

РЕПУБЛИКА БЪЛГАРИЯ
ВЪРХОВЕН АДМИНИСТРАТИВЕН СЪД



ЗАПОВЕД

№ 848

София, 24.02 2020г.

На основание чл.122, ал. 1 от Закона за съдебната власт във връзка с чл. 24 ал.1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО

И с оглед необходимостта от въвеждане на цялостен набор от мерки и действия за защита на личните данни, администрирани и обработвани от Върховния административен съд, при и по повод осъществяване на административната му дейност:

Р А З П О Р Е Ж Д А М :

1. Отменям Заповед № 1768 от 03.07.2019г. на Председателя на Върховния административен съд.

2. Утвърждавам Вътрешни правила за защита на личните данни във Върховния административен съд.

3. Настоящата Заповед да се сведе до знанието на ръководителите на Първа и Втора колегия, председателите на отделения, съдиите и всички събедни служители – за сведение и изпълнение.

4. Контрол по изпълнението възлагам на главния секретар и лицето изпълняващо функции на служител по сигурността на личните данни във Върховния административен съд.


ПРЕДСЕДАТЕЛ:

(Г. Чолаков)

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ВЪВ ВЪРХОВНИЯ АДМИНИСТРАТИВЕН СЪД

Раздел I Общи положения

Предмет

Чл. 1. С настоящите Вътрешни правила се създават условия и се въвеждат подходящи технически и организационни мерки с цел да се гарантира, че обработването на лични данни във Върховния административен съд се извършва в съответствие с принципите и изискванията на 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 свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) и на Закона за защита на личните данни (*изм. и доп., ДВ, бр. 17 от 26.02.2019 г.*).

Принципи при обработване на лични данни

Чл. 2. Обработването на лични данни във Върховния административен съд се осъществява при спазването на следните принципи:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, добросъвестно и по прозрачен начин по отношение на субекта на данни;

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

3. Свеждане на данните до минимум – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;

4. Точност - поддържане на данните 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;

5. Ограничение на съхранението – данните да се обработват и съхраняват във форма, която да позволява идентифицирането на субекта на данни за период не по-дълъг от необходимото за целите, за които се обработват данните, освен ако в специален закон не е предвиден друг срок. 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;

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

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже, че обработването се извършва в съответствие и при спазването на всички принципи и разпоредби, свързани с обработването на лични данни.

Условия за достъп и работа с лични данни

Чл. 3. Дейности и операции по обработване на лични данни се извършват само от лица, чиито служебни задължения или конкретно възложена задача налагат това, при спазване на принципа „Необходимост да знае“ и след запознаване с изискванията и разпоредбите на приложимата нормативната уредба в областта на защитата на данните, настоящите Вътрешни правила, политиката за поверителност, както и всички относими вътрешни нормативни актове, свързани с обработването на лични данни, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Информация, която се предоставя на субектите на данни при събирането и обработването на свързани с тях лични данни

Чл. 4. (1) Физическите лица - субекти на данни следва да бъдат информирани относно характера и параметрите на обработването на отнасящите се до тях лични данни. Изискванията за спазване на принципа на прозрачност се прилагат, както преди или в началото на процеса по обработване, така и през целия период на обработване на данните.

(2) Преди започване на обработването всяко физическо лице, трябва да бъде информирано за:

1. данните, които идентифицират администратора и координатите за връзка с него, както и координатите за връзка с длъжностното лице по защита на данните

2. целите на обработването и правното основание за обработването на данните;

3. получателите или категориите получатели, на които могат да бъдат разкривани данните;

4. информация за това дали личните данни ще бъдат предавани на трета държава или международна организация;

5. срока, за който ще се съхраняват личните данни или критериите за определяне на този срок;

6. информация за правото на достъп до личните данни и правото на коригиране, изтриване или ограничаване на обработването на данните, правото да се направи възражение срещу обработването и правото на преносимост на данните;

7. право на оттегляне на съгласието по всяко време, в случаите при които обработването на личните данни се основава на съгласие на лицето;

8. съществуването на автоматизирано вземане на решения, включително профилиране;

9. правото на жалба до надзорен орган – Комисията за защита на личните данни и до съда;

(3) В случаите когато обработваните лични данни не са получени от субекта, администраторът предоставя на съответното физическо лице информацията по ал. 2, т. 1 – 9, в т. ч. и информация за съответните категории лични данни, които се обработват в срок не по-късно от един месец от започване на обработването. В случай, че данните се използват за установяване на връзка със субекта на данни, предоставянето на информацията става най-късно при осъществяване на първия контакт с лицето.

(4) Информацията по ал. 1 се публикува на леснодостъпно място на електронната страница на Върховния административен съд и се поставя на видно място в сградата на съда.

Раздел II

Права на субектите на данни и ред за тяхното упражняване

Чл. 5. (1) Върховният административен съд в качеството си на администратор на лични данни осъществява съдействие на физическите лица при упражняване на правата им по Общия регламент относно защитата на данните, като предприема съответните технически и организационни мерки за това.

(2) Администраторът предоставя информация относно начините, по които субектите на данни могат да упражнят правата си по Общия регламент относно защитата на данните.

