след съгласуване от ръководството на СРС, дължностното лице по защита на личните данни, организира изпълнението на задължението на администратора за уведомяване на Комисията за защита на личните данни, в случаите на обработване на данните на основание чл.6, §1, б.“б“ ОРЗД и Инспектората на ВСС, в случаите когато данните се обработват на основание чл.6, §1, б.“в“ ОРЗД.

**(2)** Уведомяването следва да се извърши без ненужно забавяне и когато това е осъществимо не по-късно от 72 часа след първоначалното узнаване на нарушението.

**(3)** Уведомлението съдържа следната информация:

- описание на нарушението на сигурността, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

- името и координатите за връзка на дължностното лице, отговорно за защита на личните данни, когато нарушението е при изпълнение на функциите по чл.6, §1, б.“б“ ОРЗД и работата по обработване на данните за присъди и нарушения;

- описание на евентуалните последици от нарушението на сигурността;

- описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

**(4)** Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, дължностното лице по защита на личните данни, без ненужно забавяне, уведомява засегнатите физически лица.

**Чл.13.** Дължностното лице по защита на личните данни води регистър в електронен формат за нарушенията на сигурността на данните, който съдържа следната

информация:

- дата на установяване на нарушението;
- описание на нарушението - източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);
- описание на извършените уведомявания: уведомяване на КЗЛД, ИВСС и засегнатите лица, ако е било извършено;
- предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни;
- предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

#### **Предоставяне на данни на трети лица**

**Чл.14.(1)** Съдът може при необходимост да предоставя лични данни на трети лица, действащи в качеството на обработващ, въз основа на изричен договор или нормативен акт.

**(2)** В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на обработващ, съдът:

- изисква достатъчно гаранции от обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;
- сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията и добрите практики за обработка и защита на личните данни;
- сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679;
- информира физическите лица, чиито данни ще бъдат предоставени на обработващ;

**(3)** Обработването на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато това е регламентирано с нормативен акт.

**(4)** Съдът предава лични данни в трети страни (извън Европейския съюз) при изпълнение на съдебни поръчки въз основа на международен договор или при условията на взаимност. В тези случаи се спазват изискванията на ОРЗД и предаването се осъществява въз основа на решение на Европейската комисия за адекватно ниво на защита на данните, а при липса на такова – въз основа на подходящи гаранции по чл.56, §2, б.,а“ от Регламента/съответния международен договор, по който Република България е страна.

#### **Оценка на въздействието върху защитата на данните**

**Чл.15.(1)** Оценка на въздействието се извършва, когато това се изиска съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от СРС. Оценка на въздействието се извършва за високорискови дейности по обработване.

**(2)** Оценка на въздействието е необходимо при всяко въвеждане на ключова система, която е свързана с обработване на лични данни, включително:

- първоначалното въвеждане на нови технологии;
- автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;
- обработване на чувствителни лични данни в голям мащаб;
- мащабно, систематично наблюдение на публично обществена зона
- други операции по обработване, съдържащи се в списък на надзорния орган по

чл.35, §4 от Регламент (ЕС) 2016/679.

(3) Оценката на риска съдържа най-малко:

- системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

- оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

- оценка на рисковете за правата и свободите на субектите на данни;

- мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(4) При извършването на оценката на въздействието се иска становището на дължностното лице по защита на данните.

(5) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

#### **Срок на съхранение. Унищожаване на данните**

Чл.16.(1) СРС, 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 № 3). След изтичането на този срок нарочно определена от административния ръководител на СРС или оправомощено от него лице комисия изтрива или унищожава съхраняваните документи с лични данни, освен ако специален закон предвижда друго.

(2) Когато в процедурата по набиране и подбор на персонала работодателят е изисквал 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.17.(1) Унищожаване на личните данни се извършва от нарочно определена от административния ръководител на СРС или оправомощено от него лице комисия или лице, без да бъдат накърняване правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията в регистрите се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(3) След изтичане срока за съхранение на данните, комисия, назначена от административния ръководител, определя кои документи подлежат на унищожение, начина и мястото на извършване на процедурата

- при унищожаването на данните от регистрите се съставя протокол;

- при прехвърлянето на данните от регистрите на друг администратор се оформя двустранен протокол.

