С О Ф И Й С К И В О Е Н Е Н С Ъ Д

УТВЪРЖДАВАМ:
ПОЛК. МАДЛЕН ДИМИТРОВА
АДМИНИСТРАТИВЕН РЪКОВОДИТЕЛ-
ПРЕДСЕДАТЕЛ НА СВС

В Ъ Т Р Е Ш Н И П Р А В И Л А

за защита на личните данни

в

СОФИЙСКИЯ ВОЕНЕН СЪД

1000 София, бул. „Витоша” № 2, партер,
тел./факс: 02/980 00 61, e-mail: svs1990@abv.bg

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Вътрешните правила за защита на личните данни в Софийския военен съд определят редът, начинът, основните принципи по отношение на защитата на физическите лица във връзка с обработването на лични данни, правата и задълженията на длъжностните лица по защита на данните, регистри на лични данни, минималното ниво на технически и организационни мерки за тяхната защита, архивиране, проверка, унищожаване на данни; оценка на въздействието върху защитата на данните; особени случаи на обработване на данни; докладване и управление на инциденти.

(2) Правилата са изработени съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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 (Регламент (ЕС) 2016/679), Закона за защита на личните данни и действащото законодателство.

Чл. 2. (1) Софийският военен съд (СВС) е администратор на лични данни, със седалище, адрес на управление и кореспонденция: гр. София, Съдебна палата, ет. Партер, който се представлява от административен ръководител - председател. Работно време: от понеделник до петък от 08.30 ч. до 17.00 ч., ел. поща: svs1990@abv.bg.

(2) СВС осъществява функциите на орган на съдебната власт, предвидени в Конституцията на Република България, Закона за съдебната власт и други нормативни актове. Софийският военен съд, в качеството си на администратор по смисъла на чл. 4, т. 7 от Регламент (ЕС) 2016/679, обработва лични данни във връзка със своята основна функция – да осъществява правораздавателна дейност.

(3) Личните данни се обработват самостоятелно от администратора на лични данни, чрез възлагане на обработващи лични данни или съвместно с друг обработващ.

(4) При съвместно обработване на лични данни между СВС и друг администратор или обработващ, отношенията помежду им се уреждат със споразумение относно упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информация по чл. 13 и 14 на Регламент (ЕС) 2016/679, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на съюза или правото на държава членка, което се прилага спрямо администраторите.

Чл. 3. (1) При обработването на лични данни в СВС се спазват следните принципи:

- законосъобразност, добросъвестност и прозрачност – обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

- ограничение на целите – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

- свеждане на данните до минимум – данните да са подходящи, свързани с и ограничени до необходимото във връзка с целите на обработването;

- точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

- ограничение на съхранението – данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

- цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

- отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(2) Ако конкретната цел или цели, за които се обработват лични данни от СВС, не изискват или вече не изискват идентифициране на субекта на данните, СВС не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент (ЕС) 2016/679.

Чл. 4. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на СВС и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на СВС се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения,

съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

(4) Обработваните лични данни в регистрите на СВС 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.

Чл. 5. (1) Достъпът до лични данни се осъществява само от лица, в чиито правомощия по закон, длъжностна характеристика или конкретно възложена задача е определено задължение за обработване на данните от съответния регистър, при спазване на принципа „Необходимост да знае“. Тези лица са длъжни да познават нормативната уредба в областта на защита на личните данни, тези Вътрешни правила, както и да отчитат рисковете за правата и свободите на физическите лица, чиито лични данни се обработват в СВС.

(2) Лицата под ръководството на администратора подписват декларация (*Приложение № 1*) или се задължават с длъжностната характеристика да не разгласяват личните данни, до които са получили достъп при изпълнение на задълженията си.

(3) При нарушаване на правилата за достъп до личните данни съдебните служители на СВС носят дисциплинарна отговорност.

(4) След прекратяване на правоотношенията със СВС, 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 № 2).* Декларацията се попълва към датата на прекратяване на правоотношенията и е със срок на действие не по-малко от 2 /две/ години.

Чл. 6. (1) Всяко физическо лице, чиито лични данни се обработват в СВС, следва да бъде информирано за:

1. данните, които идентифицират СВС и координатите за връзка с него;

2. координатите за връзка с длъжностното лице по защита на данните;

3. целите и основанието за обработването;

4. категориите лични данни, отнасящи се до съответното физическо лице;

5. източника на данните;

6. получателите или категориите получатели, на които могат да бъдат разкрити данните;

7. срока на съхранение на данните;

8. правото на достъп, коригиране, изтриване или ограничаване на обработването на събраните данни;

9. правото на жалба до КЗЛД.

(2) Алинея 1 не се прилага, когато:

1. обработването е за целите на архивирането в обществен интерес, за статистически, исторически или научни цели и предоставянето на данни по ал. 1 е невъзможно или изисква прекомерни усилия;

2. получаването или разкриването на данни са изрично предвидени в закон;

3. физическото лице, за което се отнасят данните, вече разполага с информацията по ал. 1;

4. е налице изрична забрана за това по закон.

(3) Информацията по ал. 1 се поставя на видно място в сградата на СВС и се публикува на официалната интернет страница на съда.

(4) Физическите лица, чиито лични данни се обработват от СВС, извън целите на правораздаването, подписват декларация за информираност, по образец (*Приложение № 3*).

II. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл. 7. (1) Длъжностно лице по защита на данните се определя със заповед на административния ръководител – председател на СВС.

(2) Длъжностно лице по защита на данните изпълнява най-малко следните задачи:

1. информира и съветва административния ръководител на съда, а при отсъствието му – неговия заместник (в качеството му на администратор) и служителите, които извършват обработване на лични данни, за техните задължения по Регламент (ЕС) 2016/679 и на други разпоредби за защита на данни на равнище Европейски съюз или държава членка;

2. наблюдава спазването на Регламент (ЕС) 2016/679 и на други разпоредби за защита на данни на равнище Европейски съюз или държава членка;

3. наблюдава спазването на правилата и политиките на СВС и действащото законодателство по отношение на защита на личните данни;

4. допринася за повишаване на осведомеността и обучението на магистратите и служителите в СВС, участващи в дейностите по обработването;

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

6. при поискване да предоставя съвети по отношение оценка на въздействието върху защитата на личните данни и наблюдава нейното извършване;

7. сътрудничи си с КЗЛД и/или ИВСС;

8. действа като точка за контакт с КЗЛД и/или ИВСС по въпроси, свързани с обработването, включително предварителната консултация, посочена в чл. 36 от Регламент (ЕС) 2016/679, и по целесъобразност да се консултира по всякакви други въпроси;

9. води регистъра на дейностите по обработване на лични данни в СВС;

10. води регистър на нарушенията на сигурността на личните данни; подготвя уведомления да КЗЛД и субектите на данни при условията на чл. 33 и 34 от Регламент (ЕС) 2016/679, когато е приложимо;

11. произнася се по постъпили искания за упражняване на права от субекта на данни;

12. води регистър за исканията от субекти на данни;

13. извършва обучения и инструктажи по защита на данните, като води и съхранява регистър за провеждането им.

