З А П О В Е Д

№ РД – 84
гр. Пловдив, 16.03.2026 г.

На основание чл. 93, ал. 1, т. 1 и ал. 2 от ЗСВ, във връзка с прилагането на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), както и във връзка с, както и във връзка с прилагането на ЗЗЛД, който урежда обществените отношения, свързани със защитата на правата на физическите лица при обработване на личните им данни, доколкото същите не са уредени в Регламента, както и във връзка със заповед № РД – 787/07.10.2024 г. на председателя на утвърдени със заповед № 713/19.09.2019 г. на председателя на Административен съд – Пловдив

Н А Р Е Ж Д А М :

1. ОТМЕНЯМ изцяло Вътрешни правила за мерките и средствата за защита на личните данни, обработвани в Административен съд – Пловдив, утвърдени със заповед № 713/19.09.2019 г. на председателя на Административен съд – Пловдив.

2. УТВЪРЖДАВАМ нови Вътрешни правила за мерките и средствата за защита на личните данни, обработвани в Административен съд – Пловдив.

3. ИЗМЕНЯМ Политика на информираност за защита на личните данни, прилагана в Административен съд – Пловдив, утвърдена със заповед № 713/19.09.2019 г. на председателя на Административен съд – Пловдив по следния начин:

3.1. В част I Данни за администратора и за контакт с него, т. 1.2., изр. 3 се променя длъжностното лице по защита на личните данни като вместо И. Д. се вписва Д. Д. – системен администратор. Съдебният помощник Л. А. Г. ще оказва съдействие на длъжностното лице по защита на личните данни и да го замества при отсъствие.

3.2. В част III Получатели на лични данни, т. 3.1. думите „Комисия за противодействие на корупцията и за отнемане на незаконно придобито имущество“ се заменят със „Сметната палата“.

4. Възлагам на административния секретар да запознае съдиите и съдебните служители с новите Вътрешни правила за мерките и средствата за защита на личните данни, обработвани в Административен съд – Пловдив, и с промените в Политиката на информираност за защита на личните данни, прилагана в Административен съд – Пловдив, след което да се публикуват на интернет страницата на съда от системния администратор.

Настоящата заповед да се сведе до знанието на всички съдии и съдебни служители при Административен съд – Пловдив за сведение и изпълнение.

ПРЕДСЕДАТЕЛ
НА АДМИНИСТРАТИВЕН СЪД -
ПЛОВДИВ: /П/
/МАРИАНА ШОТЕВА/

УТВЪРДИЛ: /П/
/МАРИАНА ШОТЕВА – ПРЕДСЕДАТЕЛ
НА АДМИНИСТРАТИВЕН СЪД – ПЛОВДИВ/

ВЪТРЕШНИ ПРАВИЛА ЗА МЕРКИТЕ И
СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ,
ОБРАБОТВАНИ В АДМИНИСТРАТИВЕН СЪД – ПЛОВДИВ

I. ОБЩИ ПОЛОЖЕНИЯ

Предмет

Чл. 1. Тези Вътрешни правила уреждат условията и реда за обработване на лични данни, водене на регистри на лични данни, минималното ниво на технически и организационни мерки за

тяхната защита, както и упражняването на контрол при обработването на лични данни в Административен съд – Пловдив.

Понятия

Чл. 2. (1) „Лични данни" означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни" означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(3) „Обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

(4) „Регистър с лични данни" представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

(4а) „Специални категории лични данни" са такива които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, по смисъла на чл. 9, пар. 1 от Общ регламент относно защитата на данните 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.

(4б) „Принцип необходимост да се знае" означава да се достъпват лични данни на субектите само ако това е необходимо за изпълнение на служебните задължения и /или за изпълнение на конкретна служебна задача. Достъпът до личните данни на субектите е ограничен само до кръга на лицата, на които са възложени функции, чието изпълнение е невъзможно да бъде осъществено без достъп.

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

(6) „Получател на лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не.

Принципи при обработване на лични данни

Чл. 3. При обработването на лични данни в Административен съд – Пловдив се спазват следните принципи:

1. Законосъобразност, добросъвестност и прозрачност – обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране 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 на обработването;
4. 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;
5. 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;
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 спазването на всички принципи, свързани с обработването на лични данни.