(3) Физическо лице – субект на данни има право:

1. да получи от администратора потвърждение дали се обработват негови лични данни, и ако това е така, да получи достъп до данните, както и информацията по чл. 4, ал. 2 и ал. 3 от настоящите правила;

2. да поиска от администратора да коригира или допълни неточни или непълни лични данни, отнасящи се до него;

3. да поиска изтриване на свързани с него лични данни, при наличието на предвидените за това основания;

4. да изиска от администратора ограничаване на обработването, в предвидените за това случаи;

5. да получи личните данни, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и пригоден за машинно четене формат и да прехвърли тези данни на друг администратор, когато обработването е основано на съгласие или е в изпълнение на договорно задължение;

6. на възражение срещу обработването на лични данни, ако обработването на данни се основава на изпълнение на задача от обществен интерес или при упражняването на официални правомощия от страна на администратора, както и за целите на легитимните интереси на администратора;

7. да не бъде обект на решение, основаващо се на изцяло автоматизирано обработване на данни, в т. ч. и профилиране;

(4) В случай, че е подадено заявление съдържащо искане за упражняване на някое от правата по ал. 3, длъжностното лице по защита на данните

уведомява председателя на Върховния административен съд за това в срок не по-късно от 3 (три) работни дни от постъпване на заявлението.

(5) Заявление може да се подаде и по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация.

(6) Приемането и регистрирането на заявления, получени по електронен път става в сроковете и по реда съгласно Вътрешните правила за приемане и регистриране на входяща кореспонденция, изпращане на призовки и съобщения по електронен път.

(7) Заявлението 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;

2. описание на искането;

3. предпочитана форма за получаване на информация при упражняване на правата по Общия регламент;

4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(8) При подаването на заявление от упълномощено лице към заявлението се прилага и пълномощното.

(9) Когато заявление съдържащо искане за упражняване на права по ал. 3 е подадено с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал информацията да се предостави по друг начин.

(10) Длъжностното лице по защита на данните предприема съответните действия и организира изпълнението на искането. При необходимост длъжностното лице може да изисква съдействие и от други служители на администратора.

(11) В случай, че установи искането за неоснователно, длъжностното лице изготвя становище. Становището се представя на председателя на Върховния административен съд, заедно с проект на отговор до лицето подало искането.

(12) В срок не по-късно от 30 (тридесет) дни от получаване на заявление, администраторът предоставя на заявителя информация за предприетите действия.

(13) При необходимост срокът по ал. 12 може да бъде удължен с още два месеца, като се вземат предвид сложността и броя на исканията. В случай на необходимост от удължаване на срока администраторът информира заявителя за всяко такова удължаване, като посочва и причините за това.

Чл. 6. В случай, че лични данни са предоставени от физическо лице без правно основание и/или в противоречие с принципите на Общия регламент, в срок от един месец от узнаването администраторът ги връща на лицето, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването и унищожаването на данните се документират.

Раздел III

Администратор, длъжностно лице по защита на данните и регистри с лични данни

Индивидуализиране на администратора на лични данни

Чл. 7. (1) Върховният административен съд е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните, със седалище и адрес на управление: град София 1301, бул. „Александър Стамболийски“ № 18. Адресът за кореспонденция и контакт е град София 1301, бул. „Александър Стамболийски“ № 18, работно време: понеделник – петък, 08:30 часа – 17:00 часа, електронна поща: edocuments@sac.iustice.bg

(2) Обработването на лични данни може да се извършва от обработващ лични данни от името на администратора. Взаимоотношенията между администратора и обработващия лични данни се уреждат с договор или друг правен акт, който е задължителен за обработващия лични данни спрямо администратора, и който регламентира предмета и срока на действие, естеството и целта на обработването, вида лични данни и категориите субекти на данни, както и правата и задълженията на администратора и обработващия лични данни.

(3) При съвместно обработване на лични данни между Върховния административен съд и друг администратор, отношенията помежду им се уреждат със споразумение по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информацията, посочена в чл. 5, ал. 2 и ал. 3 от настоящите правила, посредством договореност помежду си, 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.

Длъжностно лице по защита на данните

Чл. 8. (1) В качеството си на публичен орган Върховният административен съд определя длъжностно лице по защита на данните

(2) Длъжностно лице по защита на личните данни се определя от председателя на Върховния административен съд.

(3) Данни за контакт с длъжностното лице по защита на данните: Петър Петров – съдебен помощник във Върховния административен съд: град София 1301, бул. „Александър Стамболийски“ № 18, работно време: понеделник – петък, 08:30 часа – 17:00 часа, електронна поща: p.petrov@sac.iustice.bg

Чл. 9. (1) Длъжностното лице по защита на данните наблюдава за спазването на принципите и разпоредбите на Общия регламент и приложимото национално законодателство в областта на защитата на данните, както и спазването на настоящите правила. Информира и консултира администратора и служителите, които извършват дейности по обработване на данни за техните задължения.

(2) При необходимост длъжностното лице изготвя становища по въпроси, свързани с дейностите по обработване на данни. Консултира и дава съвети относно необходимостта от извършване на оценка на въздействието върху защитата на данните. Наблюдава и контролира извършването на оценката на въздействието.

(3) Предприема съответните действия и организира изпълнението на искания на физически лица за упражняване на техни права, съгласно Раздел II от настоящите правила.

(4) Длъжностното лице си сътрудничи с Комисията за защита на личните данни в качеството ѝ на надзорен орган на Република България по всички въпроси, предвидени в Общия регламент относно защитата на данните или произтичащи от други правни актове на Европейския съюз или от законодателството на Република България или по въпроси, инициирани от надзорния орган.

(5) Длъжностното лице си сътрудничи с Инспектората към Висшия съдебен съвет във връзка с функциите му по осъществяване на надзор и спазване на Общия регламент относно защитата на данните и на приложимото национално законодателство съгласно разпоредбите на глава трета от Закона за защита на личните данни (ЗЗЛД).

(6) Длъжностното лице действа като точка за контакт с надзорните органи по ал. 4 и ал. 5, по въпроси, свързани с обработването, включително предварителната консултация, посочена в чл. 36 от Общия регламент относно защитата на данните, и по целесъобразност се консултира по всякакви други въпроси.

(7) Длъжностното лице води регистър на дейностите по обработване на лични данни във Върховния административен съд, съгласно разпоредбата на чл. 30 от Общия регламент.