(3) Съдебният служител, определен за „длъжностно лице по защита на данните“ действа независимо при изпълнение на задълженията си по ал. 2 и се отчита пряко пред административния ръководител-председател на СВС.

III. ПРАВА НА СУБЕКТА НА ДАННИТЕ

Чл. 8. (1) Всяко физическо лице има право на безплатен достъп до обработвани от СВС негови лични данни, извън тези, обработвани във връзка с нуждите на правораздаването.

(2) Правото на достъп се осъществява с писмено заявление до административния ръководител на СВС, по образец (*Приложение № 4*). Заявлението се подава лично от субекта на данните или изрично упълномощено лице с нотариална заверка на подписа. В заявлението следва да бъдат посочени данни относно физическата идентичност на заявителя (имена; ЕГН; номер на лична карта, дата и място на издаване, адрес, телефон за връзка, електрона поща), да бъде посочен начинът на предоставяне на информацията. В случай че заявлението се подава чрез пълномощник, следва да бъде посочено дали достъпът да бъде даден на него.

(3) Информацията може да бъде предоставена на субекта или на неговия представител под формата на устна или писмена справка, по

електронен път или на технически носител. Информацията се предоставя по посочения от субекта начин, освен в случаите, когато това е забранено по закон.

Чл. 9. (1) Заявленията за предоставяне на достъп до лични данни се разглеждат от длъжностното лице по защита на данните в 30-дневен срок.

(2) Достъпът до лични данни може да бъде ограничен, когато те не съществуват или когато предоставянето им е забранено със закон.

(3) Когато с предоставянето на достъп до лични данни има опасност да се разкрият данни и за трети лица, на субекта на данни се предоставя информация, съдържаща само отнасящи се за него лични данни.

(4) Във всички случаи на предоставяне на информацията, с изключение „под формата на писмена справка“, следва да бъде отбелязано в Регистър, отразяващ извършваните действия, между лицето, което предоставя исканата информация, или оправомощено от административния ръководител лице, и лицето, което е упражнило правото си на заявление по чл. 8, ал. 2.

Чл. 10. Третите страни получават достъп до лични данни, обработвани в СВС, при наличие на законово основание за обработването на лични данни (напр. органи на съдебна власт, ВСС, НАП, НОИ, Висш съдебен съвет, Висш адвокатски съвет, Национално бюро за правна помощ и др.п.).

Чл. 11. (1) Всяко физическо лице има право да поиска от СВС да заличи или да коригира негови лични данни, ако за обработването им не съществува основание или те са непълни, или неточни.

(2) Заявленията за коригиране и заличаване на лични данни се подават от лицата по реда на чл. 8 и се разглеждат от длъжностното лице по защита на данните в 30-дневен срок.

Чл. 12. Администраторът на лични данни може да откаже пълно или частично упражняването на правата на субектите на данни, когато то би създало 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 преследване на нарушения на етичните кодекси при регулираните професии; защитата на субекта на данните или на правата и свободите на други лица.

IV. РЕГИСТРИ НА ЛИЧНИ ДАННИ В СОФИЙСКИЯ ВОЕНЕН СЪД

Чл. 13. (1) В СВС се обработват лични данни в следните регистри:

1. Регистър „Съдии“;
2. Регистър „Съдебни служители“;
3. Регистър „Съдебни заседатели и вещи лица“;
4. Регистър „Участници в конкурсни процедури в администрацията на Софийския военен съд”;
5. Регистър „Счетоводство, финансова дейност и контрагенти”
6. Регистър „Лични данни на физически лица, подали молби, заявления, жалби, предложения и искания“;
7. Регистър „Правораздаване“;
8. Регистър „Видеонаблюдение“.

(2) Общото описание на всеки регистър, целите на обработването, правното основание, категориите субекти, категориите лични данни, източниците на данни, обработващите данните, носителите, категориите получатели и възможността на предаване на данни в трети държави, местосъхранението на данните и сроковете за съхранение са посочени в Регистър на дейностите в Софийския военен съд по обработване на лични данни на основание чл. 30 от Регламент (ЕС) 2016/679 (*Приложение № 5*).

(3) За личните данни на физическите лица в Регистър „Правораздаване“, обработвани в СВС на основание чл. 6, пар. 1, б. „в“ и б. „д“ от Регламент (ЕС) 2016/679 (спазване на законово задължение, което се прилага спрямо администратора и упражняване на официални правомощия, които са предоставени на администратора за целите на правораздаването), включително особено чувствителни лични данни по чл. 9, пар. 1 от Регламент (ЕС) 2016/679, във връзка с чл. 9, пар. 2, б. „е“ от Регламент (ЕС) 2016/679 (администраторът на данни действа в качество на правораздаващ орган) се прилагат правилата на Глава осма от ЗЗЛД.

V. МЕРКИ ЗА ЗАЩИТА

Чл. 14. СВС 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. 15. СВС прилага защита на личните данни, която включва:

1. физическа защита – с цел предотвратяване на нерегламентиран достъп и защита на помещенията на съда, в които се извършват дейности по обработване на лични данни, като се използват сигнално-охранителна

система, видеонаблюдение, използване на заключващи механизми, оборудване с пожароизвестителни и пожарогасителни средства;

2. персонална защита – по смисъла на чл. 17 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 използване на уникални потребителски акаунти и пароли; администриране на достъпа до мрежите; защита от зловреден софтуер.

Чл. 16. Физическата защита на личните данни в СВС се осигурява чрез следните технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на помещенията, в които се извършват дейности по обработване на лични данни:

1. личните данни се обработват само в служебните помещения на СВС, като достъпът до тях е физически ограничен и контролиран - само за магистрати и 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;

2. комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения, 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;

3. организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения;

4. зони с контролиран достъп са всички помещения на територията на СВС, в които се събират, обработват и съхраняват лични данни.

5. всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп чрез принципа „необходимост да знае” с оглед изпълнението на работните им задължения.

6. всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал;

7. достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, включително сървъри, са защитени по адекватен начин, в зони с контрол на достъпа;

8. документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика);

9. оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства;

10. пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложимата нормативна уредба.