Условия за достъп до лични данни

Чл. 4. (1) Право на достъп до регистрите с лични данни имат само магистратите и съдебните служители в Административен съд – Пловдив, съобразно възложените им от закона правомощия и нормативно определените им функции, както и обработващите лични данни, на които Административен съд – Пловдив е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните (напр. Служба по трудова медицина).

(2) Съдиите и съдебните служители носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от щатния състав може да бъде основание за налагане на дисциплинарни санкции на съответните длъжностни лица.

(3) Съдиите и съдебните служители нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения.

Права на физическите лица при обработване на отнасящи се за тях лични данни

Чл. 5. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, следва да бъде уведомено за:

1. данните, които идентифицират администратора;

2. целите на обработването на личните данни и правното основание за обработването;

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

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

5. срока за съхранение на личните данни;

6. за правото на достъп и правото на коригиране, изтриване или ограничаване на обработването на събраните данни, правото на възражение и правото на преносимост при условията на Регламент (ЕС) 2016/679 - Общия регламент относно защитата на данните;

7. правото на оттегляне на съгласието по всяко време, когато обработването на личните данни се основава на съгласие на лицето;

8. правото на жалба до надзорен орган - Комисията за защита на личните данни, когато се касае до обработка на лични данни от Административен съд - Пловдив в качеството му на

обикновен администратор или до Инспектората към Висшия съдебен съвет, когато се касае за обработка на лични данни от Административен съд - Пловдив при изпълнение на функциите му на орган на съдебната власт;

9. източника на данните;

10. съществуване на автоматизирано вземане на решения, включително профилиране.

(2) Алинея 1 не се прилага, когато:

1. обработването е за статистически, исторически или научни цели и предоставянето на данните по ал. 1 е невъзможно или изисква прекомерни усилия;

2. вписването 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 в закон.

(3) Информацията по ал. 1 се обявява на леснодостъпно място на електронната страница на Административен съд – Пловдив.

Чл. 6. (1) Всяко физическо лице, чийто лични данни ще се обработват от администратора, съгласно Регламент (ЕС) 2016/679 притежава следните права:

1. Информираност;
2. Право на достъп;
3. Право на коригиране;
4. Право на изтриване (право “да бъдеш забравен”);
5. Право на ограничаване на обработването;
6. Право на преносимост на данните;
7. Право на възражение;
8. Право на лицето да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включително профилиране.

Чл. 7. (1) Администраторът на лични данни може да откаже предоставяне на информация в случаите на чл. 54, ал. 3 от ЗЗЛД, а именно, когато упражняването създава риск за:

1. националната сигурност, отбраната, обществения ред и сигурността;
2. предотвратяване, разследване, наказателно преследване на престъпления и изпълнение на наложените наказания;

3. други важни цели от широк обществен интерес (парични, бюджетни, данъчни въпроси, обществено здраве, социална сигурност);

4. защитата на независимостта на съдебната власт и съдебните производства;

5. предотвратяване, разследване, разкриване и преследване на нарушения на етичните кодекси на регулираните професии;

6. защита на субекта на данните или на правата и свободите на други лица;

7. изпълнение на гражданскоправни искове.

След отпадане на някое от посочените обстоятелства администраторът предоставя без забавяне исканата информация в срока по чл. 53, ал. 3 от ЗЗЛД - в срок до два месеца от получаване на искането, като срокът може да се удължи с още един месец, когато това се налага заради сложността или броя на исканията.

(2) Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, които го засягат, и ако това е така, да получи достъп до тях, както и информация за:

1. обстоятелствата по чл. 54, ал. 1, т. 3 - 5 и ал. 2, т. 1 – 3 от ЗЗЛД;

2. обработваните категории лични данни;

3. личните данни, които са в процес на обработване, и всякаква налична информация за техния произход, освен ако тя е защитена от закон тайна.

(3) Правото на достъп до данните и информацията чл. 54, ал. 1 от ЗЗЛД може да се ограничи изцяло или частично, като се отчитат основните права и законните интереси на засегнатото физическо лице в случаите по чл. 54, ал. 3 от ЗЗЛД. В тези случаи се прилага чл. 54, ал. 4 от ЗЗЛД.

В случаите по ал. 3 администраторът информира писмено в срока по чл. 53, ал. 3 от ЗЗЛД субекта на данните за всеки отказ за достъп или за ограничаването на достъпа и за причините за това. Тази информация може да не бъде предоставена, когато нейното предоставяне би възпрепятствало постигането на някоя от целите по чл. 54, ал. 3 от ЗЗЛД. Администраторът информира субекта на данните за правото му на жалба до комисията, съответно до инспектората, или за търсене на защита по съдебен ред.