(8) Данните за контакт с длъжностното лице по защита на данните се обявяват на леснодостъпно място на електронната страница на Върховния административен съд и се съобщават на Комисията за защита на личните данни съгласно чл. 37, пар. 7 от Регламент (ЕС) 2016/679.

Регистри на лични данни

Чл. 10. (1) Във Върховния административен съд се обработват лични данни в следните регистри:

1. Регистър „Съдии във Върховния административен съд и административните съдилища“;
2. Регистър „Съдебни служители и участници в конкурсни процедури в администрацията на Върховния административен съд“;
3. Регистър „Лични данни на физически лица, страни и участници в производствата“;
4. Регистър „Лични данни на физически лица - податели на молби, жалби, предложения, сигнали, заявления и искания“;
5. Регистър „Контрагенти, обществени поръчки, търгове, стопанско-икономически правоотношения“;
6. Регистър „Видеонаблюдение“

Раздел IV

Регистър „Съдии във Върховния административен съд и административните съдилища“

Общо описание на регистъра

Чл. 11. В регистъра се обработват лични данни на съдии, назначени и командировани във ВАС и административните съдилища, с оглед изпълнение на нормативните изисквания на Закона за съдебната власт (ЗСВ),

Административнопроцесуалния кодекс, Гражданския процесуален кодекс, Наредба за служебните командировки и специализации в чужбина и други нормативни актове.

Категории лични данни, обработвани в регистъра.

Чл. 12. В регистъра се обработват следните лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес), месторождение, телефони за връзка и други;
2. социална идентичност: данни относно образование (учебно заведение, образователна степен и допълнителна квалификация и специализация), както и 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. икономическа идентичност – данни относно имотното и финансово състояние на лицата, банкова сметка;
5. лични данни относно съдебното минало на лицата;
6. данни за здравословното състояние на лицата;
7. данни за дейности и членства на лицата, съгласно чл. 195а от ЗСВ;
8. фотографски образ (снимка).

Технологично описание на регистъра

Чл. 13. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Данните в регистъра се предоставят от физическите лица като се съдържат в техни молби, предложения, заявления и др. или в документи, предоставяни от органи на съдебна власт при провеждане на нормативно регламентирани процедури.

(4) Данните в регистъра се съхраняват както следва:

- 3 (три) година след приключване на съответния конкурс;
- 10 (десет) години след прекратяване на правоотношенията със съответния съдия;
- съгласно Правилника за администрацията на Върховния административен съд, личните данни, които са въведени в съдебни актове, са със срок за съхранение, както следва:
 - а) свършените дела и други книжа – 10 години;
 - б) срочните книги, докладните книги и книгите за веществени доказателства – 25 години;

в) азбучните указатели и описните книги – 100 години, след изтичането на които същите се предават за съхранение в Централния държавен архив.

(5) Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 14. (1) Данните от регистъра се обработват от длъжностни лица от отдел „Финанси и счетоводство“, отдел „Човешки ресурси и правно обслужване“, отдел „Компютри и статистика“, сектор „Класифицирана информация“, служба „Архив“, служители, назначени към Кабинета на председателя и други, определени от председателя на Върховния административен съд служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на магистратите и кандидатите за магистрати, при спазване на принципа „Необходимост да се знае“.

(2) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Предоставяне на лични данни на трети лица

Чл. 15. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Министерство на правосъдието, Инспектората към Висшия съдебен съвет, Националния институт на правосъдието, Национална агенция за приходите, Национален осигурителен институт и т.н.),

(2) Данни от регистъра се предоставят на банкови институции във връзка с изплащане на трудови възнаграждения.

(3) Данните от регистъра могат да бъдат предоставяни на обработващи лични данни.

(4) Във връзка с използването на пощенски и куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(5) Данните от регистъра могат да се предават в други държави, извън ЕС и ЕИП единствено при командироване на магистрати, като предоставените данни са само за физическата и социалната идентичност на лицата. Предоставянето се извършва при прилагане на изискванията на глава V от Регламент (ЕС) 2016/679.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 16. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на председателя на Върховния административен съд.

(3) В комисията по ал. 2 задължително участва длъжностното лице по защита на данните.

(4) За резултатите от проверката се съставя доклад.

(5) Докладът по ал. 4 може да съдържа предложение за предприемане на допълнителни организационни и технически мерки за защитата на данните, в

случай че проверката установи необходимост от това. В този случай докладът се представя на председателя на Върховния административен съд за запознаване.

(6) Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 17. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Раздел V

Регистър „Съдебни служители и участници в конкурсни процедури в администрацията на Върховния административен съд“

Общо описание на регистъра

Чл. 18. В регистъра се обработват лични данни на всички служители, извън посочените в раздел IV, назначени на трудови, служебни или граждански правоотношения във Върховния административен съд.

Личните данни се обработват с цел:

1. изпълнение на нормативните изисквания на Конституцията на Република България, Закона за съдебната власт, Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за данъците върху доходите на физическите лица, Закона за безопасни условия на труд, Наредбата за служебните командировки и специализации в чужбина и др.

2. индивидуализиране на трудови, служебни и граждански правоотношения.

3. използване на събраните данни за съответните лица за служебни цели:

а) за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански правоотношения;

б) за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

в) за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори;

г) за водене на счетоводна отчетност, удържане на дължими данъци и други дейности относно възнагражденията на посочените по-горе лица по трудови и служебни правоотношения и граждански договори;

д) за командироване на лицата при изпълнение на служебните им ангажименти.