(4) Унищожаването на данни на хартиен носител или магнитен носител се извършва по начин, непозволяващ тяхното възстановяване, например чрез нарязване с шредер машина и/или чрез изгаряне или разрушаване(отваряне) на корпуса и разтрошаване на носителя на данни; или от външна фирма, която представя гаранции за унищожаване на данните при спазване на технология непозволяваща разпознаването им. Електронните данни се изтриват от електронната база данни по начин,

непозволяващ възстановяване на информацията.

#### **Права на субектите на данни**

**Чл.18.(1)** Всяко лице, чиито данни се обработват на основание чл.6, §1, б.,б“ ОРЗД има право на достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за обема и целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

**(2)** Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона.

**(3)** Всяко лице има право писмено да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

**(4)** Правото на достъп се осъществява чрез писмено или електронно заявление до администратора на лични данни – Софийски районен съд. Подаването на заявлението по електронен път е при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация.

**(5) Заявлението ал.4 следва да 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. предпочтита форма на получаване на информация (устна справка, писмена справка, предоставяне на исканата информация на електронен носител);

4. подпись, дата на подаване на заявлението и пълен и точен адрес за кореспонденция;

5. при подаване на заявление от упълномощено лице, към заявлението се прилага и пълномощното.

**(6)** 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 предпочтита 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 административния ръководител на съда лице), и лицето, което е упражнило правото си на заявление по ал.4.

**(7) Субектите на данни имат също правото да:**

- бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;

- подават жалби до регуляторния орган – КЗЛД или Инспектората към ВСС или да обжалва актовете и действията на администратора по реда на чл. 38 - чл. 40 ЗЗЛД.

#### **Употреба на „бисквитки“(cookies) в интернет страницата на СРС**

**Чл.19.(1)** Интернет страницата на СРС може да използва следните видове „бисквитки“ със съответното им предназначение:

- сигурност и идентифициране: Целта им е да разпознаят потребителя в рамките на конкретната сесия, да контролират сигурността и да гарантират, че информацията, която потребителят въвежда се вижда единствено от него.

- ефективност и функционалност: „Бисквитките“ за производителност целят събиране на статистическа информация и предоставяне на съдържание спрямо индивидуалните предпочитания на потребителите. Чрез тях анонимно се измерват броя посещения, разгledаните подстраници, активността на посетителите, както и повторните посещения на интернет страницата. Тези „бисквитки“ помагат за анализ на трафика, което позволява подобряване на страницата, както и цялостното потребителско улеснение.

(2) Повечето браузъри са настроени да приемат „бисквитки“ по подразбиране. Въпреки това, ако посетителят на интернет страницата на СРС не желае „бисквитките“ да бъдат съхранявани на неговото устройство, той има възможност да ги ограничи чрез промяна на настройките. Контролирането, изключването или блокирането на „бисквитките“ се управлява от използвания браузър. При пълна забрана на използването на всички „бисквитки“, може да се рефлектира върху функционалното представяне на сайта, неговата ефективност и достъпването на определена информация.

(3) Всички „бисквитки“, които се ползват се заличават/изтриват автоматично след определен период от време. Този период варира до 365 дни според предназначението на конкретната „бисквитка“.

(4) СРС не записва каквато и да е персонална информация на посетителя на интернет страницата си.

(5) Сайтът на СРС събира данни в лог файлове. Тази информация съдържа IP на потребителя, използвания браузър, операционната система, времето на посещение, посетените страници. СРС си запазва правото да използва IP адресите на потребителите за разкриване на идентичността им в случаите, когато това е необходимо в изпълнение на закона.

#### **Допълнителни разпоредби**

**Чл.20.** Всички магистрати и служители в Софийски районен съд са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

**Чл.21.** Надзор и осигуряване спазването на Регламент (ЕС) 2016/679 и Закон за защита на личните данни при обработване на лични данни в СРС във връзка с изпълнение на функциите му на орган на съдебната власт осъществява Инспектората към Висшия съдебен съвет съгласно Глава Трета от Закона за защита на личните данни.

**Чл.22.** За всички неурядени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общий регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

**Чл.23.** СРС си запазва правото да прави изменения и допълнения в настоящите правила. При извършване на промени в Правилата, те ще бъдат своевременно оповестени на официалната интернет страница - <http://www.srs.justice.bg/>.