Чл. 17. (1). Персоналната защита на личните данни в СВС се осъществява при спазване на следните мерки:

1. задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни, по образец (*Приложение № 6*);

2. достъпът до личните данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „необходимост да знае“;

3. забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.пр.) както между служителите, така и между тях и трети, неоторизирани лица;

4. лицата, обработващи лични данни, задължително подписват декларация за неразпространение на лични данни, станали им известни във

връзка със служебните им задължения. Декларацията се съхранява в кадровото досие на всеки служител. Подписване на декларация не се изисква, ако съответното задължение е включено в длъжностната характеристика на лицето;

5. периодично обучение и инструктаж по защита на данните, които се отразяват в протокол по образеца по т. 1;

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

Чл. 18. Документална защита на личните данни в СВС се осъществява при спазване на следните мерки:

1. определяне на регистрите, които ще се поддържат на хартиен носител - на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на СВС, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;

2. определяне на условията за обработване на лични данни - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на СВС, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

3. регламентиране на достъпа до регистрите с лични данни – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае”;

4. определяне на срокове за съхранение - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок;

5. процедури за унищожаване - документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на СВС или за установяването, упражняването или защитата на правни претенции, се унищожават по начин, непозволяващ тяхното възстановяване (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

6. правила за размножаване и разпространение - копиране и разпространяване на лични данни е разрешено единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на

закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Чл. 19. (1) Защитата на автоматизираните информационни системи и/или мрежи в СВС включва следният набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни:

1. комуникационно-информационните системи, използвани за обработка на лични данни, физически се разполагат в специални защитени помещения, 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 ангажименти за поддръжката на нормалното функциониране на тези системи, които не са от състава на СВС;

2. 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;

3. създаване на индивидуални акаунти и използване на персонални пароли от магистрати и служителите от състава на СВС за достъп до служебния компютър, като паролите подлежат на задължителна промяна на всеки шест месеца, а в случай на нерегламентиран достъп – в момента на установяването;

4. 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);

5. забранява се предоставянето на персоналните пароли на трети лица, с изключение на случаите на принципа „необходимост да знае“;

6. определя се ниво на достъп до следните WEB базирани системи – Система за случайно разпределение на дела и Система за изчисляване на натовареността на магистратите чрез персонални профили и пароли, и КЕП за лицата, на които е разрешен достъпът до тях;

7. определя се ниво на достъп до съществуващата деловодна информационна система от типа САС "Съдебно деловодство", разработен от "Информационно обслужване" АД, чрез персонални профили и пароли за лицата, на които е разрешен достъпът до нея;

8. в зависимост от възложените функции, ограничава се достъпът до външни мрежови ресурси - интернет връзки с трети страни, сегменти на хостинг системи на трети страни;

9. 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;

10. 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.;

11. забранено е инсталирането на софтуерни продукти, различни от предвидените за изпълнение на служебните функции;

12. забранено е ползване на хардуерни и/или софтуерни инструменти от магистратите и служителите на СВС, които биха могли да послужат, за да се компрометира сигурността на информационните системи;

13. в СВС се използва единствено софтуер с уредени авторски права, инсталиран от оторизирано за това лице;

14. при съмнение или установяване на компрометирана компютърна система, работещият с нея е задължен да уведоми системния администратор и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър /чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация/;

15. отдалечен достъп до автоматизираната система за управление на дела не е предвиден да се осигурява, с изключение на случаите на принципа „необходимост да знае“;

16. възможност за установяване лицето, имало неразрешен достъп до регистрите и книгите;

17. при регистриране на неправомерен 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 административния ръководител или оправомощено от него лице за предприемане на мерките по чл. 33 от Регламент (ЕС) 2016/679;

18. 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;

19. публикуването на съдебните актове в интернет страницата на СВС се извършва на основание чл. 64 от Закона за съдебната власт, при

спазване на изискванията на ЗЗЛД, ЗЗКИ, настоящите вътрешни правила и Вътрешните правила за организацията по публикуване на съдебните актове в Интернет, утвърдени от административния ръководител на съда;

20. след постигане целта на обработване на личните данни, съдържащи се в поддържаните от СВС 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).

VI. АРХИВИРАНЕ. ПРОВЕРКА ЗА СЪСТОЯНИЕТО НА ЛИЧНИТЕ ДАННИ. УНИЩОЖАВАНЕ

Чл. 20. (1) Документите и преписките, по които работата е приключила, се архивират, в това число документи (кадрови (служебни) дела и трудови досиета) на освободени магистрати и съдебни служители.

(2) Документите, по приключили конкурси в СВС се връщат на неизбраните кандидати в 6-месечен срок от приключване на конкурса, а преписките се архивират.

(3) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожароизвестителни системи и пожарогасители, които задължително се заключват.

(4) Документите на електронен носител се съхраняват на специализирани сървъри, компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица от СВС съобразно възложените им правомощия.

Чл. 21. (1) Носителите на лични данни, обработвани в СВС по всички входящи и изходящи съдебни книжа и документи по съдебните дела и входящата и изходяща кореспонденция на съда се администрират,

обработват деловодно и архивират по реда и условията на ПАС, Вътрешните правила за организацията на деловодната и архивна дейност в Софийския военен съд, при спазване на разпоредбите на настоящите Вътрешни правила.

(2) Носителите на лични данни, обработвани в СВС, съдържащи класифицирана информация се администрират, обработват деловодно и архивират при спазване на законовите изисквания на ЗЗКИ и ППЗЗКИ.

Чл. 22. (1) Веднъж годишно се извършва проверка за състоянието и целостта на личните данни, съдържащи се в регистъра и необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на административния ръководител – председател на СВС.

(3) За работата си комисията съставя доклад (в два еднообразни екземпляра), който трябва да включва преценка на необходимостта за обработка на лични данни или за унищожаване.

(4) Докладът се предоставя на длъжностното лице по защита на данните за становище. Докладът на комисията и становището на длъжностното лице по защита на данните по него се представят на административния ръководител – председател на СВС.

(5) Екземпляр от доклада на комисията по ал. 3, в едно със становището на длъжностното лице по защита на данните, ако съдържат констатации за необходимост от унищожаване на лични данни, се предава на комисията по чл. 66 и сл. от Правилника за администрацията в съдилищата за последващи действия, съобразно приложимата нормативна уредба.

Чл. 23. (1) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от СВС регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) Носителите на лични данни, обработвани в СВС по всички входящи и изходящи съдебни книжа и документи по съдебните дела и входящата и изходяща кореспонденция на съда се унищожават по реда и условията на ПАС, настоящите Вътрешни правила и Вътрешните правила за организацията на деловодната и архивна дейност в Софийския военен съд, като се вземе становището и на съдебния служител, изпълняващ функциите на лице по защита на данните.