Категории лични данни, обработвани в регистъра

Чл. 19. В регистъра се обработват следните лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес), месторождение, телефони за връзка и други;

2. социална идентичност: данни относно образование (учебно заведение, образователна степен и допълнителна квалификация и специализация), както и трудова дейност, стаж, професионална биография и други;

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. икономическа идентичност – данни относно имотното и финансово състояние на лицата, банкова сметка;

5. лични данни относно съдебното минало на лицата;

6. данни за здравословното и психическото състояния на лицата, когато това е приложимо;

7. фотографски образ (снимка).

Технологично описание на регистъра

Чл. 20. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Личните данни в регистъра се предоставят от физическите лица при кандидатстване за заемана на определена длъжност във Върховния административен съд, както и при последваща необходимост.

Данните на кандидатите за заемане на длъжност във Върховния административен съд се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(4) Данните в регистъра се съхраняват както следва:

- 50 (петдесет) години – за документи, свързани с възникването, изменението и прекратяването на трудови правоотношения (трудова книжка);

- 3 (три) години за протоколи от проведени конкурси на кандидати за работа;

- 5 (пет) години след прекратяване на правоотношението – за трудови досиета на служители в администрацията на ВАС;

- 6 (шест) месеца – документи на кандидати за работа в администрацията, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок. След изтичането на този срок съхраняваните документи с лични

данни се връщат на кандидата, при поискване от негова страна или се изтриват и унищожават, освен ако специален закон предвижда друго.

Съгласно Правилника за администрацията на Върховния административен съд, личните данни, които са въведени в съдебни актове, са със срок за съхранение, както следва:

а) свършените дела и други книжа – 10 години;
б) срочните книги, докладните книги и книгите за веществени доказателства – 25 години;

в) азбучните указатели и описните книги – 100 години, след изтичането на които същите се предават за съхранение в Централния държавен архив.(5)
Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър, само ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 21. (1) Данните от регистъра се обработват от *главния секретар и длъжностни лица от дирекция „Финанси и управление на съдебното имущество“, отдел „Финанси и счетоводство“, отдел „Човешки ресурси и правно обслужване“, отдел „Компютри и статистика“, сектор „Класифицирана информация“, служба „Архив“, служители, назначени към Кабинета на председателя и други, определени от председателя на Върховния административен съд служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на съдебните служители, при спазване на принципа „Необходимост да се знае“.*

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

Предоставяне на лични данни на трети лица

Чл. 22. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение (Националния осигурителен институт, Национална агенция за приходите и други).

(2) Данни от регистъра се предоставят на банкови институции във връзка с изплащане на трудови възнаграждения.

(3) Данните от регистъра могат да бъдат предоставяни на обработващи лични данни.

(4) Във връзка с използването на пощенски и куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(5) Данните от регистъра могат да се предават в други държави, извън ЕС и ЕИП единствено при командироване на магистрати, като предоставените данни са само за физическата и социалната идентичност на лицата. Предоставянето се извършва при прилагане на изискванията на глава V от Регламент (ЕС) 2016/679.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 23. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на председателя на Върховния административен съд.

(3) В комисията по ал. 2 задължително участва длъжностното лице по защита на данните.

(4) За резултатите от проверката се съставя доклад.

(5) Докладът по ал. 4 може да съдържа предложение за предприемане на допълнителни организационни и технически мерки за защитата на данните, в случай че проверката установи необходимост от това. В този случай докладът се представя на председателя на Върховния административен съд за запознаване.

(6) Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 24. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Раздел VI

Регистър „Лични данни на физически лица, страни и участници в производствата“

Общо описание на регистъра

Чл. 25. (1) В регистъра се обработват лични данни на физически лица, които са страни или участници в административните производства.

Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Конституцията на Република България, Административнопроцесуалния кодекс, Гражданския процесуален кодекс, Закон за съдебната власт

2. за установяване на връзка с лицата.

Категории лични данни, обработвани в регистъра.

Чл. 26. (1) В регистъра се обработват следните лични данни:

1. Физическа идентичност – име, адрес, телефон, ЕГН, паспортни данни и други.
2. Икономическа идентичност – данни относно имотното и финансово състояние на лицето, в зависимост от съдържанието на жалбата, искането и т.н.
3. Социална идентичност – данни относно образование, трудова дейност и други като същите са в зависимост от съдържанието на жалбата, искането и т.н.
4. Лични данни относно съдебното минало на лицата.
5. Лични данни относно здравословното състояние на лицата – медицински документи, експертизи, медицински епикризи, документи от трудово експертни лекарски комисии и др.
6. Други данни, посочени от лицата в подадените от тях жалби

Технологично описание на регистъра

Чл. 27. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Личните данни в регистъра се предоставят от физически лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Данните в регистъра се съхраняват както следва:

Съгласно Правилника за администрацията на Върховния административен съд, личните данни, които са въведени в съдебни актове, са със срок за съхранение, както следва:

- а) свършените дела и други книжа – 10 години;
- б) спрочните книги, докладните книги и книгите за веществени доказателства – 25 години;
- в) азбучните указатели и описните книги – 100 години, след изтичането на който същите се предават за съхранение в Централния държавен архив.

(5) Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър, само ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 28. (1) Данните от регистъра се обработват от магистратите, главния секретар и от длъжностни лица от дирекция „Финанси и управление на съдебното имущество“, отдел „Финанси и счетоводство“, отдел „Човешки ресурси и правно обслужване“, отдел „Компютри и статистика“, сектор „Класифицирана информация“, служба „Архив“, служители, назначени към Кабинета на председателя и други, определени от председателя на Върховния административен съд служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на страни и участници в административните и съдебни производства, при спазване на принципа „Необходимост да се знае“.

(2) Лицата по ал. 1 нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Предоставяне на лични данни на трети лица

Чл. 29. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на задължение, произтичащо от нормативен акт, при спазване на баланса и защитимия интерес, съобразно Регламент (ЕС) 2016/679.