Коригиране, допълване, изтриване или ограничаване на обработването на лични данни може да се откаже, като се отчитат основните права и законните интереси на засегнатото физическо лице, в случаите по чл. 54, ал. 3 от ЗЗЛД. В тези случаи се прилага чл. 54, ал. 4 от ЗЗЛД. Администраторът информира писмено субекта на данните за отказа, както и за причините за него в срока по чл. 53, ал. 3 от ЗЗЛД. Администраторът може да не информира субекта на данните за отказа по ал. 6 в случаите по чл. 54, ал. 3 от ЗЗЛД, като се прилага съответно чл. 54, ал. 4 и 5 от ЗЗЛД.

(4) Субектите на данни имат възможност да упражнят правата си информация, на достъп до на данните, право на коригиране, допълване, изтриване или ограничаване на обработването чрез Инспектората към Висшия съдебен съвет.

Чл. 8. (1) Достъп на физически лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство; след подаване на заявление, респективно искане за достъп на информация; и след тяхното легитимиране. Заявлението се вписва в Регистър на исканията (Приложение № 2). Страните по съдебни дела не подават заявление.

(2) Решението за предоставяне или отказване достъп до лични данни за съответното лице се съобщава в 1-месечен срок от подаване на заявлението, респ. искането.

(3) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(3) Третите страни получават достъп до лични данни, обработвани в Административен съд – Пловдив, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ и др.п.).

II. АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ, ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ И РЕГИСТРИ С ЛИЧНИ ДАННИ

Администратор на лични данни

Чл. 9. (1) Администратор на лични данни по смисъла на чл. 4, ал. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679 е Административен съд – Пловдив със седалище и адрес на управление и за кореспонденция и контакт : град Пловдив 4000, ул. „Иван Вазов" 20. Работно време: понеделник - петък, 08:30 часа - 17:00 часа, електронна поща: plovdiv-adms@.justice.bg; телефон/факс: 032/ 261 070.

(2) Като администратор на лични данни, при обработването на лични данни Административен съд – Пловдив спазва принципите за защита на личните данни, предвидени в Регламента и законодателството на Европейския съюз и Република България.

(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 Административен съд – Пловдив и друг администратор или обработващ, 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 членове 13 и 14 на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, 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.

Чл. 10. Като юридическо лице, възникнало по силата на закон, Административен съд – Пловдив осъществява правораздавателна дейност, регламентирана в Конституцията на Република България, Закона за съдебната власт, Административнопроцесуален кодекс и др. нормативни актове, във връзка с която обработва лични данни и сам определя целите и средствата за обработването им.

Чл. 11. Всеки правен субект, който обработва лични данни по възлагане и от името на администратора, е обработващ лични данни и следва да подпише споразумение за обработка на данни, а за магистратите и служителите от Административен съд – Пловдив да се вмени, като задължение в длъжностните им характеристики включващо клаузите по чл. 28, пар. 2-4 от Общия регламент относно защитата на данните.

Длъжностно лице по защита на данните

Чл. 12. (1) В качеството си на публичен орган Административен съд – Пловдив определя длъжностно лице по защита на данните.

(2) Длъжностно лице по защита на личните данни се определя от Председателя на съда.

Чл. 13. (1) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

1. информира и съветва администратора и служителите, които извършват обработване, за техните задължения по силата на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка;

2. наблюдава спазването на Общия регламент относно защитата на данните и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка;

3. наблюдава спазването на настоящите правила и действащото законодателство по отношение на защитата на личните данни;

4. допринася за повишаване на осведомеността на служителите във Административен съд - Пловдив, участващи в дейностите по обработване;

5. извършва необходимите одити (проверки) за прилагането на изискванията за защита на личните данни Административен съд – Пловдив;

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

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

8. сътрудничи си с Комисията за защита на личните данни в качеството й 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;

9. действа като точка за контакт за надзорния орган 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;

10. води регистър за нарушенията на сигурността на данните;
11. води регистър за искания от субекти на данни.

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

Регистри на лични данни в Административен съд – Пловдив

Чл. 14. В Административен съд – Пловдив се обработват лични данни в следните регистри:

1. „Регистър на дейностите по обработване на лични данни“;
2. Регистър „Човешки ресурси и участници в конкурси процедури в администрацията на Административен съд – Пловдив“;
3. Регистър „Правораздаване и съдебна дейност“;
4. Регистър „Контрагенти, обществени поръчки, счетоводна дейност“.