**Чл.24.** Неразделна част от настоящите правила са следните приложения:

Приложение № 1 – декларация за съгласие;

Приложение № 2 – декларация за конфиденциалност;

Приложение № 3 – декларация за участници в конкурси.

**Чл.25.** Тези правила са приети и утвърдени със Заповед № АС-.../.....2021 г. на административния ръководител на СРС.

## **ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ**

Долуподписаният/ата .....  
ЕГН ....., адрес .....

### **ДЕКЛАРИРАМ, ЧЕ:**

Давам съгласието си Софийски районен съд да обработва моите лични данни за целите на:

.....  
.....  
със средства, съобразени с разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателство на Република България относно защитата на личните данни.

Уведомен/а съм, че мога да оттегля моето съгласие по всяко време.

Информиран/а съм, че имам право на информация за събираните от мен данни, за правото на достъп до тях, да искам данните ми да бъдат коригирани или изтрити, да искам обработването на данните ми да бъде ограничено и да възразя срещу определен начин на обработване на личните ми данни.

Дата: .....  
гр. София

Декларатор : .....  
(име, фамилия, подпись)

## ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИЈАЛНОСТ

Долуподписаният/ата .....  
ЕГН ....., постоянен адрес .....

ДЕКЛАРИРАМ, ЧЕ:

1. По време на изпълнение на служебните ми функции като тайна лични данни, които се обработват от администратора и са ми станали известни при и по повод служебните ми функции.
  2. Задължавам се да не разгласявам по никакъв начин конфиденциална информация за Софийски районен съд (СРС), магистратите и/или съдебните служители, работещи в съда, станала ми известна в отношенията ми със СРС.
  3. Разгласяване на лични данни и/или конфиденциална информация по смисъла на настоящата Декларация представлява всякакъв вид устно или писмено изявление, предаване на информация на хартиен, електронен или друг носител, включително по поща, факс или електронна поща, както и всякакъв друг начин на разгласяване на информация, в това число чрез средствата за масово осведомяване, печатните издания или Интернет.
  4. Задълженията по т.1 и т.2 от настоящата декларация са без ограничение в територията и са за срок от 5 (пет) години от прекратяване на правоотношението мисъл СРС.
  5. Задължението за запазване на конфиденциалност не се прилага по отношение на информация, която е била публично оповестена.
  6. Запознат/а съм, че нося отговорност за неспазване на настоящата Декларация, в т.ч. за всички преки и непосредствени вреди, нанесени в резултат от неспазването на Декларацията.

Настоящата декларация е подписана в два еднообразни екземпляра – по един за декларатора и за СРС.

Дата: ..... Декларатор : .....  
гр. София (име, фамилия, подпись)

До  
Административния ръководител -  
председател на Софийски районен съд

## ДЕКЛАРАЦИЯ

Долуподписаният/ата, .....

име, презиме, фамилия

ЕГН .....,

адрес: .....

/посочва се постоянен адрес; в случай, че постоянен и настоящ адрес се различават, кандидатът посочва настоящ адрес/

телефон: ....., ел.поща: .....

## ДЕКЛАРИРАМ, ЧЕ:

Съм съгласен/на Софийски районен съд да съхранява и обработва личните ми данни съгласно изискванията и при спазване на разпоредбите на Закона за защита на личните данни и във връзка с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. (ОРЗД), които предоставям във връзка с подаване на документи за участие в конкурсна процедура.

Известно ми е, че:

- моите лични данни, които съм предоставил/а на Софийски районен съд в рамките на процедурата по кандидатстване за длъжността „.....“ се обработват от съда за целите на конкурсната процедура, както и за целите на подбор на персонал;
- информиран/а съм, че Софийски районен съд може да обработва моите лични данни само доколкото това е необходимо във връзка с конкурсната процедура, както и във връзка с подбора на персонал;
- заявлението и всички приложени към него документи се съхраняват в Софийски районен съд в срок от 2 (две) години, считано от окончателното приключване на конкурсната процедура, съответно след изтичането на срока на обжалване на процедурата;
- при желание, всеки кандидат може да получи обратно комплекта си с документи преди изтичане на посочения по-горе срок, но не по-рано от 6 (шест) месеца от окончателното приключване на конкурсната процедура, съответно след изтичането на срока на обжалване на процедурата.

Дата: ..... г.

Декларатор: .....