(2) Във връзка с използването на пощенски и куриерски услуги - приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(3) Данните от регистъра могат да се предават в други държави, извън ЕС и ЕИП с оглед изпълнение на задължение, произтичащо от нормативен акт. Предоставянето се извършва при прилагане на изискванията на глава V от Регламент (ЕС) 2016/679.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 30. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на председателя на Върховния административен съд.

(3) В комисията по ал. 2 задължително участва длъжностното лице по защита на данните.

(4) За резултатите от проверката се съставя доклад.

(5) Докладът по ал. 4 може да съдържа предложение за предприемане на допълнителни организационни и технически мерки за защитата на данните, в случай че проверката установи необходимост от това. В този случай докладът се представя на председателя на Върховния административен съд за запознаване.

(6) Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учреденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 31. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването

технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Раздел VII

Регистър „Лични данни на физически лица – податели на молби, жалби, предложения, сигнали, заявления и искания“

Общо описание на регистъра

Чл. 32. (1) В регистъра се обработват лични данни на физически лица, сезирали Върховния административен съд и неговата администрация молби, жалби, предложения, сигнали, заявления и искания, които нямат качеството страни и/или участници в производствата пред съда.

Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Конституцията на Република България, Административнопроцесуалния кодекс, Гражданския процесуален кодекс, Закон за съдебната власт, Закон за достъп до обществена информация, Закон за защита на личните данни, Кодекс на труда и други.
2. за установяване на връзка с лицата.

Категории лични данни, обработвани в регистъра.

Чл. 33. (1) В регистъра се обработват следните лични данни:

1. Физическа идентичност – име, адрес, телефон, ЕГН, паспортни данни и други.
2. Икономическа идентичност – данни относно имотното и финансово състояние на лицето, в зависимост от съдържанието на жалбата, искането и т.н.
3. Социална идентичност – данни относно образование, трудова дейност и други като същите са в зависимост от съдържанието на жалбата, искането и т.н.
4. Лични данни относно здравословното състояние на лицата – медицински документи, експертизи, медицински епикризи, документи от трудово експертни лекарски комисии и др., в зависимост от съдържанието на жалбата, искането и т.н.
5. Друга информация, която може да се дефинира като лични данни, посочена от лицата в техните жалби, молби, искания, предложения, сигнали, заявления и др. или в документи, предоставяни от държавни органи и органи на местното самоуправление.

Технологично описание на регистъра

Чл. 34. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и електронен носител.

(3) Личните данни в регистъра се предоставят от физически лица, за които се отнасят данните или от други лица в предвидените от нормативен акт случаи.

(4) Данните в регистъра се съхраняват както следва:
10 (десет) години – преписки, образувани по жалби, молби и сигнали на физически лица.

2. 5 (пет) години - преписки, образувани по заявления за достъп до обществена информация.

(5) Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър, само ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 35. (1) Данните от регистъра се обработват от магистратите, главния секретар и от длъжностни лица от дирекция „Финанси и управление на съдебното имущество“, отдел „Финанси и счетоводство“, отдел „Човешки ресурси и правно обслужване“, отдел „Компютри и статистика“, сектор „Класифицирана информация“, служба „Архив“, служители, назначени към Кабинета на председателя и други, определени от председателя на Върховния административен съд служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на страни и участници в административните и съдебни производства, при спазване на принципа „Необходимост да се знае“.

(2) Лицата по ал. 1 нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Предоставяне на лични данни на трети лица

Чл. 36. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на задължение, произтичащо от нормативен акт, при спазване на баланса и защитимия интерес, съобразно Регламент (ЕС) 2016/679.

(2) Във връзка с използването на пощенски и куриерски услуги - приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(3) Данните от регистъра могат да се предават в други държави, извън ЕС и ЕИП с оглед изпълнение на задължение, произтичащо от нормативен акт.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 37. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на председателя на Върховния административен съд.

(3) В комисията по ал. 2 задължително участва длъжностното лице по защита на данните.

(4) За резултатите от проверката се съставя доклад.

(5) Докладът по ал. 4 може да съдържа предложение за предприемане на допълнителни организационни и технически мерки за защитата на данните, в случай че проверката установи необходимост от това. В този случай докладът се представя на председателя на Върховния административен съд за запознаване.

(6) Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 38. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Раздел VIII

Регистър „Контрагенти, обществени поръчки, търгове и стопанско-икономически правоотношения“

Общо описание на регистъра

Чл. 39. В регистъра се обработват лични данни на физически лица в изпълнение на договори, по които Върховния административен съд е страна, както и при провеждане на процедури за задоволяване икономическите, социални и битови потребности на служителите във ВАС и експлоатация на учебните бази предоставени за управление на ВАС. Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Закона за съдебната власт, Закон за обществените поръчки, Закон за задълженията и договорите, Търговски закон и други;
2. управление на човешките ресурси, финансово-счетоводна дейност, осигуряване на материално-техническата база на ВАС и органите на съдебната власт;
3. за установяване на връзка с лицата.

Категории лични данни, обработвани в регистъра.

Чл. 40. В регистъра се обработват следните лични данни:

1. физическа идентичност: имена и паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес), телефони за връзка и други;

2. социална идентичност: данни относно образование, трудова дейност, стаж, професионална биография и други;

3. лични данни относно съдебното минало на лицата – само в изискуемите от нормативен акт случаи;

4. други нормативно изискуеми данни на лицата, съобразно целите на процедурите.

Технологично описание на регистъра

Чл. 41. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват на хартиен и технически носител.

(3) Личните данни в регистъра се предоставят от физическите лица при или преди встъпване в договорни отношения с Върховния административен съд.

(4) Данните в регистъра се съхраняват 5 (пет) години след прекратяване на договора и извършен одит. Договорите, сключени в изпълнение на проекти с европейско или международно финансиране, се съхраняват в определения за съответната програма срок.