III. „РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ“

Чл. 15. (1) „Регистър на дейностите по обработване на лични данни“ съдържа информация за:

1. името и координатите за връзка на администратора и на длъжностното лице по защита на данните, ако има такива;
2. целите на обработването;
3. категориите субекти на данни и на категориите лични данни;
4. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
5. предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, документация за подходящите гаранции;
6. предвидените срокове за изтриване на различните категории данни;
7. общо описание на техническите и организационни мерки за сигурност.

IV. РЕГИСТЪР „ЧОВЕШКИ РЕСУРСИ И УЧАСТНИЦИ В КОНКУРСНИ ПРОЦЕДУРИ В АДМИНИСТРАЦИЯТА НА АДМИНИСТРАТИВЕН СЪД – ПЛОВДИВ“

Общо описание на регистъра

Чл. 16. В регистъра се обработват лични данни на съдии, назначени и командировани в Административен съд – Пловдив, с оглед, изпълнение на нормативните изисквания на Закона за съдебната власт (ЗСВ), Кодекса на труда, Наредба за служебните командировки и специализации в чужбина, Наредба за медицинската експертиза и други нормативни актове.

Чл. 17. В регистъра се обработват лични данни на всички служители, назначени на трудови и служебни правоотношения във Административен съд – Пловдив и на лица, участващи в конкурсни процедури в съда.

Чл. 18. Обработването на личните данни е 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, 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;

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.

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 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 съдебната власт при

провеждане на нормативно регламентирани процедури и при кандидатстване за заемана на определена длъжност във Административен съд – Пловдив, както и при последваща необходимост.

(4) Данните на кандидатите за заемане на длъжност във Административен съд – Пловдив се въвеждат директно в договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

(5) Редът и условията за съхраняването и архивирането на всички документи и книжа, както и сроковете за това, са регламентирани в глава X от ПАС, Вътрешните правила за дейността на архива в Административен съд – Пловдив, Номенклатурата на делата със срокове за съхраняване в Административен съд – Пловдив, при спазването на специалните за това закони и подзаконови нормативни актове.

(6) 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. 21. (1) Данните от регистъра се обработват от длъжностни лица от отдел „Финансова дейност и снабдяване", отдел „Стопанисване и управление на съдебното имущество“, сектор „Човешки ресурси ", отдел „Информационно обслужване, статистика и информационни технологии", служба „Регистратура за класифицирана информация", служба „Архив", служители, в чиито длъжностни характеристики е определено задължение за обработване на данните на магистратите, 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. 22. (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 и т.н.), както и на обработващи лични данни, с които администраторът има сключен договор, във връзка с командироване на магистрати.

(2) Във връзка с използването на 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 се трансферират в други държави 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.

(4) 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.

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 административния ръководител на Административен съд – Пловдив. В състава на комисията се включват длъжностното лице по защита на данните, съдебният администратор, съдия /при възникнала необходимост/ и съдебен помощник.

(3) За проверката по ал. 2 се съставя доклад.

Докладът трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. 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, назначената от председателя на съда комисия, определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина - шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни и др.) или Административен съд – Пловдив възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

V. РЕГИСТЪР „ПРАВОРАЗДАВАНЕ И СЪДЕБНА ДЕЙНОСТ“

Общо описание на регистъра

Чл. 25. (1) В регистъра се обработват лични данни на физически лица, които са страни или участници в административните производства, както и на физически лица, сезирали Административен съд – Пловдив и неговата администрация с жалби, молби, искания, предложения, сигнали и др. 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. 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 др.;

3. социална идентичност - данни относно образование, трудова дейност и други като същите са в зависимост от съдържанието на жалбата, искането и др.;

4. лични данни относно съдебното минало на лицата;
5. лични данни относно здравословното състояние на лицата;
6. други данни, посочени от лицата в подадените от тях жалби, молби, искания, предложения, сигнали и др. до Административен съд – Пловдив.

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, като се съдържат в техните жалби, молби, искания, предложения, сигнали, заявления и др. или в документи, предоставяни от държавни органи и органи на местното самоуправление.