(3) Носителите на лични данни, обработвани в СВС, съдържащи класифицирана информация се унищожават при спазване на законовите изисквания на ЗЗКИ и ППЗЗКИ.

(4) В случаите, в които се налага унищожаване на носител на лични данни, СВС прилага необходимите действия за заличаването на личните

данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване или изгаряне.

(3) Унищожаване се осъществява от комисия, назначена със заповед на административния ръководител – председател на СВС и след уведомяване на длъжностното лице по защита на данните.

(4) За извършеното унищожаване на носители на лични данни се съставя протокол, подписан от членовете на комисията по ал. 3, който се представя на административния ръководител – председател за утвърждаване.

VII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 24. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед риска за физическите лица и естеството на обработка на лични данни, извършвана от СВС. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходима при:

1. първоначално въвеждане на нови технологии;

2. автоматизирано обработване, включително профилиране или автоматизирано вземане на решения;

3. обработване на чувствителни лични данни в голям мащаб;

4. други операции по обработване, съдържащ се в списък на надзорния орган по чл. 35, пар. 4 от Регламент (ЕС) 2016/679.

(3) Оценка на риска съдържа най-малко:

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

2. оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

3. оценка на рисковете за правата и свободите на субектите на данни;

4. мерките за справяне с рисковете, включително гаранциите; мерките за сигурност и механизмите за осигуряване на защита на личните данни и за спазване на изискванията по опазване на личните данни, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(4) При извършване на оценка на въздействието се иска становището на длъжностното лице по защита на данните.

(5) Ако извършената оценка на въздействието покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска, следва да се извърши консултация с КЗЛД или ИВСС преди планираното обработване.

Чл. 25. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, СВС може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

(2) Доклади за състоянието, рисковете и нивото на чувствителност на информацията се изготвят от длъжностното лице по защита на данните веднъж на 2 години или при промяна на характера на обработваните лични данни.

VIII. ОСОБЕНИ СЛУЧАИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 26. Когато лични данни са предоставени от субекта на данни на СВС 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 комисия, определена със заповед на административния ръководител на съда.

IX. ДОКЛАДВАНЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 27. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

X. ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

Чл. 28. Системите за докладване на нарушения; системите за контрол на достъпа до вътрешносъдебни ресурси; системите за контрол на достъпа, работното време и трудовата дисциплина в СВС, по смисъла на чл. 25и от ЗЗЛД са разработени и утвърдени в Устройствения правилник на СВС; Правилника за вътрешния трудов ред; Вътрешните правила за организацията и управлението на човешките ресурси; Правила за здравословни и безопасни условия на труд; Вътрешни правила за изграждане и функциониране на СФУК; Идентифициране и оценка на рисковете в СВС; Правила за подаване на сигнали за нарушения на Етичния кодекс на съдебните служители в СВС; Вътрешни правила за организация на деловодната и архивна дейност; Вътрешни правила за осъществяване на предварителен контрол за законосъобразност; Правила за осъществяване на текущ контрол на договорите, сключени в СВС; Вътрешни правила за информационна осигуреност и сигурност, достъп по Интернет и работа с компютърната, копирната и принтерна техника в СВС; Правила за искане и предоставяне на достъп до обществена информация; Вътрешни правила за организация дейността на съдебните заседатели в СВС; Вътрешни правила за организацията по провеждане на първоначално обучение по защита на класифицирана информация на новоизбраните съдебни заседатели; Вътрешни правила за организацията по провеждане на обучение по КИ в СВС; Вътрешни правила за работа с медиите; Правила за разделяне на отговорностите в СВС; Вътрешен правилник за документооборота на счетоводните документи и формата на счетоводството; Процедури за преглед на вътрешните правила, процедури, дейности и операции в СВС и Процедури за наблюдение в СВС се прилагат и при обработването на лични данни на физически лица, при спазване и на настоящите Вътрешни правила.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички магистрати и служители от Софийския военен съд са длъжни да спазват ежедневно при изпълняване на заеманата от тях длъжност и възложените им служебни функции настоящите Вътрешни правила.

§ 2. 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.

§ 3. Неразделна част от правилата са:

- **Приложение № 1** – декларация по чл. 5, ал. 2 от Правилата;

- Приложение № 2 – декларация по чл. 5, ал. 4 от Правилата;
- Приложение № 3 – декларация по чл. 6, ал. 4 от Правилата;
- Приложение № 4 – заявление – по чл. 8, ал. 2 от Правилата;
- Приложение № 5 – регистър – по чл. 13, ал. 2 от Правилата;
- Приложение № 6 – протокол – по чл. 17, ал. 1, т. 1 от Правилата.

§ 4. Изменения и допълнения на тези правила се извършват по реда на утвърждаването им от административния ръководител на съда.

§ 5. Настоящите вътрешни правила влизат в сила от датата на утвърждаването им от административния ръководител.

Приложение № 1
по чл. 5, ал. 2 от Вътрешните правила за защита на личните данни в СВС

Д Е К Л А Р А Ц И Я

от ……,
на длъжност: ……
в ……

Задължавам се да не разгласявам лични данни, станали ми известни при и по повод изпълнение на задълженията ми като служител на длъжност …… в СВС, освен ако това не е предвидено изрично в закон или не застрашава живота и здравето на физическото лице.

Дата: .....
гр. ……

Декларатор: ……

/...../

Приложение № 2
по чл. 5, ал. 4 от Вътрешните правила за защита на личните данни в СВС

ДЕКЛАРАЦИЯ ЗА КОНФИДЕНЦИАЛНОСТ

Долуподписаният/ата ……,
(име, презиме, фамилия)
ЕГН ……., с адрес:……,
с настоящото декларирам, че за срок от 2 /две/ години от датата на подписване на настоящата декларация, ще запазя в тайна личните данни, които се обработват от администратора и станали ми известни при или по повод служебните ми функции, като …….

Дата: .....

Декларатор: .....

/......./

Приложение № 3
по чл.6, ал. 4 от Вътрешните правила за защита на личните данни в СВС

ДЕКЛАРАЦИЯ ЗА ИНФОРМИРАНОСТ

Долуподписаният/ата……,
(име, презиме, фамилия)
ЕГН…..……, адрес:……..,
с настоящото декларирам, че давам съгласието си Софийският военен съд ще 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.

Информиран съм за данните, които идентифицират администратора – СВС и координатите за връзка с него; координатите за връзка с длъжностното лице по защита на данните; категориите лични данни, които се изработват; източника на данните; получателите или категориите получатели, на които могат да бъдат разкрити данните ми; срока на съхранение.