(5) Администраторът предоставя достъп, справки, извлечения и други данни от съответния регистър, само ако е предвидено в нормативен акт.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 42. (1) Данните от регистъра се обработват от главния секретар и длъжностни лица от дирекция „Финанси и управление на съдебното имущество“, отдел „Финанси и счетоводство“, отдел „Човешки ресурси и правно обслужване“, отдел „Компютри и статистика“, сектор „Класифицирана информация“, отдел „Управление и стопанисване на съдебното имущество“, служба „Архив“, служители, назначени към Кабинета на председателя и други, определени от председателя на Върховния административен съд служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на лицата, при спазване на принципа „Необходимост да се знае“.

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

Предоставяне на лични данни на трети лица

Чл. 43. (1) Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на задължение, произтичащо от нормативен акт (Националния осигурителен институт, Национална агенция за приходите, Сметна палата и други).

(2) Данните от регистъра могат да бъдат предоставяни на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на физическите лица от този регистър.

(3) Във връзка с използването на пощенски и куриерски услуги – приемане, пренасяне и доставка и адресиране на пратките до физически лица, могат да бъдат предоставяни необходимите данни за тяхното извършване.

(4) Данните от регистъра могат да се предават в други държави, извън ЕС и ЕИП с оглед изпълнение на задължение, произтичащо от нормативен акт или в случай на изпълнение на проекти с финансиране от страни извън ЕС и ЕИП при условие, че изискванията на съответния проект налагат предаването на такива данни.

Срок за провеждане на периодични прегледи относно необходимостта от обработване/заличаване на данните

Чл. 44. (1) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в регистъра и относно необходимостта от по-нататъшното обработване.

(2) Проверката се извършва от комисия, назначена със заповед на председателя на Върховния административен съд.

(3) В комисията по ал. 2 задължително участва длъжностното лице по защита на данните.

(4) За резултатите от проверката се съставя доклад.

(5) Докладът по ал. 4 може да съдържа предложение за предприемане на допълнителни организационни и технически мерки за защитата на данните, в случай че проверката установи необходимост от това. В този случай докладът се представя на председателя на Върховния административен съд за запознаване.

(6) Докладът се предава на постоянно действаща експертна комисия, създадена в изпълнение на Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общински институции. Същата изготвя акт за унищожаване, който се изпраща в Централен държавен архив, като след потвърждаването му съответните документи подлежат на унищожаване.

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 45. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Раздел IX **Регистър „Видеонаблюдение“**

Общо описание на регистъра

Чл. 46. (1) Регистър „Видеонаблюдение“ се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на магистрати, служители и посетители към входа и на територията на сградата на Върховния административен съд, което се осъществява чрез технически средства за видеонаблюдение и видеозаснемане (камери).

(2) Информация относно наличието на видеонаблюдение се поставя на видно място в сградата на Върховния административен съд. Информацията по настоящата алинея следва да съдържа данни за използването на технически средства за наблюдение на достъпа и движението в сградата, без да се уточнява тяхното местоположение.

Категории лични данни, обработвани в регистъра.

Чл. 47. Регистър „Видеонаблюдение“ съдържа информация в записите, създадени чрез техническите средства за видеонаблюдение, способна да разкрие физическата идентичност на лицето, което е записано.

Технологично описание на регистъра

Чл. 48. (1) Технологичното описание на регистъра обхваща носителите на данни, технологията на обработване, срока за съхраняване и предоставяните услуги по регистъра.

(2) Данните в регистъра се обработват само на технически носител - DVR устройство със собствен HDD.

(3) Записите от инсталираните технически средства за видеонаблюдение, могат да се предават само на органите, упражняващи компетенциите в областта на вътрешен ред, обществена сигурност и здравеопазване, при спазване на гаранциите и условията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета. За предаването на запис се съставя протокол.

Длъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните права и задължения

Чл. 49. (1) Данните от регистъра се обработват от главния секретар и началник отдел „ИСКСС“.

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

Действия след изтичане срока на съхранение на данните в регистъра

Чл. 50. (1) Срокът за съхранение на записите, създадени чрез техническите средства за видеонаблюдение е 1 (един) месец.

(2) Унищожаването на личните данни създадени чрез средствата за видеонаблюдение се извършва автоматично след изтичане на срока по ал. 1, чрез изтриване на записите.

Раздел X

Технически и организационни мерки за защита на данните

Физическа защита на личните данни

Чл. 51. Физическата защита на личните данни се осъществява при спазване на следните мерки:

1. Контрол на достъпа на външни лица в сградата на Върховния административен съд.

2. Личните данни се обработват в кабинетите на лицата, в чиито длъжностни характеристики е определено задължението за обработване на данни от определени регистри.

3. Помещенията, в които се обработват лични данни, са оборудвани със заключване на вратите.

4. Сградата на Върховния административен съд е оборудвана с пожарогасителни средства и пожароизвестителна система.

5. Елементите на комуникационно - информационните системи, използвани за обработване на лични данни, се намират в помещение с ограничен достъп.

6. Външни лица имат достъп до помещенията, в които се обработват лични данни, само в присъствието на упълномощени служители.

Персонална защита на личните данни

Чл. 52. Персоналната защита на личните данни се осъществява при спазване на следните мерки:

1. Лицата, обработващи лични данни, се запознават със Общия регламент за защита на данните, Закона за защита на личните данни, настоящите Вътрешни правила, както и с други нормативни актове, относими към съответната дейност по обработване.

2. Лицата, обработващи лични данни, 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.

3. Лицата, обработващи лични данни, се запознават с рисковете за физическите лица, които произтичат от обработването.

4. При участие в комисии, определени от председателя или главния секретар, лицата обработващи лични данни, в изпълнение на поставените задачи подписват декларация за неразгласяване на информацията на трети лица.