(4) Редът и условията за съхраняването и архивирането на всички документи и книжа, както и сроковете за това, са регламентирани в глава X от ПАС, Вътрешните правила за дейността на архива в Административен съд – Пловдив, Номенклатурата на делата със срокове за съхраняване в Административен съд – Пловдив, при спазването на специалните за това закони и подзаконови нормативни актове.

(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, съдебните секретари, съдебните деловодители и от длъжностни лица от отдел „Финансова дейност и снабдяване", отдел „Информационно обслужване, статистика и информационни технологии", служба „Архив", сектор „Пресслужба и информация“ и 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 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 трансферират в други с оглед изпълнение на задължение, произтичащо от нормативен акт.

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 административния ръководител на Административен съд – Пловдив. В състава на комисията се включват длъжностното лице по защита на данните, съдия /при възникнала необходимост/, съдебен помощник и съдебният администратор.

(3) За проверката по ал. 2 се съставя доклад.

Докладът трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. 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. 31. (1) След изтичане на срока за съхранение на данните, комисия определя кои документи подлежат на унищожение и мястото на извършване на процедурата.

(2) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина - шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни, унищожаване на звукозаписи от електронни устройства и компютри по начин възпрепятстващ възстановяването им и др.) или Административен съд – Пловдив възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи. Редът за извършването на звукозаписите и видеозаписите от съдебните заседания, сроковете за съхранението им и комисията по унищожаването им се определят със заповед на председателя на Административен съд Пловдив, при спазване на съобразно установените законови срокове.

VI. РЕГИСТЪР „КОНТРАГЕНТИ, ОБЩЕСТВЕНИ ПОРЪЧКИ, СЧЕТОВОДНА ДЕЙНОСТ“

Общо описание на регистъра

Чл. 32. (1) В регистъра се обработват лични данни на физически лица в изпълнение на договори, по които Административен съд – Пловдив е страна, както и при провеждане на процедури за задоволяване икономическите, социални и битови потребности на служителите на съда. Същите се обработват с цел:

1. изпълнение на нормативните изисквания на Закона за съдебната власт, Закона за обществените поръчки, Закона за счетоводство, Закона за задълженията и договорите, Кодекс на труда,Търговския закон и други;

2. управление на човешките ресурси, финансово-счетоводна дейност, осигуряване на материално-техническата база на Административен съд – Пловдив;

3. 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: 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. 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 технически носител.

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

(4) Редът и условията за съхраняването и архивирането на всички документи и книжа, както и сроковете за това, са регламентирани в глава X от ПАС, Вътрешните правила за дейността на архива в Административен съд – Пловдив, Номенклатурата на делата със срокове за съхраняване в Административен съд – Пловдив, при спазването на специалните за това закони и подзаконови нормативни актове.

(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 съдебния администратор, административния секретар и длъжностни лица от отдел „Финансова дейност и снабдяване“, сектор „Стопанисване и управление на съдебното имущество“ отдел „Информационно обслужване, статистика и информационни технологии", служба „Архив", сектор „Пресслужба и информация“ и 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. 36. (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 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 не се трансферират в други държави, освен при международна проверка на проекти с европейско или международно финансиране.

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 Административен съд – Пловдив, включваща длъжностното лице по защита на данните, съдебен помощник и съдебният администратор.

(3) За проверката по ал. 2 се съставя доклад.

Докладът трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. 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) Унищожението се извършва посредством няколко начина, определени в зависимост от наличните към момента на унищожението технически възможности (чрез разрязване с помощта на машина - шредер и/или чрез изгаряне или разрушаване (отваряне) на корпуса на носителя на данни и др.) или Административен съд - Пловдив възлага на изпълнител тези действия с договор с предмет конфиденциално унищожаване на документи.

VII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

Физическа защита на личните данни

Чл. 39. Физическата защита в Административен съд – Пловдив се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 40 . (1) Основните организационни мерки за физическа защита в Административен съд – Пловдив включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
3. определяне на организацията на физическия достъп.

(2) Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран - само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп на 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.

(3) Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(4) 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.

(5) Зони с контролиран достъп са всички помещения на територията на Административен съд – Пловдив, в които се събират, обработват и съхраняват лични данни.

(6) Използваните технически средства за физическа защита на личните данни в Административен съд – Пловдив са съобразени с действащото законодателство и нивото на въздействие на тези данни. 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.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

(8) 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.