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

Дата: .....

Декларатор: …….

/**.....**/

Приложение № 4
по чл.8, ал. 2 от Вътрешните правила за защита на личните личните в СВС

ДО
АДМИНИСТРАТИВНИЯ РЪКОВОДИТЕЛ
ПРЕДСЕДАТЕЛ НА
СОФИЙСКИЯ ВОЕНЕН СЪД

З А Я В Л Е Н И Е
за упражняване на права в областта
на защита на личните данни

от ……
(име, презиме и фамилия)
……
(Идентификационни данни: ЕГН; лична карта №, номер и място на издаване)

Адрес за кореспонденция: ……
……
Телефон; ел.поща:……

УВАЖАЕМА ГОСПОДИН/ГОСПОЖО ПРЕДСЕДАТЕЛ,

В съответствие с чл. 37б от Закона за защита на личните данни, с настоящото заявление бих искал/а да упражня следните свои права в областта на защитата на личните данни, произтичащи от Регламент (ЕС) 2016/679 *(отбелязва се относимото):*

- **право на информация** по чл. 13-14 от Регламента;
- **право на достъп** по чл. 15 от Регламента до всички лични данни/до следните лични данни: ……
…….
…….
- **право на коригиране** по чл. 16 от Регламента на следните неточни данни, отнасящи се до мен/попълване по чл. 16 от Регламента на следните непълни данни, отнасящи се до мен: ……..
……..
……..
- **право на изтриване** по чл. 17 от Регламента на следните лични данни ….
.....
поради приложимост на хипотезата на ……..
- **право на ограничаване** по чл. 18 от Регламента на обработването на следните лични данни, отнасящи се до мен, поради приложимост на хипотезата на ……
- **право на възражение** по чл. 21 от Регламента срещу обработването на следните лични данни, отнасящи се до мен ……
.....

Желая комуникацията между нас, респективно исканата от мен информация, да бъде реализирана в следната форма:

- в устна форма;
- в писмена форма;
- по електронен път.

Дата: .....

Декларатор: .....

/......./

Приложение № 5
по чл.13, ал. 2 от Вътрешните правила за защита на личните данни в СВС

РЕГИСТЪР НА ДЕЙНОСТИТЕ В СОФИЙСКИЯ ВОЕНЕН СЪД

по обработване на лични данни на основание чл. 30 от Общия регламент относно защита на данните

Администратор на лични данни: Софийски военен съд, представляван от административен ръководител - председател
Координати за връзка с администратора: гр. София, Съдебна палата, ет. Партер; ел. поща: svs1990@abv.bg.

Длъжностно лице по защита на данните:
……
……
……
(име, длъжност, контакти)

Открит на …… г.

I. РЕГИСТЪР „СЪДИИ“

1.	**Цели на обработването**	Изпълнение на нормативните изисквания на Закона за съдебната власт (ЗСВ), Закона за отбраната и въоръжените сили на Република България (ЗОВСРБ), Наказателно-процесуалния кодекс, Закона за защита на класифицираната информация (ЗЗКИ), Кодекс за социално осигуряване (КСО), Закона за счетоводството (ЗС), Закона за данъците върху доходите на физическите лица (ЗДДФЛ), Закона за безопасни условия на труд (ЗБУТ), Наредба за командировките в страната и др.
2.	**Правно**	Чл. 6, пар. 1, б. „в“ и б. „д“ от Регламент (ЕС)

	основание	2016/679 – спазване на законово задължение, което се прилага спрямо администратора и упражняване на официални правомощия, които са предоставени на администратора
3.	**Категории субекти**	Съдии в Софийския военен съд.
4.	**Категории лични данни**	1. Физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка, снимка във военна униформа с военно звание и др. 2. социална идентичност: данни относно образование (учебно заведение, образователна степен, допълнителни квалификации и специализации), трудова дейност, стаж, професионална биография, атестация, ранг, военно звание, награди и поощрения, дисциплинарни наказания; 3. семейна идентичност – данни относно семейното положение на лицата (наличие на брак, развод, брой и имена на членове на семейството, в това число деца до 18 години); 4. икономическа идентичност – данни относно имотното и финансово състояние на лицата; 5. лични данни относно съдебното минало на лицата; 6. данни за здравословното състояние на лицата.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления, рапорти, предложение и др. или в документи, предоставяни от органи на съдебна власт при провеждане на нормативно регламентирани процедури.
6.	**Обработващ данните**	Длъжностни лица – съдебен администратор; човешки ресурси; деловодител; деловодител „КИ“; съдебен служител, изпълняващ задълженията на „ССИ“; главен счетоводител; системен администратор и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни на магистратите, при спазване на принципа „необходимост да знае“.
7.	**Носители на**	Хартиен и технически носител.

	данни	
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение (ВСС; ИВСС, НИП, НОИ, НАП и др.); служба по трудова медицина; както и на обработващи лични данни, във връзка с командироване на магистрати. Данните от регистъра могат да се предоставят и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	При командироване на магистрати, като предоставените данни са само за физическата и социалната идентичност на лицата. Предоставянето се извършва при прилагане на глава V от Регламент (ЕС) 2016/679.
10.	**Къде се съхраняват данните**	Деловодство; регистратура „КИ“; в служебен кабинет на „човешки ресурси“; в архив.
11.	**Срок на съхранение**	- 10 години след прекратяване правоотношението със съответния съдия; - съгласно ПАС, личните данни, които са обработени във връзка с правораздаването: по съдебните дела – 10 години; по присъдите и решенията – 10 години, след което се предават в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; оригиналните заповеди, описните книги и азбучниците – 100 години, предават се в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; книгите за открити и закрити заседания – 25 години. Ведомости за заплати – 50 години; Лични данни, обработени във връзка със счетоводна информация – в сроковете по чл. 12 от ЗС. Лични данни, обработени във връзка с

		класифицирана информация – в сроковете по ЗЗКИ.
12.	**Общо описание на мерките**	Физическа защита; персонална защита; документална защита; защита на АИС и мрежи.