Документална защита на личните данни

Чл. 53. Документалната защита на личните данни се осъществява при спазване на следните мерки:

1. Регистрите с лични данни, обработвани от Върховния административен съд, се поддържат на хартиен или електронен носител.

2. Обработването на личните данни се извършва в рамките на работното време на Върховния административен съд.

3. Достъп до регистрите с лични данни, обработвани от Върховния административен съд, имат само служители, в чиито длъжностни характеристики е определено задължение за обработване на данните, при спазване на принципа „Необходимост да се знае“ или на които е поставена конкретна задача.

4. Личните данни се събират само за конкретни цели, в съответствие с нормативните изисквания към Върховния административен съд.

5. Сроковете за съхранение на личните данни от различните регистри е определен в утвърдената Номенклатура на делата със срокове за съхранение във Върховния административен съд.

6. Личните данни на хартиен носител се съхраняват в определените за целта служебни помещения в сградата на Върховния административен съд.

7. Архивирането на лични данни на хартиен носител се осъществява в съответствие със Закона за съдебната власт, Вътрешните правила за дейността на учредения архив във Върховния административен съд, Номенклатура на делата със срокове за съхраняване във Върховния административен съд и Закона за националния архивен фонд.

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

9. Работните варианти и излишните копия от документи и работни материали от регистрите, които са на хартиен носител и съдържат лични данни, се унищожават чрез машини за унищожаване на документи (шредер).

10. След изтичане на срока за съхранение документите от регистрите същите се унищожават. Унищожаването се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожаването технически възможности и вида на носителите на данни или Върховният административен съд възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Унищожаването се документира.

Защита на автоматизирани информационни системи и/или мрежи

Чл. 54. Защитата на автоматизирани информационни системи и мрежи се осъществява при спазване на следните мерки:

1. При работа с данните от регистрите, поддържани от Върховния административен съд се използват съответните софтуерни продукти за обработване. Данните се въвеждат в база данни и се съхраняват на сървър. Всеки упълномощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

2. Администраторът създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира, което включва стандартни и базови конфигурации за защита на операционната система, защитни стени, рутери и мрежови устройства. За защита на данните е инсталирана антивирусна програма и се извършва периодична профилактика на софтуера и системните файлове.

3. За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите данни, са осигурени непрекъсваеми токозахранващи устройства (UPS).

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

5. Организационни мерки за гарантиране нивото на сигурност:

а) Охрана на сградата на Върховния административен съд е денонощна и се осъществява от Главна дирекция „Охрана“;

б) Забранено е изнасянето на преносими лични носители на данни от сградата на съда.

в) Работните компютърни конфигурации, както и цялата ИТ инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели.

г) 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.

9. Отдалечен достъп до данни от регистрите се осъществява само от обработващи лични данни, с които Върховният административен съд има сключен договор.

Раздел XI

Оценка на въздействието върху защитата на данните

Чл. 55. (1) Оценка на въздействието върху защитата на данните се извършва, когато съществува вероятност определена дейност по обработване, по-специално обработване, при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица. Оценка на въздействието се извършва и за дейности по обработване, включени в списъка на видовете операции по обработване на лични данни, за които се изисква извършване на оценка на въздействието, съставен от Комисията за защита на личните данни, съгласно чл. 35, пар. 4 от Общия регламент.

(2) Длъжностното лице по защита на данните изготвя становище относно необходимостта от извършване на оценка на въздействието. Становището трябва да съдържа отговор най-малко на следните въпроси:

1. да се извърши или не оценка на въздействието;

2. каква методика да се използва при извършването на оценката на въздействие;

3. дали оценката на въздействие да се извърши от служители на администратора или да се възложи на външен изпълнител;

4. какви технически и организационни мерки да се приложат, с цел рисковете за правата и свободите на физическите лица да бъдат сведени до минимум;

(3) След извършване на оценка на въздействието, длъжностното лице изготвя становище дали оценката е извършена в съответствие с принципите и изискванията на Общия регламент.

(4) Оценката на въздействието върху защитата на данните следва да 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, 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.

(5) В случай, че оценката на въздействието покаже, че обработването ще породи висок риск за правата и свободите на физическите лица, ако администраторът не предприеме мерки за ограничаване на риска или рискът не може да бъде ограничен с прилагането на съответните технически и организационни мерки, които администратора счита за подходящи, преди планираното обработване следва да се извърши предварителна консултация с надзорния орган.

Раздел XII

Защита на данните на етапа на проектирането и по подразбиране

Чл. 56. Върховният административен съд в качеството си на администратор на лични данни въвежда както към момента на определяне на средствата за обработване, така и към момента на самото обработване на данни, подходящи технически и организационни мерки с оглед осигуряване съответствието на дейностите по обработване с принципите и изискванията за защита на личните данни. Това задължение се отнася както до видовете и обема на личните данни, които ще бъдат събрани, така и до степента на обработването, сроковете на съхраняването им и тяхната достъпност.

Чл. 57. Върховният административен съд въвежда технически и организационни мерки, за да гарантира и за да е в състояние на докаже, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните данни, характера на обработването, сроковете на тяхното съхранение и тяхната достъпност.

Раздел XIII

Процедура по уведомяване при установяване на нарушение на сигурността на личните данни

Чл. 58. (1) В случай на установено нарушение на сигурността на данните, служителят, констатирал инцидента, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен своевременно да информира главния секретар и длъжностното лице по защита на данните за нарушението.

(2) Уведомяването по ал. 1 се извършва писмено, по електронен път или по друг начин, който позволява да се установи неговото извършване. Уведомлението следва да съдържа описание на фактите и обстоятелствата, които са известни на този етап от установяване на нарушението.