Чл. 41. (1). Основните технически мерки за физическа защита в Административен съд – Пловдив включват:

1. използване на ключалки и заключващи механизми;

2. използване на контрол на достъп с електронно заключване и отключване с магнитни карти и чипове;

3. шкафове, метални каси;

4. оборудване на помещенията с пожароизвестителни и пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в шкафове, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават съответните съдебни служители по силата на служебните им задължения и длъжностната характеристика.

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

(4) Пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Персонална защита на личните данни

Чл. 42. (1) Основните мерки за персонална защита на личните данни, приложими в Административен съд – Пловдив, са:

1. Лицата, обработващи лични данни са задължени да познават нормативната уредба в областта на защита на личните данни (Общия регламент относно защитата на данните (ЕС) 2016/679, Закона за защита на личните данни и настоящите Правила и Политиката по сигурност на информацията в Административен съд – Пловдив, утвърдена от административния ръководител през 2019 г. Съдии и съдебни служители се запознават с настоящите Вътрешни правила след утвърждаването им, включително и при последващо актуализиране, както и при постъпване на работа, което се удостоверява с полагане на подпис в „Списък за запознаване на вътрешните правила за защита на личните данни обработвани в Административен съд - Пловдив“;
2. Запознаване и осъзнаване на опасностите за личните данни, обработвани от Административен съд – Пловдив;
3. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..) между щатния състав и всякакви други лица, които са неоторизирани;
4. Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

(2) За лични данни, оценени с по-висока степен на риск, като чувствителни лични данни, се прилагат освен мерките по ал. 1 и следните допълнителни мерки:

1. Провеждане на специализирани обучения за работа и опазване на лични данни, в случай че спецификата на служебните задължения изисква подобно;
2. Приемане мерки за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения изисква подобно.

Документална защита на личните данни

Чл. 43. (1) Основните мерки за документална защита на личните данни, са:

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 Административен съд – Пловдив, 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 бизнес дейност на Административен съд – Пловдив, 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 Административен съд – Пловдив или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(2) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 1, се прилагат и следните допълнителни мерки:

1. Контрол на достъпа до регистрите, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа на „Необходимост да знае”, за да изпълняват техните задължения;

2. Правила за размножаване и разпространение, които разрешават копиране и разпространяване на лични данни 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;

Защита на автоматизираните информационни системи и/или мрежи

Чл. 44. (1) Защитата на автоматизираните информационни системи и/или мрежи в Административен съд – Пловдив включва 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.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на Административен съд – Пловдив. Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да се знае”;

2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка.

3. Управление на външни връзки и/или свързване, включващо от своя страна:

а) дефиниране на обхвата на вътрешната мрежа: Като вътрешна мрежа се разглежда локална жична мрежа и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на Административен съд – Пловдив. Като външна мрежа се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на Административен съд – Пловдив;

б) регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено съдиите и служителите и/или специално упълномощени от административния ръководител на Административен съд – Пловдив лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимост да се знае“. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола;

в) администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на системния администратор. В отговорностите му са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Административен съд – Пловдив;

г) контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на системния администратор. Той е задължен да предприеме адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на Административен съд – Пловдив, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти;

4. Защитата от зловреден софтуер включва:

а) използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира,

инсталира и поддържа от системния администратор. Забранено е инсталирането на софтуерни продукти без изричното му одобрение;

б) използване на вградената функционалност за защита на операционната система и/или хардуера, които се настройват единствено от системния администратор или от оторизирани от ръководството на Административен съд – Пловдив лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена;

в) активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции;

г) забрана за пренос на данни от външен носител;

д) при съмнение или установяване на заразяване на 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). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.

5. Политика по създаване и поддържане на резервни копия за възстановяване, която регламентира:

а) основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на Административен съд – Пловдив;

б) начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител;

в) отговорност за архивиране има системният администратор;

г) срокът на архивиране следва да е съобразен с действащото законодателство;

д) съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа;

6. Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти и др. носители на информация, еднократно записваеми носители и др.);

7. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на Административен съд – Пловдив;

8. Данните, които вече не са необходими за целите на Административен съд – Пловдив и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства);

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на Административен съд – Пловдив:

а) отдалечен достъп до вътрешната мрежа на Административен съд – Пловдив не е предвиден. По изключение, и след изричната санкция от ръководството на съда, може да се разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни;

б) публикуването на служебна информация на интернет страницата на Административен съд – Пловдив или в интернет пространството, независимо под каква форма и на каква платформа, се

извършва единствено от системния администратор или след писмено разрешение от административния ръководител на Административен съд – Пловдив.

2. Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на Административен съд – Пловдив, включват:

а) забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на Административен съд – Пловдив, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър;

б) мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (магнитни карти за контрол на достъпа, ключалки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Правила и мерки за осигуряване на защита на личните данни при компютърна обработка

Чл. 45. (1) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) Административен съд – Пловдив прилага адекватни мерки за технически и административен контрол (ограничаване на IP, MAC адрес, уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност, като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) С цел повишаване сигурността на достъпа до информация в случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(5) Лични данни за лицата възпроизведени със звукозапис и видеозапис от съдебните заседания по административните дела ще бъдат съхранявани и обработвани от съдии и служители на съда, като след отпадане на основанието за достъп до тях или изтичане сроковете за съхранението достъпът ще се преустановява чрез изтриването им от устройствата по начин непозволяващ възстановяването им.

Чл. 46. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 47. (1) В Административен съд – Пловдив се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от системния администратор. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни, предварително се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

(4) Съдии и служители, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

VIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

Чл. 48. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Административен съд – Пловдив. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при:

1. при използване на нови технологии;

2. автоматизирано обработване, включително профилиране или

автоматизирано вземане на решения;

3. обработване на чувствителни лични данни в голям мащаб;

4. мащабно, систематично наблюдение на публично обществена зона;

5. обработване на лични данни за присъди и нарушения;

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

(3) Оценката 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, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на

спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

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

(5) Ако извършената оценката на въздействието покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска, следва да се извърши консултация с Комисия по защита на личните данни преди планираното обработване.

IX. ПРОЦЕДУРА ПО ДОКЛАДВАНЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Чл. 49. (1) При регистриране на неправомерен достъп/нарушение на сигурността до информационните масиви за лични данни, или при друго нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен своевременно да информира и длъжностното лице по защита на данните за инцидента.

(2) Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му.

(3) Длъжностното лице писмено уведомява за инцидента администратора, като му предоставя наличната информация относно характера на инцидента, времето на установяване, вида на щетите, предприетите мерки за ограничаване на щетите.

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

Чл. 50. (1) В случай, че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след съгласуване с администратора, длъжностното лице по защита на личните данни, организира изпълнението на задължението на администратора за уведомяване на Комисията за защита на личните данни.

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

(3) Уведомлението 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.

(4) 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 личните данни, без ненужно забавяне, уведомява засегнатите физически лица.

Чл. 51. Длъжностното лице по защита на личните данни води регистър за нарушенията на сигурността на данните, 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 уведомявания: 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.

X. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 52. Всички съдии и служители в Административен съд – Пловдив са длъжни да се запознаят с настоящите Вътрешни правила срещу подпис в „Списъка за запознаване с вътрешните правила за защита на личните данни обработвани в Административен съд - Пловдив“ и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 53. Контрол по прилагане на мерките за физическа, персонална и документална защита на личните данни осъществява лицето по защита на лични данни, определено със заповед на председателя на Административен съд – Пловдив, а контролът по криптографската защита и защита на автоматизирани информационни системи и мрежи от системен администратор.

Чл. 54. Надзор и осигуряване спазването на Регламент (ЕС) 2016/679 и Закон за защита на личните данни при обработване на лични данни в Административен съд – Пловдив във връзка с изпълнение на функциите му на орган на съдебната власт осъществява Инспектората към Висшия съдебен съвет съгласно Глава Трета от Закона за защита на личните данни (изм. и доп., ДВ бр. 17 от 26.02.2019 г.).

Чл. 55. (1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Закона за защита на личните данни (изм. и доп., ДВ бр. 17 от 26.02.2019 г.), Общия регламент относно защитата на данните (ЕС) 2016/679 и приложимото право на Европейския съюз.

(2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

1. Приложение № 1 „Декларация за съгласие“;
2. Приложение № 2 „Искане за предоставяне на достъп до лични данни“;
3. Приложение № 3 „Декларация по процедура за провеждане на конкурс“.

Чл. 56. Вътрешните правила са Утвърдени със Заповед на административния ръководител-председател на Административен съд – Пловдив и се актуализират по реда на тяхното утвърждаване.

Настоящите Вътрешни правила са утвърдени със заповед № РД - 84/16.03.2026 г. на председателя на Административен съд – Пловдив.