II. РЕГИСТЪР „СЪДЕБНИ СЛУЖИТЕЛИ“

1.	**Цели на обработването**	1. в изпълнение на ЗСВ; Кодекс на труда (КТ); ЗЗД, КСО, ЗС, ЗДДФЛ, ЗЗКИ, ЗБУТ, Закон за противодействие на корупцията и за отнемане на незаконно придобито имущество (ЗПКОНПИ), Наредба за командировките в страната и др. 2.Индивидуализиране на трудови и граждански правоотношения; 3.за служебни цели: - за всички дейности, свързани с възникване, изменение и прекратяване на трудовите и граждански правоотношения; - за изготвяне на всякакви документи на лицата във връзка с трудовите им правоотношения (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др.); - за установяване на връзка с лицето, за изпращане на кореспонденция, отнасяща се до изпълнението на задълженията им по трудови или граждански договори; - за водене на счетоводна отчетност, удържане на дължими данъци и други дейности по трудови правоотношения; - за командироване на лицата при изпълнение на служебните им задължения.
2.	**Правно основание**	Чл. 6, пар. 1, б. „б“ и „в“ от Регламент (ЕС) 2016/679 – за изпълнение на договор, по който субектът на данните е страна; обработването е необходимо за спазване на законово задължение, което се прилага спрямо администратора.

3.	**Категории субекти**	Съдебни служители в Софийския военен съд
4.	**Категории лични данни**	1. физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др. 2. социална идентичност: данни относно образование (учебно заведение, образователна степен, допълнителни квалификации и специализации), трудова дейност, стаж, професионална биография, атестация, ранг, награди и поощрения, дисциплинарни наказания; 3. семейна идентичност – данни относно семейното положение на лицата (наличие на брак, развод, брой и имена на членове на семейството, в това число деца до 18 години); 4. икономическа идентичност – данни относно имотното и финансово състояние на лицата; 5. лични данни относно съдебното минало на лицата; 6. данни за здравословното състояние на лицата.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления, рапорти, предложения и др. или в документи, предоставяни от други органи.
6.	**Обработващ данните**	Длъжностни лица – съдебен администратор; човешки ресурси; деловодител; деловодител „КИ“; служител, изпълняващ задълженията на „ССИ“; главен счетоводител; системен администратор и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни, при спазване на принципа „необходимост да знае“.
7.	**Носители на данни**	Хартиен и технически носител.
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение (ВСС; ИВСС, НИП, НОИ, НАП и др.); служба по трудова медицина; както и на обработващи лични данни, във връзка с командироване на съдебни служители. Данните от регистъра могат да се предоставят и на определени кредитни институции (банки) във

		връзка с изплащането на дължимите възнаграждения на физическите лица. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	При командироване на съдебни служители, като предоставените данни са само за физическата и социалната идентичност на лицата. Предоставянето се извършва при прилагане на глава V от Регламент (ЕС) 2016/679.
10.	**Къде се съхраняват данните**	Деловодство; регистратура „КИ“; в служебен кабинет на „човешки ресурси“; в архив.
11.	**Срок на съхранение**	- 10 години след прекратяване правоотношението със съответния съдебен служител; - съгласно ПАС, личните данни, които са обработени във връзка с правораздаването: по съдебните дела – 10 години; по присъдите и решенията – 10 години, след което се предават в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; оригиналните заповеди, описните книги и азбучниците – 100 години, предават се в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; книгите за открити и закрити заседания – 25 години. Ведомости за заплати – 50 години. Лични данни, обработени във връзка със счетоводна информация – в сроковете по чл. 12 от ЗС. Лични данни, обработени във връзка с класифицирана информация – в сроковете по ЗЗКИ.
12.	**Общо описание на мерките**	Физическа защита; персонална защита; документална защита; защита на АИС и мрежи.

III. РЕГИСТЪР „СЪДЕБНИ ЗАСЕДАТЕЛИ И ВЕЩИ ЛИЦА“

1.	**Цели на обработването**	Изпълнение на нормативните изисквания на ЗСВ, ЗОВСРБ, НПК, КСО, ЗС, ЗДДФЛ, ЗЗКИ Наредба № 7 от 28.09.2017 г., издадена от ВСС (обн. ЗВ, бр. 81 от 10.10.2017 г.); Наредба № 2 от 29.06.2015 г. за вписването, квалификацията и възнагражденията на вещите лица, издадена от министъра на правосъдието (обн., ДВ, бр. 50 от 3.07.2015 г., изм., бр. 28 от 8.04.2016 г., изм. и доп., бр. 82 от 5.10.2018 г.) и др.
2.	**Правно основание**	Чл. 6, пар. 1, б. „в“ и б. „д“ от Регламент (ЕС) 2016/679 – спазване на законово задължение, което се прилага спрямо администратора и упражняване на официални правомощия, които са предоставени на администратора.
3.	**Категории субекти**	Съдебни заседатели и кандидати за съдебни заседатели; вещи лица и кандидати за вещи лица.
4.	**Категории лични данни**	1. физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др. 2. социална идентичност: данни относно образование (учебно заведение, образователна степен, допълнителни квалификации и специализации), трудова/служебна дейност, стаж, професионална биография, атестация, ранг, военно звание, награди и поощрения, дисциплинарни наказания; 3. икономическа идентичност – данни относно имотното и финансово състояние на лицата; 5. лични данни относно съдебното минало на лицата; 6. данни за здравословното състояние на лицата.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления, рапорти, предложения и др. или в документи, предоставяни от органи на съдебна власт при провеждане на нормативно регламентирани процедури, както и от други органи – военни формирования, учебни заведения, научни институти и др.

6.	**Обработващ данните**	Длъжностни лица – магистрати; човешки ресурси; главен счетоводител; деловодител; деловодител „КИ“; съдебен служител, изпълняващ задълженията на „ССИ“; системен администратор и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни на магистратите, при спазване на принципа „необходимост да знае“
7.	**Носители на данни**	Хартиен и технически носител.
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение (органи на съдебна власт; ВСС; ИВСС, НИП, НОИ, НАП и др). Данните от регистъра могат да се предоставят и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	Предоставянето се извършва при прилагане на глава V от Регламент (ЕС) 2016/679.
10.	**Къде се съхраняват данните**	Деловодство; в служебен кабинет на „човешки ресурси“; регистратура „КИ“; в архив.
11.	**Срок на съхранение**	- 10 години; - съгласно ПАС, личните данни, които са обработени във връзка с правораздаването: по съдебните дела – 10 години; по присъдите и решенията – 10 години, след което се предават в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; оригиналните заповеди, описните книги и азбучниците – 100 години, предават се в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; книгите за открити и закрити заседания – 25 години. Лични данни, обработени във връзка със счетоводна информация – в сроковете по чл. 12

		от ЗС. Лични данни, обработени във връзка с класифицирана информация – в сроковете по ЗЗКИ.
12.	**Общо описание на мерките**	Физическа защита; персонална защита; документална защита; защита на АИС и мрежи.