(3) Длъжностното лице по защита на данните въз основа на наличната информация, извършва преценка, за това дали нарушението на сигурността на данните има вероятност да породи риск за правата и свободите на физическите лица, чийто данни са засегнати.

Чл. 59. (1) Длъжностното лице уведомява председателя на Върховния административен съд за нарушението на сигурността на данните. Уведомяването се извършва писмено, по електронен път или по друг начин, който позволява да се установи неговото извършване.

(2) Уведомлението по ал. 1 съдържа описание на фактите и обстоятелствата, които са известни на този етап от установяване на нарушението, становището на длъжностното лице относно наличието на вероятност нарушението да породи риск за правата и свободите на субектите на данни, както и предложение да се уведоми надзорния орган. В случай, че се установи вероятност нарушението да породи висок риск за правата и свободите на субектите на данни, длъжностното лице прави предложение за изготвяне на съобщение до физическите лица, чийто данни са засегнати.

(3) Длъжностното лице организира изпълнението на задължението на администратора за уведомяване на Комисията за защита на личните данни, в качеството и на надзорен орган.

(4) Уведомяването на Комисията за защита на личните данни следва да се извърши, когато това е осъществимо, не по-късно от 72 часа след узнаване за нарушението.

(4) Уведомлението до Комисията за защита на личните данни съдържа следната информация:

1. 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;

2. името и координатите за връзка на длъжностното лице по защита на личните данни;

3. описание на евентуалните последици от нарушението на сигурността;

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

(5) В случай, че уведомлението не бъде изпратено в срок не по-късно от 72 часа от узнаването за нарушението, се посочват причините за забавянето.

(6) Когато нарушението е установено при обработващ лични данни, администратора, в уведомлението по ал. 1 предоставя и данните за контакт с обработващия, както и координати на длъжностното лице по защита на данните на обработващия, ако е определено такова.

Чл. 60. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, длъжностното лице по защита на данните, без ненужно забавяне, организира съобщаването на засегнатите физически лица, чийто данни са компроментирани в следствие на нарушението.

Чл. 61. При съвместно обработване на данни с друг администратор, в споразумението за съвместно обработване на данни се определят отговорностите на администраторите относно спазване и реализиране на задълженията по чл. 33 и чл. 34 от Общия регламент относно защитата на данните.

Чл. 62. Длъжностното лице по защита на личните данни води регистър за нарушенията на сигурността, който съдържа следната информация:

1. дата на установяване на нарушението;
2. описание на нарушението - източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);
3. описание на извършените уведомления: уведомяване на Комисия за защита на личните данни и засегнатите лица, ако е било извършено;
4. предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни;
5. предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 63. 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.

ПРОТОКОЛ
за унищожаване на лични данни¹

Днес, ... 20.....г.
подписаният/ата
служител на длъжност/комисия в състав:
....., упълномощен със
Заповед № на/назначена със
Заповед № на да извърши унищожаване
на лични данни, част от регистър с лични данни „.....“ (описват
се видовете лични данни, които се унищожават/ брой записи с лични данни)
съставих/съставихме настоящия протокол за унищожаване на лични данни с
изтекъл срок на съхранение/получени без основание, включително и резервни
копия от тях, както следва:

1. Данни на магнитни носители за многократен запис, чрез трайно изтриване, вкл. презаписването на носителите.
2. Данни съхранявани на хартиен носител, чрез нарязване
3. Данни съхранявани на оптични носители за еднократен запис, чрез физическо унищожаване на носителите.
4. Данни получени чрез входяща кореспонденция по електронен път, чрез изтриване на електронното писмо (съобщение), в т.ч. и всички прикачени (добавени) файлове.

Унищожените данни не са обработвани чрез интернет услуги.

Служител/Комисия в състав:
/...../

¹ Този протокол се прилага и в случаите, при които се унищожават/изтриват лични данни, предоставени от субект на данни без правно основание или в противоречие с принципите на Общия регламент относно защитата на данните, ако връщането им е невъзможно или изисква несъразмерно големи усилия

Приложение № 2
към чл. 59, ал. 4
от Вътрешните правила
за защита на личните данни
във Върховния административен съд

ОБРАЗЕЦ НА УВЕДОМЛЕНИЕ ДО НАДЗОРНИЯ ОРГАН ЗА НАРУШЕНИЕ НА
СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

До:

Комисия за защита на личните данни

Адрес: гр. София 1592, бул. „Проф. Цветан Лазаров“ № 2

На вниманието на:

Данни за администратора:

Върховен административен съд

Адрес: гр. София 1301, бул. „Александър Стамболийски“ № 18

електронна поща: edocuments@sac.iustice.bg

Данни за контакт с длъжностно лице по защита на данните:

Три имена

Телефон:

e-mail:

Адрес: гр. София 1301, бул. „Александър Стамболийски“ № 18,

Описание на естеството на нарушението на сигурността на личните данни:

.....
.....

Дата и час на узнаване:

Причини за забавяне на уведомяването: (ако е приложимо)

Описание:

.....
.....

Категории лични данни, които са засегнати от нарушението:

.....
.....

Засегнати субекти: (описват се категориите субекти и приблизителен брой)

.....
.....

Засегнати записи на лични данни: (приблизителен брой на засегнатите записи)

.....
.....

Последици от нарушението на сигурността на личните данни: (описват, както

установените последици (ако има такива), така и потенциалните, които могат да настъпят)

Поетапно уведомяване² (ако е приложимо)

Предприети или предложени мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност, мерки за намаляване на евентуалните неблагоприятни последици:

Доказателства: (описание)

Оценка на риска/технически и организационни мерки:

Дата:

подпис:

² Съгласно чл. 33, пар. 4 от Общия регламент относно защитата на данните, когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.