IV. РЕГИСТЪР „УЧАСТНИЦИ В КОНКУРСНИ ПРОЦЕДУРИ В АДМИНИСТРАЦИЯТА НА СОФИЙСКИЯ ВОЕНЕН СЪД“

1.	**Цели на обработването**	Индивидуализиране, допускане и участие на физически лица в обявени конкурси за заемане на длъжност в администрацията на Софийския военен съд; ЗСВ; КТ и др.
2.	**Правно основание**	Чл. 6, пар. 1, б. „б“ и б. „в“ от Регламент (ЕС) 2016/679 - за предприемане на стъпки по искане на субекта на данните преди сключване на договор страна; обработването е необходимо за спазване на законово задължение, което се прилага спрямо администратора.
3.	**Категории субекти**	Физически лица – кандидати за съдебни служители в Софийския военен съд.
4.	**Категории лични данни**	1. физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др. 2. социална идентичност: данни относно образование (учебно заведение, образователна степен, допълнителни квалификации и специализации), трудова дейност, стаж, професионална биография, атестация, ранг, награди и поощрения, дисциплинарни наказания; 3. семейна идентичност – данни относно семейното положение на лицата (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години); 4. лични данни относно съдебното минало на лицата; 6. данни за здравословното състояние на лицата.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления и др. документи,

		или в документи, предоставяни от други органи.
6.	**Обработващ данните**	Длъжностни лица – съдебен администратор; човешки ресурси; системен администратор и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни на магистратите, при спазване на принципа „необходимост да знае“
7.	**Носители на данни**	Хартиен и технически носител.
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	Предоставянето се извършва при прилагане на глава V от Регламент (ЕС) 2016/679.
10.	**Къде се съхраняват данните**	Деловодство; в служебен кабинет на „човешки ресурси“; в архив.
11.	**Срок на съхранение**	- 6 месеца след провеждане на конкурсната процедура – за кандидати, които с които не са сключени трудови договори. - в сроковете, определени в регистър II, графа 11 от настоящото Приложение – за лицата, с които са сключени трудови договори.
12.	**Общо описание на мерките**	Физическа защита, персонална защита, документална защита, защита на АИС и мрежи.

V. РЕГИСТЪР „СЧЕТОВОДСТВО, ФИНАНСОВА ДЕЙНОСТ И КОНТРАГЕНТИ“

1.	**Цели на обработването**	Изплащане на трудовите възнаграждения на магистрати и съдебни служители; изплащане на възнаграждения на съдебни заседатели; вещи лица и пътни разноски на свидетели; изплащане на суми по предоставени услуги, съгласно сключени договори. ЗСВ; КТ; ЗЗД, КСО, ЗС, ЗДДФЛ, ЗЗКИ, ЗБУТ,

		НПК, Наредба за командировките в страната и др.
2.	**Правно основание**	Чл. 6, пар. 1, б. „б“ и б. „в“ от Регламент (ЕС) 2016/679 – за изпълнение на договор, или за предприемане на стъпки преди сключване на договор и за спазване на законово задължение, което се прилага спрямо администратора
3.	**Категории субекти**	Магистрати и съдебни служители в Софийския военен съд; съдебни заседатели; вещи лица; свидетели по дела; физически лица - контрагенти
4.	**Категории лични данни**	1. физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др. 2. семейна идентичност – данни относно семейното положение на лицата (наличие на брак, развод, брой и имена на членове на семейството, в това число деца до 18 години); 4. икономическа идентичност – данни относно имотното и финансово състояние на лицата, вкл. банкова информация – за превеждане на начислените възнаграждения по банков път; 6. данни за здравословното състояние на лицата – за магистрати и съдебни служители; 7. данъчна и осигурителна информация.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления и други, предоставени от тях документи или в документи, предоставяни от други органи.
6.	**Обработващ данните**	Длъжностни лица – съдебен администратор; човешки ресурси; главен счетоводител; системен администратор; магистрати и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни на магистратите, при спазване на принципа „необходимост да знае“.
7.	**Носители на данни**	Хартиен и технически носител.
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение (ВСС; ИВСС, НИП, НОИ, НАП и др.); служба по трудова медицина; както и на обработващи лични данни, във

		връзка с командироване на магистрати и съдебни служители. Данните от регистъра могат да се предоставят и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	При командироване на магистрати и съдебни служители, като предоставените данни са само за физическата и социалната идентичност на лицата. Предоставянето се извършва при прилагане на глава V от Регламент (ЕС) 2016/679.
10.	**Къде се съхраняват данните**	Служебен кабинет на „главен счетоводител“; деловодство; служебен кабинет на „човешки ресурси“; в архив.
11.	**Срок на съхранение**	- лични данни, обработени във връзка със събирането на счетоводна информация – в сроковете по чл. 12 от ЗС; - съгласно ПАС, личните данни, които са обработени във връзка с правораздаването: по съдебните дела – 10 години; по присъдите и решенията – 10 години, след което се предават в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; оригиналните заповеди, описните книги и азбучниците – 100 години, предават се в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; книгите за открити и закрити заседания – 25 години. Лични данни, обработени във връзка със счетоводна информация – в сроковете по чл. 12 от ЗС.
12.	**Общо описание на мерките**	Физическа защита; персонална защита; документална защита; защита на АИС и мрежи.

VI. РЕГИСТЪР „ЛИЧНИ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА, ПОДАЛИ МОЛБИ, ЗАЯВЛЕНИЯ, ЖАЛБИ, ПРЕДЛОЖЕНИЯ И ИСКАНИЯ“

1.	**Цели на обработването**	1. Изпълнение на нормативните изисквания на Конституцията на Република България, ЗСВ, НПК, АПК, ГПК, Закон за достъп до обществената информация (ЗДОИ), Закона за защита на личните дънни (ЗЗЛД), Наредба № 6 от 03.08.2016 г. за извършването на процесуални действия и удостоверителни изявления в електронна форма, издадена от ВСС (Обн., ДВ, бр. 67/18.08.2017 г.) и др.; 2. Извършване на процесуални действия и удостоверителни изявления в електронна форма. 3. за установяване на връзка с лицата.
2.	**Правно основание**	Чл. 6, пар. 1, б. „в“ и б. „д“ от Регламент (ЕС) 2016/679 – спазване на законово задължение, което се прилага спрямо администратора и упражняване на официални правомощия, които са предоставени на администратора
3.	**Категории субекти**	Физически лица, сезирали Софийския военен съд със заявления, молби, жалби, предложения, сигнали и др. извън пряката правораздавателна дейност по конкретни производства по делата в съда.
4.	**Категории лични данни**	1. физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др. 2. други данни, изисквани от специални закони, съобразно искането, както и данни, посочени от лицата в подадените от тях жалби, молби, заявления, искания, предложения, сигнали и др.
5.	**Източник на данните**	Предоставят се от физическите лица, като се съдържат в техни заявления и други, предоставени от тях документи или в документи, предоставяни от други органи.
6.	**Обработващ данните**	Длъжностни лица – магистрати, съдебен администратор; човешки ресурси; главен счетоводител; системен администратор;

		деловодител; деловодител „КИ“; съдебен секретар и други длъжностни лица, на които администраторът е възложил задачи по обработване на данни, при спазване на принципа „необходимост да знае“.
7.	**Носители на данни**	Хартиен и технически носител.
8.	**Категории получатели**	Държавни институции, с оглед изпълнение на нормативно задължение. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	Данните могат да се трансферират в трети държави с оглед изпълнение на задължение, произтичащо от нормативен акт.
10.	**Къде се съхраняват данните**	Деловодство; в архив.
11.	**Срок на съхранение**	- 10 години.
12.	**Общо описание на мерките**	Физическа защита; документална защита; персонална защита; защита на АИС и мрежи.

VII. РЕГИСТЪР „ПРАВОРАЗДАВАНЕ“

1.	**Цели на обработването**	Във връзка с основната дейност на СВС – правораздаване. Конституцията на РБ, ЗСВ, НПК, АПК, ГПК, Наредба № 6 от 03.08.2016 г. за извършването на процесуални действия и удостоверителни изявления в електронна форма, издадена от ВСС (Обн., ДВ, бр. 67/18.08.2017 г.) и др.
2.	**Правно основание**	Чл. 6, пар. 1, б. „в“ и б. „д“ от Регламент (ЕС) 2016/679 – спазване на законово задължение, което се прилага спрямо администратора и упражняване на официални правомощия, които са предоставени на администратора.
3.	**Категории субекти**	Страни (подсъдими; граждански ищци; граждански ответници; частни тъжители; частни

		обвинители; защитници) и участници (обвиняеми; пострадали; свидетели; повереници; вещи лица) в съдебните производства по дела, образувани и разглеждани в Софийския военен съд; адвокати.
4.	**Категории лични данни**	1. Физическа идентичност: имена; ЕГН, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка и др.; 2. социална идентичност: данни относно образование (учебно заведение, образователна степен, допълнителни квалификации и специализации), трудова дейност, стаж, професионална биография, атестация, ранг, военно звание, награди и поощрения, дисциплинарни наказания; 3. семейна идентичност – данни относно семейното положение на лицата (наличие на брак, развод, брой и имена на членове на семейството, в това число деца до 18 години); 4. икономическа идентичност – данни относно имотното и финансово състояние на лицата; 5. лични данни относно съдебното минало на лицата; 6. данни за здравословното състояние на лицата; 7. включително особено чувствителни лични данни по чл. 9, пар. 1 от Регламент (ЕС) 2016/679, във връзка с чл. 9, пар. 2, б. „е“ от Регламент (ЕС) 2016/679 – администраторът на данни действа в качество на правораздаващ орган; 7. други данни, изискващи се по закон или за изясняване на обстоятелствата по делото.
5.	**Източник на данните**	Предоставят се от физическите лица и от други органи на съдебна власт; органи на държавна и местна власт; учреждения и организации; други физически и юридически лица, във връзка с правораздавателната дейност.
6.	**Обработващ данните**	Длъжностни лица – магистрати, съдебен администратор; деловодител; деловодител „КИ“; съдебен секретар; главен счетоводител; системен администратор и други длъжностни лица, на които администраторът е възложил

		задачи по обработване на данни, при спазване на принципа „необходимост да знае“.
7.	**Носители на данни**	Хартиен и технически носител; Хартиени и електронни регистри; АИС и мрежи; дела на хартиен и електронен носител.
8.	**Категории получатели**	Органи на съдебна власт; държавни институции, с оглед изпълнение на нормативно правомощие. Данните от регистъра могат да се предоставят и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица и/или събиране на присъдени глоби, обезщетения, разноски и др.. Във връзка с ползването на куриерски услуги – приемане, пренасяне и доставка, и адресиране на пратките до физическите лица, необходимите данни могат да бъдат предоставяни.
9.	**Предаване в трети държави**	При наличие на нормативно основание.
10.	**Къде се съхраняват данните**	Деловодство; регистратура „КИ“; в архив
11.	**Срок на съхранение**	- съгласно ПАС, личните данни, които са обработени във връзка с правораздаването: по съдебните дела – 10 години; по присъдите и решенията – 10 години, след което се предават в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“ оригиналните заповеди, описните книги и азбучниците – 100 години, предават се в дирекция „Военноисторически архив“ към Държавна агенция „Архиви“; книгите за открити и закрити заседания – 25 години. Личните данни, обработени във връзка с класифицирана информация – в сроковете по ЗЗКИ.
12.	**Общо описание на мерките**	Физическа защита; документална защита; персонална защита; защита на АИС и мрежи.

VIII. РЕГИСТЪР „ВИДЕОНАБЛЮДЕНИЕ“

1.	**Цели на обработването**	Контрол на достъпа до служебни помещения - съхраняват се и се обработват лични данни чрез създаване на видеозапис от средства за наблюдение в регистратурата за класифицирана информация на Софийския военен съд
2.	**Правно основание**	Защита на легитимен интерес (чл. 6, пар. 1, т. „е“ от Регламент (ЕС) 2016/679)
3.	**Категории субекти**	Магистрати, служители и посетители
4.	**Категории лични данни**	Физическа идентичност: записи на образ и звук.
5.	**Източник на данните**	Физически лица – магистрати, служители и посетители.
6.	**Обработващ данните**	Системен администратор; служител по сигурността на информацията; деловодител – регистратура КИ.
7.	**Носители на данни**	технически средства, АИС мрежи, магнитен носител.
8.	**Категории получатели**	МВР; органи за охрана на съдебната власт; др. органи на съдебната власт.
9.	**Предаване в трети държави**	Данните могат да се трансферират в трети държави с оглед изпълнение на задължение, произтичащо от нормативен акт.
10.	**Къде се съхраняват данните**	Регистратура „КИ“; АИС и мрежи.
11.	**Срок на съхранение**	30 дни
12.	**Общо описание на мерките**	Физическа защита; персонална защита; защита на АИС и мрежи.

Приложение № 6
по чл.17, ал. 1, т. 1 от
Вътрешните правила за защита на личните данни в СВС

П Р О Т О К О Л

За проведено обучение/инструктаж по защита на личните данни

Тема на обучението:
..……
…….

Вид на инструктажа: ……..
(първоначален/периодичен; групов/индивидуален)

Лице по защита на данните: ……

№ по ред	дата	име	длъжност	подпис	Подпис на дл. лице по защита на данните	Подпис на адм. ръководител